Protocol Configuration and Monitoring
Reference Volume 2
Version 3.4
Chapter 2. Using TN3270

Overview
Placement of the TN3270 Server Function
TN3270E Server Function
TN3270 Host On-Demand Client Caching

General TN3270E Server Configuration
Loading the TN3270 Server Code
Configuring TN3270 under the APPN Protocol
Server IP Address
Server TCP Ports
Defining PUs
Defining LUs
Configured LUs

Dynamic Definition of Dependent LUs (DDDLU)
Host-Initiated Dynamic Definition of Dependent LUs (HIDLU)
Client to LU Mapping
Client IP Address to LU/Pool Mapping
Server TCP Port to Pool Association
Port and IP Address Mapping Combined
Load Balancing among Multiple PUs

Example Configurations
Configuring TN3270 using DLUR
Configuring TN3270E Using a Subarea Connection

Chapter 3. Configuring and Monitoring APPN

Accessing the APPN Configuration Process
APPN Configuration Command Summary
APPN Configuration Command Detail
Enable/Disable
Set
Add
Delete
Running Banyan VINES on the Bridging Router ........................................... 303
Running Banyan VINES over WAN Links ...................................................... 303

Chapter 7. Configuring and Monitoring VINES ............................................. 305
Accessing the VINES Configuration Environment ....................................... 305
VINES Configuration Commands ............................................................... 305
Add ............................................................................................................. 305
Delete ......................................................................................................... 306
Disable ...................................................................................................... 306
Enable ........................................................................................................ 306
List ............................................................................................................. 307
Set .............................................................................................................. 308
Accessing the VINES Monitoring Environment ........................................... 308
VINES Monitoring Commands .................................................................. 309
Counters .................................................................................................... 309
Dump .......................................................................................................... 310
Route ......................................................................................................... 311

Chapter 8. Using DNA IV ............................................................................. 313
DNA IV Overview ...................................................................................... 313
DNA IV Terminology and Concepts ............................................................. 314
Routing ...................................................................................................... 315
Routing Tables .......................................................................................... 315
Area Routers ............................................................................................. 315
Configuring Routing Parameters ................................................................. 316
IBM's Implementation of DNA IV ................................................................. 316
Managing Traffic Using Access Control ....................................................... 317
Managing Traffic Using Area Routing Filters ............................................. 320
Configuring DNA IV .................................................................................. 325

Chapter 9. Configuring and Monitoring DNA IV ......................................... 329
DNA IV Configuration and Monitoring Commands ....................................... 329
Define/Set .................................................................................................. 330
Purge .......................................................................................................... 338
Set .............................................................................................................. 338
Show .......................................................................................................... 338
Show/List .................................................................................................. 341
Zero ............................................................................................................ 347

Chapter 10. Using OSI/DECnet V ................................................................. 349
OSI Overview ............................................................................................ 349
NSAP Addressing ....................................................................................... 350
IDP .............................................................................................................. 350
DSP ............................................................................................................ 351
IS-IS Addressing Format ............................................................................. 351
GOSIP Version 2 NSAPs ............................................................................ 351
Multicast Addresses ................................................................................... 352
OSI Routing ............................................................................................... 353
IS-IS Protocol ............................................................................................. 353
IS-IS Areas ................................................................................................ 353
IS-IS Domain ............................................................................................. 353
IS to IS Hello (IIH) Message ..................................................................... 355
L1 IIH Message .......................................................................................... 355
L2 IIH Message .......................................................................................... 356
Point-to-Point IIH Message ....................................................................... 356
Designated IS ............................................................................................ 356
Chapter 13. Configuring and Monitoring NHRP

Chapter 14. Using IP Version 6 (IPv6)
Chapter 15. Configuring and Monitoring IPv6 ........................................... 445
Accessing the IPv6 Configuration Environment ........................................ 445
IPv6 Configuration Commands ................................................................. 445
  Add ........................................ 445
  Change .................................... 451
  Delete .................................... 452
  Disable ................................... 452
  Enable .................................... 452
  List ....................................... 453
  Move ....................................... 455
  Set ......................................... 455
  Update ..................................... 458
  Update Packet-filter Commands ......................................................... 458
Accessing the IPv6 Monitoring Environment ............................................. 463
IPv6 Monitoring Commands ................................................................. 463
  Access-control ................................ 464
  Cache ..................................... 464
  Counters ................................... 464
  Dump routing tables ................................................................. 464
  Interface addresses ............................................................... 465
  Internal address ...................................... 465
  Mcast ..................................... 465
  Mld .......................................... 465
  Reset ....................................... 466
  Route ....................................... 466
  Sizes ........................................ 466
  Sniffer .................................... 466
  Static routes .................................. 467
  Packet-filter ................................... 467
  Path-mtu .................................... 467
  Ping6 ........................................ 468
  Traceroute6 ................................... 468
  Tunnels ....................................... 469
IPv6 Dynamic Reconfiguration Support .................................................... 469
  CONFIG (Talk 6) Delete Interface .................................................. 469
  GWCON (Talk 5) Activate Interface ............................................... 470
  GWCON (Talk 5) Reset Interface .................................................. 470
  GWCON (Talk 5) Component Reset Commands ........................................ 470
  CONFIG (Talk 6) Immediate Change Commands ....................................... 470

Chapter 16. Configuring and Monitoring Neighbor Discovery Protocol (NDP) ....................... 473
Accessing the NDP Configuration Environment ......................................... 473
NDP Configuration Commands ............................................................ 473
  Add ........................................ 473
  Change .................................... 475
  Delete .................................... 477
  Disable ................................... 477
  Enable .................................... 477
  List ....................................... 478
  Set ......................................... 478
Accessing the NDP Monitoring Environment ............................................. 478
NDP Monitoring Commands ................................................................. 479
  DHCPv6-Relay ................................ 479
  Dump ....................................... 479
  List ......................................... 479

Using PIM

Accessing the PIM Configuration Environment

PIM Configuration Commands

Delete

Disable

Enable

List

Set

Accessing the PIM Monitoring Environment

PIM Monitoring Commands

Dump routing tables

Clear

Interface

Join

Leave

Mcache

Mgroups

Mstats

Neighbor

PIM

Summary PIM

Ping

Reset

Traceroute

Variables

PIM Dynamic Reconfiguration Support

CONFIG (Talk 6) Delete Interface

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) Component Reset Commands

PIM for IPv6 Dynamic Reconfiguration Support

CONFIG (Talk 6) Delete Interface

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) Component Reset Commands

Multicast Forwarding Cache Dynamic Reconfiguration Support

CONFIG (Talk 6) Delete Interface

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) Reset Interface

Non-Dynamically Reconfigurable Commands

Multicast Forwarding Cache V6 Dynamic Reconfiguration Support

CONFIG (Talk 6) Delete Interface

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) Reset Interface

Non-Dynamically Reconfigurable Commands
<table>
<thead>
<tr>
<th>Chapter 18. Configuring and Monitoring Routing Information Protocol (RIP6)</th>
<th>501</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing the RIP6 Configuration Environment</td>
<td>501</td>
</tr>
<tr>
<td>RIP6 Configuration Commands</td>
<td>501</td>
</tr>
<tr>
<td>Add</td>
<td>501</td>
</tr>
<tr>
<td>Change</td>
<td>502</td>
</tr>
<tr>
<td>Delete</td>
<td>504</td>
</tr>
<tr>
<td>Disable</td>
<td>504</td>
</tr>
<tr>
<td>Enable</td>
<td>506</td>
</tr>
<tr>
<td>List</td>
<td>507</td>
</tr>
<tr>
<td>Set</td>
<td>507</td>
</tr>
<tr>
<td>Accessing the RIP6 Monitoring Environment</td>
<td>510</td>
</tr>
<tr>
<td>RIP6 Monitoring Commands</td>
<td>510</td>
</tr>
<tr>
<td>Dump</td>
<td>511</td>
</tr>
<tr>
<td>List</td>
<td>511</td>
</tr>
<tr>
<td>Ping6</td>
<td>511</td>
</tr>
<tr>
<td>Reset</td>
<td>511</td>
</tr>
<tr>
<td>Traceroute6</td>
<td>511</td>
</tr>
<tr>
<td>RIP6 Dynamic Reconfiguration Support</td>
<td>511</td>
</tr>
<tr>
<td>CONFIG (Talk 6) Delete Interface</td>
<td>511</td>
</tr>
<tr>
<td>GWCON (Talk 5) Activate Interface</td>
<td>511</td>
</tr>
<tr>
<td>GWCON (Talk 5) Reset Interface</td>
<td>512</td>
</tr>
<tr>
<td>GWCON (Talk 5) Component Reset Commands</td>
<td>512</td>
</tr>
<tr>
<td>CONFIG (Talk 6) Immediate Change Commands</td>
<td>512</td>
</tr>
<tr>
<td>Non-Dynamically Reconfigurable Commands</td>
<td>512</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 19. Configuring and Monitoring BGP6</th>
<th>513</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing the BGP6 Configuration Environment</td>
<td>513</td>
</tr>
<tr>
<td>BGP6 Configuration Commands</td>
<td>513</td>
</tr>
<tr>
<td>Add</td>
<td>514</td>
</tr>
<tr>
<td>Attach</td>
<td>519</td>
</tr>
<tr>
<td>Change</td>
<td>519</td>
</tr>
<tr>
<td>Delete</td>
<td>521</td>
</tr>
<tr>
<td>Disable</td>
<td>522</td>
</tr>
<tr>
<td>Enable</td>
<td>523</td>
</tr>
<tr>
<td>List</td>
<td>523</td>
</tr>
<tr>
<td>Move</td>
<td>526</td>
</tr>
<tr>
<td>Set</td>
<td>526</td>
</tr>
<tr>
<td>Update</td>
<td>526</td>
</tr>
<tr>
<td>Accessing the BGP6 Monitoring Environment</td>
<td>528</td>
</tr>
<tr>
<td>BGP6 Monitoring Commands</td>
<td>528</td>
</tr>
<tr>
<td>Disable Neighbor</td>
<td>529</td>
</tr>
<tr>
<td>Dump Routing Tables</td>
<td>529</td>
</tr>
<tr>
<td>Enable Neighbor</td>
<td>530</td>
</tr>
<tr>
<td>List</td>
<td>530</td>
</tr>
<tr>
<td>Neighbors</td>
<td>532</td>
</tr>
<tr>
<td>Parameter</td>
<td>533</td>
</tr>
<tr>
<td>Paths</td>
<td>534</td>
</tr>
<tr>
<td>Ping6</td>
<td>534</td>
</tr>
<tr>
<td>Policy-List</td>
<td>535</td>
</tr>
<tr>
<td>Reset Neighbor</td>
<td>535</td>
</tr>
<tr>
<td>Sizes</td>
<td>535</td>
</tr>
<tr>
<td>Traceroute6</td>
<td>536</td>
</tr>
<tr>
<td>BGP6 Dynamic Reconfiguration Support</td>
<td>536</td>
</tr>
<tr>
<td>CONFIG (Talk 6) Delete Interface</td>
<td>536</td>
</tr>
<tr>
<td>GWCON (Talk 5) Activate Interface</td>
<td>536</td>
</tr>
</tbody>
</table>
Figures

1. Extended Border Node Connectivity ........................................ 15
2. Data Flow in an APPN Configuration Using DLSw Port ...................... 37
3. Logical View with Frame Relay Bridged Frame/BAN Connection Network Support ........................................ 38
4. APPN Frame Relay Bridged Frame/BAN Connection Network .................... 39
5. Single Connection Network using BAN with 1 Frame Relay Port .................. 40
6. Single Connection Network using BAN with Multiple Frame Relay Ports ................. 40
7. Multiple Connection Networks using BAN ........................................ 40
8. Single Connection Network using Bridging with One Frame Relay Port ................. 41
9. Single Connection Network Using Bridging with Multiple Frame Relay Ports ................. 41
10. Multiple Connection Networks Using Bridging ...................................... 42
11. Example of Zone Filtering ........................................................ 281
12. Example of Network Filtering ..................................................... 283
13. Sample Routing Table .............................................................. 300
14. Sample Neighbor Table ............................................................ 301
15. Example of Inclusive Access Control ........................................... 319
16. Example of Exclusive Access Control ............................................ 320
17. Example of Area Routing Filter for Security ................................... 322
18. Example of Blending DECnet Domains ........................................... 324
19. OSI Network ........................................................................... 349
20. NSAP Address Structure ............................................................ 350
21. IS-IS NSAP Addressing Interpretation ........................................ 351
22. GOSIP Address Format .............................................................. 352
23. OSI Domain ............................................................................ 354
24. Synonymous Areas .................................................................. 355
25. Internal and External Routing Metrics .......................................... 360
27. NHRP in a Classic IP Environment .............................................. 410
28. NHRP in a Classic IP Environment with non-NHRP Device ................. 410
29. NHRP in an ELAN Environment .................................................. 411
30. NHRP in an ELAN Environment with LAN Switches .......................... 412
31. NHRP in a Mixed Classical IP and ELAN Environment ...................... 413
32. NHRP to an Egress Router ........................................................ 413
33. Using Disallowed Router-to-Router Shortcuts ................................. 418
Tables

1. Implementation of APPN Network Node Functions .................................................. 3
2. Port Types Supported for APPN Routing ................................................................. 20
3. Device/model type Values ....................................................................................... 81
4. APPN Configuration Command Summary ............................................................... 95
5. Configuration Parameter List - APPN Routing ......................................................... 97
6. Configuration Parameter List - High-Performance Routing (HPR) ......................... 104
7. Configuration Parameter List - HPR Timer and Retry Options .............................. 104
8. Configuration Parameter List - Dependent LU Requester .................................... 107
9. Configuration Parameter List - APPN Node Tuning ............................................. 112
10. Configuration Parameter List - Trace Setup Questions .................................... 117
11. Configuration Parameter List - Node Level Traces ............................................. 119
12. Configuration Parameter List - Inter-process Signals Traces ............................ 124
13. Configuration Parameter List - Module Entry and Exit Traces ......................... 128
14. Configuration Parameter List - General Component Level Traces .................... 130
15. Configuration Parameter List - Miscellaneous Traces ..................................... 135
17. Configuration Parameter List - APPN ISR Recording Media ............................... 139
18. Configuration Parameter List - Port Configuration ............................................. 141
19. Configuration Parameter List - Port Configuration for ATM ............................ 146
20. Configuration Parameter List - Port Definition .................................................. 152
21. Configuration Parameter List - Port Default TG Characteristics ....................... 157
22. Configuration Parameter List - Port default LLC Characteristics ....................... 163
23. Configuration Parameter List - HPR Override Defaults ..................................... 165
24. Configuration Parameter List - Link Station - Detail ......................................... 166
25. Configuration Parameter List - Station Configuration for ATM ....................... 178
27. Configuration Parameter List - Modify Dependent LU Server ......................... 186
29. Configuration Parameter List - Modify HPR Defaults ........................................ 190
30. Configuration Parameter List - LEN End Node LU Name ................................... 191
31. Configuration Parameter List - Connection Network - Detail ......................... 192
32. Configuration Parameter List - Connection Network Configuration for ATM .... 195
33. Configuration Parameter List - TG Characteristics (Connection Network) ........ 199
34. Configuration Parameter List - APPN COS - Mode Name to COS Name Mapping - Detail 202
35. Configuration Parameter List - APPN Additional port to Connection Network ...... 204
36. Configuration Parameter List - APPN Implicit Focal Point .................................. 204
37. Configuration Parameter List - APPN Local PU .................................................. 205
38. Configuration Parameter List - Routing List Configuration .................................. 208
39. Configuration Parameter List - COS Mapping Table Configuration .................. 212
40. TN3270E Configuration Command Summary .................................................... 215
41. Configuration Parameter List - Set TN3270E ...................................................... 215
42. Configuration Parameter List - Add TN3270E Implicit ....................................... 219
43. Configuration Parameter List - Add TN3270E LU .............................................. 221
44. Configuration Parameter List - Add TN3270E Map ............................................ 225
45. Configuration Parameter List - Add TN3270E Port ............................................ 226
46. Configuration Parameter List - Delete TN3270E LU .......................................... 227
47. Configuration Parameter List - Delete TN3270E Implicit ................................... 228
48. Configuration Parameter List - Delete TN3270E Map ........................................ 229
49. Configuration Parameter List - Delete TN3270E Port ........................................ 230
50. APPN Monitoring Command Summary .............................................................. 231
51. TN3270E Server Monitoring Command Summary ............................................ 233
52. Flags. .................................................................................................................. 234
53. APING Output Description .................................................................................. 235
<table>
<thead>
<tr>
<th>No.</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>54</td>
<td>List appc_sessions Output Description</td>
<td>237</td>
</tr>
<tr>
<td>55</td>
<td>Output Description</td>
<td>238</td>
</tr>
<tr>
<td>56</td>
<td>List dlur-dlus Output Description</td>
<td>238</td>
</tr>
<tr>
<td>57</td>
<td>List dlur lu Output Description</td>
<td>239</td>
</tr>
<tr>
<td>58</td>
<td>Output Description</td>
<td>241</td>
</tr>
<tr>
<td>59</td>
<td>Output Description</td>
<td>241</td>
</tr>
<tr>
<td>60</td>
<td>Output Description</td>
<td>241</td>
</tr>
<tr>
<td>61</td>
<td>Output Description</td>
<td>242</td>
</tr>
<tr>
<td>62</td>
<td>Output Description</td>
<td>242</td>
</tr>
<tr>
<td>63</td>
<td>Output Description</td>
<td>243</td>
</tr>
<tr>
<td>64</td>
<td>Output Description</td>
<td>244</td>
</tr>
<tr>
<td>65</td>
<td>Output Description</td>
<td>244</td>
</tr>
<tr>
<td>66</td>
<td>Output Description</td>
<td>246</td>
</tr>
<tr>
<td>67</td>
<td>Output Description</td>
<td>247</td>
</tr>
<tr>
<td>68</td>
<td>Output Description</td>
<td>248</td>
</tr>
<tr>
<td>69</td>
<td>Output Description</td>
<td>249</td>
</tr>
<tr>
<td>70</td>
<td>Partner Table</td>
<td>250</td>
</tr>
<tr>
<td>71</td>
<td>Connection Table</td>
<td>250</td>
</tr>
<tr>
<td>72</td>
<td>Output Description</td>
<td>251</td>
</tr>
<tr>
<td>73</td>
<td>Output Description</td>
<td>253</td>
</tr>
<tr>
<td>74</td>
<td>Output Description</td>
<td>254</td>
</tr>
<tr>
<td>75</td>
<td>Output Description</td>
<td>254</td>
</tr>
<tr>
<td>76</td>
<td>Output Description</td>
<td>256</td>
</tr>
<tr>
<td>77</td>
<td>Output Description</td>
<td>256</td>
</tr>
<tr>
<td>78</td>
<td>Output Description</td>
<td>256</td>
</tr>
<tr>
<td>79</td>
<td>Output Description</td>
<td>257</td>
</tr>
<tr>
<td>80</td>
<td>Log view Submenu Syntax</td>
<td>258</td>
</tr>
<tr>
<td>81</td>
<td>Output Description (Summary Page, left to right)</td>
<td>260</td>
</tr>
<tr>
<td>82</td>
<td>Output Description (Event Details)</td>
<td>260</td>
</tr>
<tr>
<td>83</td>
<td>Output Description</td>
<td>261</td>
</tr>
<tr>
<td>84</td>
<td>Output Description</td>
<td>263</td>
</tr>
<tr>
<td>85</td>
<td>Output Description</td>
<td>264</td>
</tr>
<tr>
<td>86</td>
<td>TN3270E Monitoring Command Summary</td>
<td>265</td>
</tr>
<tr>
<td>87</td>
<td>Flag Description</td>
<td>266</td>
</tr>
<tr>
<td>88</td>
<td>Output Description</td>
<td>266</td>
</tr>
<tr>
<td>89</td>
<td>Output Description</td>
<td>267</td>
</tr>
<tr>
<td>90</td>
<td>Output Description</td>
<td>268</td>
</tr>
<tr>
<td>91</td>
<td>Output Description</td>
<td>269</td>
</tr>
<tr>
<td>92</td>
<td>Output Description</td>
<td>270</td>
</tr>
<tr>
<td>93</td>
<td>Output Description</td>
<td>271</td>
</tr>
<tr>
<td>94</td>
<td>Output Description</td>
<td>271</td>
</tr>
<tr>
<td>95</td>
<td>Output Description</td>
<td>272</td>
</tr>
<tr>
<td>96</td>
<td>Output Description</td>
<td>273</td>
</tr>
<tr>
<td>97</td>
<td>Output Description</td>
<td>274</td>
</tr>
<tr>
<td>98</td>
<td>AppleTalk Phase 2 Configuration Commands Summary</td>
<td>285</td>
</tr>
<tr>
<td>99</td>
<td>AppleTalk Phase 2 Monitoring Command Summary</td>
<td>292</td>
</tr>
<tr>
<td>100</td>
<td>Vines IP Header Fields Summary</td>
<td>298</td>
</tr>
<tr>
<td>101</td>
<td>Client and Service Node VINES ARP States</td>
<td>302</td>
</tr>
<tr>
<td>102</td>
<td>VINES Configuration Commands Summary</td>
<td>305</td>
</tr>
<tr>
<td>103</td>
<td>VINES Monitoring Command Summary</td>
<td>309</td>
</tr>
<tr>
<td>104</td>
<td>DNA IV and DNA V Algorithm Considerations</td>
<td>325</td>
</tr>
<tr>
<td>105</td>
<td>NCP Configuration and Monitoring Commands</td>
<td>329</td>
</tr>
<tr>
<td>106</td>
<td>IS-IS Multicast Addresses</td>
<td>352</td>
</tr>
<tr>
<td>107</td>
<td>OSI Configuration Commands Summary</td>
<td>367</td>
</tr>
<tr>
<td>108</td>
<td>OSI/DECnet V Monitoring Commands Summary</td>
<td>391</td>
</tr>
<tr>
<td>109</td>
<td>NHRP Configuration Command Summary</td>
<td>421</td>
</tr>
</tbody>
</table>
IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.
Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

Advanced Peer-to-Peer Networking
APPN
eNetwork
IBM
OS/2
SecureWay
VTAM

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

NetView is a trademark of Tivoli Systems, Inc. in the United States or other countries or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.
This manual belongs to the product library described in IBM 2210 Nways Multiprotocol Router Publications on page xxiv and describes a group of protocols supported by the 2210. A specific 2210 might not support all of the features and functions described in these manuals. If a feature or function is device-specific, that restriction is indicated in the relevant manual.

This manual refers to the 2210 as either “the router” or “the device.” The examples in the library represent the configuration of a 2210, but the actual output you see may vary. Use the examples as a guideline to what you might see while configuring your device.

Who Should Read This Manual

This manual is intended for persons who install and operate computer networks. Although experience with computer networking hardware and software is helpful, you do not need programming experience to use the protocol software.

Getting Additional Information

Changes may be made to the documentation after the books are printed. If additional information is available or if changes are required after the books have been printed, the changes will be in a file (named README) on the CD-ROM. You can view the file with an ASCII text editor.

About the Software

IBM Nways Multiprotocol Routing Services is the software that supports the IBM 2210 (licensed program number 5801-ARR). This software has these components:

- The base code, which consists of:
  - The code that provides the routing, bridging, data link switching, and SNMP agent functions for the device.
  - The router user interface, which allows you to configure, monitor, and use the Multiprotocol Routing Services base code installed on the device. The router user interface is accessed locally through an ASCII terminal or emulator attached to the service port, or remotely through a Telnet session or modem-attached device.

The base code is installed at the factory on the 2210.

- The Configuration Program for IBM Nways Multiprotocol Routing Services (referred to in this book as the Configuration Program) is a graphical user interface that enables you to configure the device from a stand-alone workstation. The Configuration Program includes error checking and online help information.

The Configuration Program is not pre-loaded at the factory; it is shipped separately from the device as part of the software order.

You can also obtain the Configuration Program for IBM Nways Multiprotocol Routing Services from the IBM Networking Technical Support home page. See Configuration Program User’s Guide for Nways Multiprotocol and Access Services, GC30-3830, for the server address and directories.
Conventions Used in This Manual

The following conventions are used in this manual to show command syntax and program responses:

1. The abbreviated form of a command is underlined as shown in the following example:
   
   `reload`

   In this example, you can enter either the whole command (reload) or its abbreviation (rel).

2. Keyword choices for a parameter are enclosed in brackets and separated by the word or. For example:
   
   `command [keyword1 or keyword2]`

   Choose one of the keywords as a value for the parameter.

3. Three periods following an option mean that you enter additional data (for example, a variable) after the option. For example:
   
   `time host ...`

   In this example, you enter the IP address of the host in place of the periods, as explained in the description of the command.

4. In information displayed in response to a command, defaults for an option are enclosed in brackets immediately following the option. For example:
   
   `Media (UTP/STP) [UTP]`

   In this example, the media defaults to UTP unless you specify STP.

5. Keyboard key combinations are indicated in text in the following ways:
   • `Ctrl-P`
   • `Ctrl -`

   The key combination `Ctrl -` indicates that you should press the Ctrl key and the hyphen simultaneously. In certain circumstances, this key combination changes the command line prompt.

6. Names of keyboard keys that you press are indicated like this: `Enter`

7. Variables (that is, names used to represent data that you define) are denoted by italics. For example:
   
   `File Name: filename.ext`

IBM 2210 Nways Multiprotocol Router Publications

**Library reorganization:** Beginning with Version 3.2, the following changes to the organization of the library took place:

- The information in the `Software User's Guide` titled *Understanding, Using and Configuring Features* was moved into a new manual, *Using and Configuring Features*.

- The chapters on using, configuring, and monitoring the DIALs feature were moved into the *Using and Configuring Features* book.

**Information updates and corrections:** To keep you informed of engineering changes, clarifications, and fixes that were implemented after the books were printed, refer to the IBM networking home page at:

http://www.networking.ibm.com
The following list shows the books that support the IBM 2210.

**Operations and Network Management**

**SC30-3681**  
*Software User’s Guide*  
This book explains how to:
- Configure, monitor, and use the IBM Nways Multiprotocol Routing Services software shipped with the router.
- Use the Multiprotocol Routing Services command-line router user interface to configure and monitor the network interfaces and link-layer protocols shipped with the router.

**SC30-3992**  
*Using and Configuring Features*

**SC30-3680**  
*Protocol Configuration and Monitoring Reference Volume 1*

**SC30-3865**  
*Protocol Configuration and Monitoring Reference Volume 2*

These books describe how to access and use the Multiprotocol Routing Services command-line router user interface to configure and monitor the routing protocol software and features shipped with the router.

They include information about each of the protocols that the devices support.

**SC30-3682**  
*Event Logging System Messages Guide*

This book contains a listing of the error codes that can occur, along with descriptions and recommended actions to correct the errors.

**Configuration**

**Online help**  
The help panels for the Configuration Program assist the user in understanding the program functions, panels, configuration parameters, and navigation keys.

**GC30-3830**  
*Configuration Program User’s Guide for Nways Multiprotocol and Access Services*

This book discusses how to use the Configuration Program.

**GG24-4446**  
*IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios*

This book contains examples of how to configure protocols using IBM Nways Multiprotocol Routing Services.

**Safety**

**SD21-0030**  
*Caution: Safety Information - Read This First*

This book provides translations of caution and danger notices applicable to the installation and maintenance of an IBM 2210.
The following list shows the books in the IBM 2210 Nways Multiprotocol Router library, arranged according to tasks.

**Planning and Installation**

**GA27-4068**  
*IBM 2210 Introduction and Planning Guide*

**GC30-3867**  
*IBM 2210 Nways Multiprotocol Router Installation and Initial Configuration Guide*

These books are shipped with the 2210. They explain how to prepare for installation, install the 2210, perform an initial configuration, and verify that the installation is successful.

These books provide translations of danger notices and other safety information.

**Diagnostics and Maintenance**

**SY27-0345**  
*IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual*

This book is shipped with the 2210. It provides instructions for diagnosing problems with and repairing the 2210.

---

**Summary of Changes for the IBM 2210 Software Library**

The following list applies to the changes in the software that were made in Version 3 Release 4:

- **Frame Relay enhancements:**
  - New Frame Handler (FH) support
  - PU throttling to handle bursts of traffic in support of 3745 controllers
  - New interface type (Frame Relay subinterface) to allow virtual interfaces on the same physical interface
  - Unnumbered IP support

- **VPN enhancements:**
  - CPE enhancements:
    - Policy information from LDAP servers is locally stored.
    - Policy quick configuration.
    - Policy consistency checking.
    - Policy information may now be retrieved from LDAP servers within an administrative domain.
    - IPSec tunnel ping.
  - IP enhancements:
    - Voice routing enhancements:
      • IP Header Compression on PPP (RFCs 2507, 2508, 2509)
      • Interleaving voice traffic between fragmented data packets on multi-link PPP
      • Interleaving voice traffic between fragmented data packets on Frame Relay
      • Bypassing PPP or Frame Relay packet compression and encryption for voice traffic
    - IP loopback address

This support allows users to define IP addresses on a special interface to support TN3270 Gateway, Network Dispatcher, and IPSec requirements.

- IPv6
An inter-domain routing function (BGP4+) is provided for IPv6 that supports IPv6 routing and addressing information and uses TCP6 for transport.

IPv6 traffic is supported over ATM ethernet LAN emulation without encapsulation or tunneling.

- Multiple forwarding paths
  IP routing can use up to four equal-cost static routes to support multiple parallel links to a given address and mask.
- IP route aggregation
- Multicast enhancements:
  - Protocol Independent Multicast-Dense Mode (PIM-DM) for IPv4.
  - Network administrators can now control the flow of IP multicast data into and out of their networks by using inbound and outbound traffic filters.
- Not-so-stubby area (NSSA)
  OSPF supports not-so-stubby area (NSSA) as defined in RFC 1587 and the latest Internet draft is now supported.
- Random Early Detection (RED)
- Differential services policing enhancements
- VRRP enhancements:
  - The hardware MAC address may be used instead of a virtual MAC address to identify a redundant gateway; this can offer a performance improvement.
  - When more than one backup candidate is available, preempt options can be configured.
  - For selecting the master IP router, additional criteria, such as available route or network interface, can be used to support non-IP functions.
- Dial-on-demand alternate interface for WAN reroute
- TN3270 enhancements
  - LU capping
  - LU-pool load balancing
  - Talk 5 disconnect of TN3270 sessions
  - Additional reporting information
  - Support of addresses 1 and 255
- Network Dispatcher enhancements
  - Advertising of network dispatcher cluster addresses by routing protocols
  - A new SSL Advisor
- DLSw SDLC PU1 support
- Ethernet encapsulation support for both ethernet type II (default) and 802.3 simultaneously on the same interface
- DHCP enhancements:
  - Hardfile backup for lease information
  - Multiple IP address support for DHCP interfaces
  - Short lease support
- RADIUS enhancements
  - Radius scalability
  - Login of Last Resort
- L2TP Scalability
- Thin Server enhancement
  Connection to an alternate or back-up master server
Summary of Changes

- Service file retrieval enhancements

Clarifications and corrections

In hard copy and PDF, the technical changes and additions are indicated by a vertical line (|) to the left of the change.

Getting Help

At the command prompts, you can obtain help in the form of a listing of the commands available at that level. To do this, type `?` (the `help` command), and then press Enter. Use `?` to list the commands that are available from the current level. You can usually enter a `?` after a specific command name to list its options.

Exiting a Lower Level Environment

The multiple-level nature of the software places you in secondary, tertiary, and even lower level environments as you configure or operate the 2210. To return to the next higher level, enter the `exit` command. To get to the secondary level, continue entering `exit` until you receive the secondary level prompt (either `Config>` or `+`).

For example, to exit the ASRT protocol configuration process:
```
ASRT config> exit
Config>
```

If you need to get to the primary level (OPCON), enter the intercept character (`Ctrl-P` by default).
Chapter 1. Using APPN

This chapter describes APPN® and includes the following sections:

- "What is APPN?" on page 3
- "What APPN Functions Are Implemented on the Router?" on page 3
- "APPN Network Node Optional Features" on page 5
- "Supported DLCs" on page 20
- "Router Configuration Process" on page 20
- "APPN Configuration Notes" on page 43

What is APPN?

Advanced Peer-to-Peer Networking® (APPN) extends the SNA architecture by enabling Type 2.1 (T2.1) nodes to communicate directly without requiring the services of a SNA host computer.

Peer-to-Peer Communications

T2.1 nodes can activate connections with other T2.1 nodes and establish LU-LU sessions with other nodes. The relationship between a pair of T2.1 nodes is referred to as a peer relationship because either side can initiate communication.

Prior to APPN, a T2.1 node could communicate directly with another T2.1 node, but required the services of a centralized SNA host to locate its partner and any associated resources. All routes between the two nodes were predefined. APPN enhanced the T2.1 node function by:

- Requiring network resources to be defined only at the node where they are located
- Distributing information about these resources throughout the network as needed
- Dynamically generating routes between nodes using current information about the network's topology and the desired class of service

APPN Node Types

The APPN architecture allows four types of nodes in a network:

- APPN network nodes
- APPN end nodes
- Low-entry networking (LEN) end nodes
- PU 2.0 nodes supported by DLUR

The router can be configured as an APPN network node that supports connections with all four node types. The router cannot function as an end node for APPN.

APPN Network Node

An APPN network node provides directory and routing services for all resources (LUs) in its domain. A network node's domain consists of:

- Local resources owned by the node
- A control point (CP), which manages the node's resources
- Resources owned by APPN end nodes and LEN end nodes that use the services of the network node

APPN network nodes also:

- Exchange information about the topology of the network. This information is exchanged each time network nodes establish a connection or when there is a change in the topology of the network (such as when a network node is
Using APPN

deactivated, brought on line, or when a link is congested or fails). When a network node receives a topology update, it broadcasts this information to other active and network nodes with which it has CP-CP sessions.

- Act as intermediate nodes, receiving session data from one adjacent node and passing that data on to the next adjacent node along the route.

As a network node, the router can act as a server to attached APPN end nodes and LEN end nodes and provide functions that include:

**Directory services**

The network node, communicating with other network nodes, can locate a resource in the network on behalf of an APPN end node. The network node also maintains a local directory of APPN and LEN end node resources that it can search on behalf of an attached APPN end node, attached LEN end node, or other network nodes.

**Topology and Routing services**

At the request of an APPN end node, the network node dynamically determines the route from an origin logical unit (LU) to a destination LU in the network. The network node also maintains information on other network nodes and the routes to those nodes. The route is based on the current topology of the network.

**Management services**

The network node can pass alert conditions to a designated focal point to allow centralized problem management. The network node is responsible for processing alert conditions for all the resources in its domain. [Managing a Network Node](#) describes this process.

**APPN End Nodes**

An APPN end node provides limited directory, routing, and management services for logical units (LUs) associated with the node. An APPN end node selects a network node to be its network node server. If the network node agrees to act as the APPN end node’s server, the end node can register its local resources with the network node. This enables the network node server to intercept and pass along search requests for resources located on the APPN end node.

The APPN end node and its network node server communicate by establishing CP-CP sessions. An APPN end node may be connected to a number of network nodes, but only one of these nodes acts as the APPN end node’s server at any one time.

The APPN end node forwards all requests for unknown resources to the network node server. The network node server, in turn, uses its search facilities to locate the requested resource and calculate a route from the APPN end node to the resource.

**LEN Nodes**

A LEN node is a T2.1 node without APPN extensions. A LEN node can establish peer connections with other LEN nodes, APPN end nodes, and APPN network nodes, as long as all of the required destination LUs are registered with the LEN node. A LEN node can also serve as a gateway between an APPN network and a SNA subarea network.

Because a LEN node cannot establish CP-CP sessions with an APPN network node server, it cannot register its resources with the server or request that the server search for a resource and dynamically calculate a route to that resource. A LEN node may indirectly use the directory and routing services of a network node by pre-defining remote LUs (owned by nonadjacent nodes) as being located on an
APPN network node, although the actual location may be anywhere in the network. When the LEN node needs to initiate a session with the remote LU, it sends a session activation request (BIND) for the LU to the network node. In this case, the network node acts as the LEN node’s network node server, locating the requested resource, calculating a route, and forwarding the BIND to its correct destination.

When configuring the router network node, you can specify the names of LUs that are associated with an attached LEN end node. These LU names reside in the router network node’s local directory. If the router network node receives a request to search for one of these LEN end node resources, it will be able to find the LU in its local directory and return a positive response to the node originating the search. To reduce the number of LU names you need to specify for an attached LEN end node, the router supports the use of generic LU names, which allow a wildcard character to represent a portion of an LU name.

**PU 2.0 Nodes**
A PU 2.0 node is a type T2.0 node containing dependent LUs. PU 2.0 nodes are supported by the Dependent LU Requestor (DLUR) function which is implemented by an APPN end node or network node. PU 2.0 nodes require the services of a system services control point, which is made available through the DLUR-enabled APPN node. Note that APPN nodes can contain dependent LUs supported by the DLUR function. However, the router does not contain dependent LUs.

### What APPN Functions Are Implemented on the Router?

The router implements the APPN Release 2 base architecture functions as defined in the Systems Network Architecture APPN Reference. The APPN network node functions implemented by the router are summarized in [Table 1]. Notes on specific functions follow the table. For a description of the APPN management services supported by the router, see “Managing a Network Node” on page 17.

APPN uses LU 6.2 protocols to provide peer connectivity between CP-CP session partners. The router network node implements the LU 6.2 protocols required for CP-CP sessions and those used in sessions between a network node CP and its network management focal point. The router implementation of APPN does not provide an application program interface to support user-written LU 6.2 programs.

**Table 1. Implementation of APPN Network Node Functions**

<table>
<thead>
<tr>
<th>APPN Function</th>
<th>Yes</th>
<th>No</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Session services and supporting functions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple CP-CP sessions</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mode name to class of service (CoS) mapping</td>
<td>X</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Limited resource link stations</td>
<td>X</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>BIND segmentation and reassembly</td>
<td>X</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Session-level security</td>
<td>X</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td><strong>Intermediate session routing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intermediate session routing</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routing of dependent LU sessions</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed and adaptive session-level pacing</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RU segmentation and reassembly</td>
<td>X</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td><strong>Directory services</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast searches</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directed searches</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory caching</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safe storage of directory services cache</td>
<td>X</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1. Implementation of APPN Network Node Functions (continued)

<table>
<thead>
<tr>
<th>APPN Function</th>
<th>Yes</th>
<th>No</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central directory server</td>
<td>X</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Central directory client</td>
<td>X</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Registration of APPN EN LUs with network node server</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition of LEN node LUs on network node server</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of wild cards to define attached LEN node resources</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accept multiple &quot;resource found&quot; conditions</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network node server for DLUR EN - Option set 1116</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Topology and routing services**

<table>
<thead>
<tr>
<th>Topology and routing services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology exchange</td>
</tr>
<tr>
<td>Periodic topology broadcasts</td>
</tr>
<tr>
<td>Topology database maintenance</td>
</tr>
<tr>
<td>Topology awareness of CP-CP sessions</td>
</tr>
<tr>
<td>Randomized route computation</td>
</tr>
<tr>
<td>Cached routing trees</td>
</tr>
<tr>
<td>Safe storage of topology database</td>
</tr>
<tr>
<td>Garbage Collection Enhancements</td>
</tr>
</tbody>
</table>

**Connectivity**

<table>
<thead>
<tr>
<th>Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection network definition</td>
</tr>
<tr>
<td>Multiple transmission groups</td>
</tr>
<tr>
<td>Parallel transmission groups</td>
</tr>
</tbody>
</table>

**Management services**

<table>
<thead>
<tr>
<th>Management services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple domain support (MDS)</td>
</tr>
<tr>
<td>Explicit focal point</td>
</tr>
<tr>
<td>Implicit focal point</td>
</tr>
<tr>
<td>Held alerts</td>
</tr>
<tr>
<td>SSCP-PU sessions with focal points</td>
</tr>
<tr>
<td>SNA/MS problem diagnosis data in alerts</td>
</tr>
</tbody>
</table>

**Notes:**

1. New mode names can be defined on the router using the Command Line interface. These new mode names can be mapped to existing Class of Service (CoS) definition names or to new CoS definitions, which may be defined using the Configuration tool.

2. Limited resource link stations are supported for:
   - connection network links
   - X.25 SVC links
   - PPP links running over ISDN, V.25 bis, or V.34
   - Frame relay links running over ISDN
   - ATM SVCs
   - Token-ring links
   - Ethernet links

3. When the router activates a TG to an adjacent node, it negotiates with that node the maximum message size that can be sent across the TG. If a BIND message is larger than the negotiated message size, the router segments the BIND. Segmentation only occurs if the adjacent node is capable of reassembling the BIND. The router supports BIND reassembly.

4. A session level security feature can be enabled for connections between the router network node and an adjacent node. Both partners in the connection require a matching hexadecimal key that enables each node to verify its partner before the connection is established.
5. When routing session data to an adjacent node, the router segments a request/response unit (RU) if the message unit exceeds the maximum message size that can be sent across the transmission group. If the router receives a segmented RU, the node reassembles it.

6. After successfully locating a resource in the APPN network, the router stores or caches this information in its local directory database for future use. However, the router does not save these cached directory entries to a permanent storage medium, such as a disk, to provide for recovery if the node fails.

7. The router cannot be used as a central directory server for an APPN network. The router is capable of using a central directory server, however, to obtain directory information about the location of a resource in the network.

8. To prevent other network nodes from discarding information about the router from their topology databases, the router creates a topology database update (TDU) about itself and its locally-owned transmission groups every 5 days and broadcasts this TDU to network nodes.

9. An interval timer is associated with every resource entry in the router’s network topology database. If the router does not receive any information about a resource within 15 days, it discards the entry for that resource from the database.

10. If there is more than one least-weight route from an origin LU to a destination LU for a given class of service, the router randomly selects one of these routes for the session. This practice helps distribute the flow of traffic in the network.

11. The router maintains a copy of the network topology database. The database identifies the available routes to other network nodes for a particular class of service. When the router needs to calculate a route to a network node or to an end node adjacent to that network node, it uses information in the topology database to generate a routing tree for that network node. The routing tree identifies the optimal routes to the network node for the class of service required.

   When the router generates a new routing tree, it stores that tree in a cache. When the router receives a service request, it checks this cache first to see if a route has been computed. Use of the cache reduces the number of route calculations required. When the router receives topology information that invalidates a routing tree, it discards the tree. The router recalculates the tree as needed and caches the new tree.

12. The router can be defined as a member of a connection network on Ethernet ports, Token-Ring ports, Frame Relay BAN ports, Enterprise Extender Support for HPR over IP, and ATM ports.

**APPN Network Node Optional Features**

In addition to the base APPN Architecture functions, the router also implements the following option set towers and new functions:

- **087** Garbage Collection Enhancements
- **1002** Adjacent Link Station name
- **1007** Parallel TGs
- **1012** LU name = CP name
- **1016** Extended Border Node
- **1061** Prerequisites for SS Extensions for NNS Support
Using APPN

1063  SS Extensions NNS Support
1067  Dependent LU Requester
1071  Generalized ODAI Usage
1101  Preloaded Directory Cache
1107  Central Resource Registration (of LUs)
1116  Network Node Server support for DLUS-Served LU registration
1119  Report Branch Topology to a Manager
1120  Branch Awareness
1121  Branch Extender
1124  Self-Configuring Branch Extender Backup
1200  Tree Caching and TG Caching
1400  High-Performance Routing (HPR)
1401  Rapid Transport Protocol (RTP)
1402  Control Flows over RTP
1405  HPR Border Node
   Node performance tuning
   Node service traces
   Accounting and node statistics collection

*Note:* When defining parallel TGs if using dynamic TG number assignment, either ALL of the links or NONE of the links must be defined between the two nodes.

**High-Performance Routing**

HPR is an enhancement to APPN architecture that provides better performance over high speed, low error rate links using existing hardware. HPR replaces the normal APPN intermediate session routing (ISR) with a Network Control Layer (NCL) containing a new type of source routing function called automatic network routing (ANR). The complete HPR route is contained in the ANR packet allowing intermediate routing nodes to route the packets with less processing overhead and storage.

HPR also eliminates the error recovery and flow control (session-level pacing) procedures for each link between nodes and moves the error recovery and flow/congestion control procedures to the end-points of an HPR connection. A transport layer using a new error recovery procedure called Rapid Transport Protocol (RTP) is used by the endpoints of the HPR connection. HPR intermediate nodes have no session or RTP connection awareness. This new transport layer features:

- Selective retransmission error recovery procedure
- Segmentation and reassembly
- Adaptive Rate-Based (ARB) flow and congestion control mechanism that meters data onto a route that allows efficient utilization of network resources while minimizing congestion. ARB uses a preventative rather than reactive approach to flow and congestion control.
• Non-disruptive Path Switch (NDPS) function that automatically reroutes traffic around node or link failures without disrupting end user sessions.
• Detection of Forward Explicit Congestion Notification (FECN) bit set, allowing RTP’s adaptive rate-based flow and congestion control algorithm to adjust the data send rate. This algorithm prevents traffic bursts and congestion, maintaining a high level of throughput.

The router implements both ANR routing and Rapid Transport Protocol. Therefore, the router can function both as an intermediate routing HPR node and as an HPR connection endpoint node.

Interoperability
HPR uses APPN network control functions including class of service (CoS)-based least-weight route calculation and transmission priority. HPR interoperates seamlessly with APPN ISR:
• The network automatically adapts to the presence of HPR-capable nodes and HPR-enabled links.
• An APPN network can have any mix of ISR and HPR links, although the greatest benefit of HPR is realized when the network has three or more HPR-enabled nodes with two or more HPR-capable links back-to-back. This allows the middle HPR node to be an HPR intermediate node and use only ANR routing, allowing session data to be routed through the middle node using only NCL.
• A given session route can be made up of a combination of ISR and HPR links.
• HPR uses the same TG and node characteristics for least-weight route calculation as APPN ISR. No special consideration is given to HPR capable nodes or links other than their potentially improved characteristics (such as higher effective capacity if a higher speed link).

Traffic types
APPN ISR uses the QLLC protocol for X.25 direct data link control, the IEEE 802.2 LLC Type 2 protocol for token-ring, Ethernet, PPP, and Frame Relay and SDLC protocol for the SDLC data link control. APPN HPR, which is supported on token-ring, Ethernet, PPP, and Frame Relay, does not use LLC Type 2 protocol, but does use some functions of an APPN link station for XID and inactivity timeout. A single APPN link station is therefore used for ISR or HPR. Different mechanisms are used to distinguish between ISR and HPR traffic depending upon the DLC type:
• For token-ring and Ethernet LAN ports:
  Each protocol that uses a port must have a unique SAP address, with the exception of DLSw (which may use the same SAP address as other protocols because DLSw frames will not be destined for the local MAC address, but rather a DLSw MAC address). A unique SAP address identifies the APPN link station for HPR traffic (Local HPR SAP address parameter). If ISR traffic is destined for a link station, then a different SAP address (Local APPN SAP address parameter) must be used. The ISR traffic uses LLC Type 2 LAN frames. The HPR traffic is handled in similar fashion to LLC Type 1 LAN frames and must have a different SAP address.
  The default SAP address for HPR traffic is X’C8’. If X’C8’ has already been used by another protocol on a port, the default must be overridden.

  Note: There is only one APPN link station even though APPN ISR and HPR traffic use different SAP addresses.
• For Frame Relay ports:
Using APPN

APPN ISR traffic and APPN HPR traffic transferred over a Frame Relay data link connection supports both the RFC 1490/2427 bridged frame format and the RFC 1490/2427 routed frame format.

- **RFC 1490/2427 routed frame format**
  APPN ISR traffic will be transferred over a Frame Relay data link connection using the connection-oriented multiprotocol encapsulation method defined in RFC 1490/2427 using:
  - **NLPID = X'08'** (Q.933 encoding)
  - **L2PID = X'4C80'** (Layer 2 protocol identifier indicating 802.2 LLC)
  - **L3PID = X'7083'** (Layer 3 protocol identifier indicating SNA-APPN/FID2)

APPN HPR traffic transferred over a frame-relay data link connection does not use IEEE 802.2 LLC. It uses a different multiprotocol encapsulation as defined in RFC 1490/2427 using:
  - **NLPID = X'08'** (Q.933 encoding)
  - **L2PID = X'5081'** (Layer 2 protocol identifier for no Layer 2 protocol)
  - **L3PID = X'7085'** (Layer 3 protocol identifier indicating SNA-APPN/HPR)

APPN HPR does not use a SAP for traffic transferred using the RFC 1490/2427 routed frame format because there is no Layer 2 protocol.

- **RFC 1490/2427 Bridged format**
  APPN HPR uses a SAP for traffic transferred using the RFC 1490/2427 bridged frame format.

  - **For PPP ports:**
    APPN ISR traffic uses 802.2 LLC over the PPP connection.
    Since there is no Layer 2 protocol used in HPR's RFC 1490/2427 encapsulation, no SAP is used for HPR traffic.

  - **For ATM ports:**
    APPN ISR traffic is not supported over native ATM ports. However, two types of APPN traffic as defined by RFC 1483 are supported:
    - During link station bring up, XIDs are transported using the following frame format:
      - **NLPID = X'09'**
      - Layer 2 protocol ID = X'4C80' (802.2 LLC header present)
      - Layer 3 protocol ID = X'7083' SNA APPN (FID2) including XID3
    - HPR traffic is transported using the following frame format:
      - **NLPID = X'09'**
      - Layer 2 protocol ID = X'4C80' (802.2 LLC header present)
      - Layer 3 protocol ID = X'7085' SNA APPN/HPR (NLP)

  - **Enterprise Extender Support for HPR over IP**

Refer to Table 2 on page 20 for a list of DLCs that support HPR.

**Note:** HPR is not supported over SDLC, X.25, or DLSw ports.

**Dependent LU Requester (DLUR)**

The DLUR option extends the support of T2.0 or T2.1 devices containing dependent LUs to APPN nodes. The DLUR function on an APPN network node or an APPN end node works in conjunction with a dependent LU server (DLUS) in a mixed APPN/subarea network. The DLUS function may reside in some other part of the mixed network from the DLUR.
The dependent LU flows (SSCP-PU and SSCP-LU) are encapsulated over an LU 6.2 (CP-SVR) pipe established between the DLUR APPN node and the DLUS SSCP. The CP-SVR pipe is made up of a pair of LU 6.2 sessions using a new CPSVRMGR mode between the DLUR and the DLUS. This pipe brings the SSCP function (in the DLUS) to the DLUR APPN node where it can be made available to attached T2.0/T2.1 nodes containing dependent LUs.

The dependent LU will appear to be located within the domain of the serving SSCP. Session initiation flows will be emulated from the DLUS, but session bind and data paths will be calculated directly between the dependent LU and its session partner. This path may or may not traverse the serving DLUS node.

Set the adjacent node type parameter to PU 2.0 Node when defining a link station to a T2.0 adjacent node containing dependent LUs. Set the adjacent node type parameter to APPN end node or LEN end node when defining a link station to a T2.1 adjacent node containing dependent LUs.

See Table 2 on page 20 for the types of ports providing connection to the downstream PU (DSPU) that are supported.

Functions Supported
The APPN DLUR option includes the following functions:

- Support for SDLC-attached downstream T2.0 nodes containing dependent LUs that do not support XID exchange.
- Support for downstream T2.0 nodes containing dependent LUs that respond with XID type 0 and XID type 1.
- Support for downstream T2.1 nodes containing dependent LUs that respond with XID type 3.
- Support for dependent LUs that is equivalent to the support provided by the Subarea environment for:
  - Activating PUs and their LUs
  - Locate and be located by other LUs in an APPN or subarea network
  - Determine LU’s characteristics
  - Allow terminal operators to logon to applications both in APPN and subarea networks
  - SSCP takeover
  - Uninterrupted LU-LU sessions, if the supporting DLUS (SSCP) fails
  - SLU init, PLU init, and Third-party init

Restrictions
The DLUR option, as implemented on the router network node, has the following functional restrictions:

- Only secondary LUs (SLUs) can be supported by the DLUR function. An LU supported by DLUR cannot function as a primary LU (PLU). Therefore, the downstream physical unit (DSPU) should be configured as secondary.
- Because only SLUs are supported, Network Routing Facility (NRF) and Network Terminal Option (NTO) are not supported.
- Extended recovery facility (XRF) and XRF/CRYPTO are not supported.
- You must be able to establish an APPN-only or APPN/HPR-only session between DLUS and DLUR. The CPSVRMGR session cannot pass through a subarea network.
VTAM Considerations for DLUR
The following are example VTAM® Switched Major Node definitions for DLUR. You should note that PATH statements are necessary only if VTAM is initiating the connection to the DSPU.

You should refer to *IBM VTAM Resource Definition Reference* for details of the DLC parameter statements for the Switched Major Node definitions.

```
DABDLURX VBUILD TYPE=SWNET,MAXGRP=400,MAXNO=400,MAXDLUR=20
************************************************************************
|IN THE DLCADDR, THE 'SUBFIELD_ID' = CV SUBFIELD OF THE CV91 |
|MINUS 0X90.                                                  |
|FOR EXAMPLE, THE CV94 SUBFIELD IS CODED ON DLCADDR=(4,X,...|
************************************************************************
************************************************************************

Following are PU Statements for 2.0 and for 2.1
************************************************************************

* 2.0 PU STATEMENT
************************************************************************

+PU20RT PU ADDR=05,PUTYPE=2,MAXPATH=8,ANS=CONT,USSTAB=AUSSTAB,
+ISTATUS=ACTIVE,MAXDATA=521,IRETRY=YES,MAXOUT=7,
+PASSLIM=5,IDBLK=017,IDNUM=00035,MODETAB=AMODETAB
+LOGAPPL=ECHO71,DLOGMOD=M23278I
************************************************************************

* Path statements are not required if the DSPU is initiating the connection to VTAM
************************************************************************

+PU20LU1 LU LOCADDR=2
+PU20LU2 LU LOCADDR=3
+PU20LU3 LU LOCADDR=4
************************************************************************

* 2.1 PU STATEMENT
************************************************************************

+PU21RT PU ADDR=06,PUTYPE=2,CPNAME=PU21RT,ANS=CONT,MAXPATH=8,
+ISTATUS=ACTIVE,USSTAB=AUSSTAB,MODETAB=AMODETAB
+LOGAPPL=ECHO71,DLOGMOD=M23278I
************************************************************************

* Following are examples of path statement coding for various DLC types.
* There is no difference in the path statement definitions between a PU 2.0 and a PU 2.1
* Path statements are required if VTAM is initiating the connection to the DSPU.
*
************************************************************************

* Below is SDLC
************************************************************************

+A20RT PATH PID=1,
+DLURNAME=GREEN,
+DLCADDR=(1,C,SOLCN),
+DLCADDR=(2,X,5353), 2 **port name
+DLCADDR=(3,X,C1) 3 **station address
************************************************************************

* Below is Frame Relay
************************************************************************

+A20RT PATH PID=2,
+DLURNAME=GREEN,
+DLCADDR=(1,C,FRPVC),
+DLCADDR=(2,X,4652303033), 2 **port name
+DLCADDR=(3,X,04), 3 **SAP address
+DLCADDR=(4,X,0024) 4 **DLCI
************************************************************************

* Below is Frame Relay BAN
************************************************************************

+A20RT PATH PID=3,
+DLURNAME=GREEN,
+DLCADDR=(1,C,FRPVC),
+DLCADDR=(2,X,4652303033),
+DLCADDR=(3,X,04), 3 **SAP address
+DLCADDR=(4,X,0024), 4 **DLCI
+DLCADDR=(8,X,400006000001) 5 **MAC addr
************************************************************************

Using APPN
**Below is DLSw**

* A20RT PATH PID=3,
  * DLURNAME=GOLD,
  * DLCADDR=(1,C,TR),  
  * DLCADDR=(2,X,44C53323534),  
  * DLCADDR=(3,X,04),  
  * DLCADDR=(4,X,400060006001)  

**Below is Token Ring**

* PATH20 PATH PID=1,
  * DLURNAME=RED,
  * DLCADDR=(1,C,TR),  
  * DLCADDR=(2,X,5452303030),  
  * DLCADDR=(3,X,04),  
  * DLCADDR=(4,X,400060011088)  

**Below is Ethernet**

* PATH20 PATH PID=1,
  * DLURNAME=RED,
  * DLCADDR=(1,C,ETHERNET),  
  * DLCADDR=(2,X,454E303030),  
  * DLCADDR=(3,X,20),  
  * DLCADDR=(4,X,400060011063)  

**Below is X25 SVC**

* A20RT PATH PID=3,
  * DLURNAME=GREEN,
  * DLCADDR=(1,C,X25SVC),  
  * DLCADDR=(2,X,583235303033),  
  * DLCADDR=(3,X,C3),  
  * DLCADDR=(21,X,000566666)  

**Below is X25 PVC**

* A20RT PATH PID=3,
  * DLURNAME=GREEN,
  * DLCADDR=(1,C,X25PVC),  
  * DLCADDR=(2,X,583235303033),  
  * DLCADDR=(3,X,0001)  

**LU statements**

* PU21LU1 LU LOCADDR=2  
* PU21LU2 LU LOCADDR=3  
* PU21LU3 LU LOCADDR=4  

**Notes:**

1. The difference between PU statement coding is:
   - For 2.0 definitions, the PU statement has IDBLK=...,IDNUM=....
   - For 2.1 definitions, the PU statement has CPNAME=....
2. Port name in ASCII defined on the router and used by DSPU
3. SAP of DSPU (noncanonical, except for Ethernet)
3a. Station address for SDLC
4. DLCI must have 4 digits because it is a half-word
5. MAC address of the DSPU (noncanonical) for Frame Relay BAN
6. MAC address of the DSPU (noncanonical, except for Ethernet MAC address, which is canonical)
7. DLSw appears to VTAM like a token ring DLC
8. Protocol identifier
9. Destination DTE address (000566666, where: 00 is fixed
Using APPN

05 is the length of the DTE address
66666 is the DTE address

10 Logical channel number. It must have 4 digits because it is a halfword.

11 LU coding

See [Chapter 2. Using TN3270” on page 71] for an example of an internal PU path statement.

APPN Connection Networks

When nodes are attached to a shared-access transport facility (SATF), any-to-any connectivity is possible. This any-to-any connectivity allows direct connections between any two nodes, eliminating routing through intermediate network nodes and the corresponding data traversing the SATF multiple times. To achieve this direct connectivity, however, TGs must be defined on each node for all the other possible partners.

Defining connections between all possible pairs of nodes attached to the SATF results in a large number of definitions (increasing on the order of the square of the number of nodes involved) and also a large number of topology database updates (TDUs) flowing in the APPN network. To alleviate these problems, APPN allows nodes to become members of a connection network to represent their attachment to an SATF. Session traffic between two nodes that have been defined as members of a connection network can be routed directly, without passing through a network node (achieves direct connectivity). To become a member of a connection network, an APPN node’s port must be “attached” to a Connection Network by defining a connection network interface. When the port is defined, a Connection Network TG is created by the APPN component to identify the direct connection from the port to the SATF (i.e. the connection network). This TG is not a conventional TG as in the case of defined link stations, but rather represents the connection to the Connection Network in the topology database.

**Note:** TGs for end nodes are not contained in the network topology database, but are contained in the node’s local topology database. TDUs do not flow through the network when a connection is established through a Connection Network or when an end node is made a member of a Connection Network.

Because the connectivity is represented by a TG from a given node to a Connection Network, normal topology and routing services (TRS) can be used for the network node server to calculate the direct path between any two nodes attached to the SATF (with TGs to the same Connection Network). DLC signaling information is returned from the destination node during the normal locate process to enable the origin node to establish a connection directly to the destination node.

Therefore, to achieve direct connectivity on an SATF, instead of each node on the SATF being defined (or connected) to each other, each node is connected to a Connection Network. The Connection Network is often visualized as a virtual node on the SATF to which all other nodes are attached. This model is frequently used and, in fact, the term Virtual Routing Node (VRN) is often interchanged with the term Connection Network.

When a connection network is defined, it is named. This name then becomes the CP name of the VRN and must follow all the requirements of any CP name. See [Table 24 on page 166] for a list of these requirements.
Restrictions

- The same connection network (VRN) can be defined on only one LAN. The same VRN can be defined on multiple ports having the same characteristics to the same LAN however.
- There is only one connection network TG from a given port to a given connection network’s VRN.
- Because the VRN is not a real node, CP-CP sessions cannot be established with or through a VRN.
- When a connection network is defined on the router network node, a fully qualified name is specified for the connection network name parameter. Only connection networks with the same network ID as the router network node may be defined. The network ID of the VRN is then the same as the network ID of the router network node.

Branch Extender

The Branch Extender (BrNN) function is designed to optimize the connection of a branch office to an APPN WAN backbone network. The BrNN isolates all the end nodes on one or more branch office LANs from the backbone WAN. The domain of a BrNN may contain only end nodes and cascaded BrNNs. The domain of a BrNN does not contain network nodes or nodes with DLUR.

When configuring a BrNN, configure link stations to the backbone to be uplinks. This causes the BrNN to appear as a conventional end node to the backbone. From the perspective of the backbone, all resources in the domain of the BrNN appear to be owned by the BrNN, hiding the topology of the BrNN’s domain from the backbone and reducing the number of broadcast locates in the backbone.

A BrNN presents a conventional network node interface over downlinks. End nodes in the domain of the BrNN register their resources with the BrNN and use the BrNN as a conventional network node server.

A BrNN accomplishes:
- Reduction of the number of network nodes in a large APPN network.
- Hidden branch office topology from the WAN and hidden WAN topology from the BrNN.
- Direct, peer-to-peer communication between defined branches connected to the same connection network.
- Reduces CP-CP session traffic on the WAN link.

The following are limitations of Branch Extender:
- Network nodes are allowed to connect only over links that a BrNN defines as uplinks.
- Only end nodes or cascaded BrNNs may be attached to a BrNN downlink. Border nodes acting as end nodes and DLUR nodes may not be attached to a BrNN downlink.
- A node cannot connect to a Branch Extender over an uplink and a downlink at the same time.
- A BrNN can have CP-CP sessions with only one network node at a time.

It is possible to configure two or more peer BrNNs in a single branch, each serving a set of ENs in the branch. When one of these BrNNs loses connectivity to its preferred network node server, it is desirable for one of the other BrNNs to take over serving the first BrNN’s ENs.
Using APPN

You can configure peer BrNNs to automatically back each other up in this situation by shifting from a peer to a cascaded BrNN configuration.

Extended Border Nodes

Extended Border Nodes (BNs) allow networks with different network IDs to connect to one another. CP-CP sessions will be established across the network boundaries, and directory services flows and session establishment will be allowed to span the interconnected networks. Topology information will not be exchanged across the network boundary. This allows networks with different network IDs to establish CP-CP sessions and provides topology isolation between different networks.

In addition to allowing networks with different network IDs to interconnect, BNs provide a mechanism to subdivide networks with the same network ID into smaller “topology subnetworks”. This subdivision provides topology isolation between the two subnetworks while allowing directory services flows and sessions to span the subnetwork boundaries.

There must be a BN on one side of the subnetwork boundary in order to use this function. When a BN connects to a non-native NN, the BN looks like an EN to the non-native NN, even though the BN is actually a NN.

There may be two BNs, one on each side of the boundary, cooperating to perform this function. When two BNs connect across a subnetwork boundary, the BN will look like a NN to the non-native BN.

A BN will appear to be the NN server for all non-native resources accessible through the BN. This allows the existing APPN directory caching and route calculation functions to work, while enabling the BN to intercept and modify all Locate and BIND flows which cross an inter-subnetwork TG (ISTG).

BNs implement piece-wise optimal session route calculation. Each subnetwork calculates its own part of the session’s route selection control vector (RSCV) to the entry point in the next non-native subnetwork. While the RSCV will be optimal through the native subnetwork, there is no guarantee that the end-to-end session path will be optimal.

Network Topology Example

Figure 1 on page 13 shows many of the connectivity options provided by the BN function. In general, you can get from any network to any other network except that NetF can only reach network NetE and NetE is the only network that can reach NetF.
Note: Solid lines represent intersubnetwork TGs.

In this figure:

- Netid subnetwork NetA has been divided into topology subnetworks. The left-most topology subnetwork contains BNa1 which is connected across an intersubnetwork TG to BNa2 in the right topology subnetwork. The netid of both BNa1 and BNa2 is NetA.
- BNa1 is non-native to all the other extended border nodes, including NetA2.
- BNa2, BNa3 and BNa4 are all native to the right topology subnetwork of NetA, and non-native to the other networks, including the subnetwork containing BNa1.
- A BN can interconnect multiple networks as BNa4 connects topology subnetwork of NetA to both NetB and NetD.
- Multiple links can connect two networks as the right topology subnetwork of NetA and NetB are connected by both BNa3/BNb1 and BNa4/BNb2.
- Both ends of an inter-network link must be BNs, unless one of the networks is a peripheral network. In this case, the peripheral network may use a conventional non-BN network node to connect to the BN in the adjoining network. This is shown where peripheral network NetC connects to NetB with NNc.
- Any LU in networks NetA, NetB, NetC, NetD, or NetE can get to any other LU in any of those networks. Both NetC and NetE are connected using conventional non-BN network nodes.
Using APPN

- Network NetE is connected using conventional non-BN network node NNe to BNs in NetA2 and NetF. You can not have a network node interconnecting non-peripheral networks, so it is not possible to get from NetF to any network other than NetE.
- You can get from NetA2 to NetE and from NetE to NetA2 since NNe is in a peripheral network. Similarly, you can get from NetF to NetE and from NetE to NetF.

**Session Services Extensions (SSE) for NNS Support**
The SSE function of a router is enabled when the router is enabled for APPN. This is true even if the Extended Border Node function is not enabled. This means that the router may act as the network node server for a VTAM end node. As such, it can handle NNS functions for end nodes requesting SLU-initiated sessions, third part initiated sessions, session request queuing, automatic login, session-release requests, and EN TG vector registration.

The SSE function is not used when the router is acting as a Branch Extender since downstream VTAMs are not allowed in that configuration.

**Network Requirements**
There are no requirements for other APPN nodes in a network as long as they are not directly connected to a BN across a topology boundary. APPN nodes that are connected to a BN across a topology boundary (across an ISTG) must meet one of these requirements:
- APPN Ver1 with option set 1013, Interoperability with peripheral extended border node
- APPN Ver2, where option set 1013 is part of the base software.

Nodes attached using ISTGs that do not meet either of these requirements will generate alerts and do not handle some of the new flows associated with BNs. However, if other paths through the network are available, you may still have end-to-end connectivity.

**Branch Extender vs. Extended Border Node**
Both Branch Extender and Extended Border Nodes serve to minimize network topology. The choice of which to use depends upon the network.

A branch extender is the appropriate choice when you have a single network with one or more groups of end nodes where each group of end nodes typically needs to communicate with other end nodes in that group, and only occasionally need to interact with the backbone network.

None of the devices downstream from the branch extender may be network nodes, DLUR, VTAM, or VTAM end nodes.

With the branch extender in place the backbone network’s view of the branch extender is as a giant end node with all the downstream LUs being owned by this giant end node. The backbone has no knowledge of the topology downstream from the branch extender, thus reducing the overhead of topology exchanges. Conversely, the branch extender’s network node server, which is part of the backbone, will have knowledge of all the LUs owned by the branch extender if the branch extender is configured to register resources. This serves to reduce the number and size of broadcast searches and topology updates.
An **extended border node** is the appropriate choice when you have multiple networks you want to tie together, or when you have a large network you want to subdivide without restriction on what node types are allowed in the subdivided pieces. There is no concept of upstream or downstream and you can have additional extended border nodes, network nodes, end nodes, DLUR, VTAM, or VTAM end nodes located anywhere in your network. Unlike the branch extender, an extended border node cannot register resources with another network.

**Managing a Network Node**

The router network node can act as an APPN entry point that forwards APPN-related alerts to an APPN focal point. APPN focal points may be defined explicitly or implicitly.

You can use SNMP to access these IETF standardized MIBs:
- APPC (RFC 2051)
- APPN (RFC 2155)
- HPR (RFC 2238)
- DLUR (RFC 2232)
- Extended Border Node
- TN3270 Base
- TN3270 Response Time

You can also use SNMP to access these enterprise-specific MIBs:
- IBM APPN Memory
- IBM Accounting
- IBM HPR NCL
- IBM HPR Route Test
- IBM Branch Extender Node
- IBM TN3270 Connection Rejection

**Entry Point Capabilities for APPN-related Alerts**

The router network node can serve as an APPN entry point for alerts related to the APPN protocol. As an entry point, the router is responsible for forwarding APPN and LU 6.2 generic alerts about itself and the resources in its domain to a focal point for centralized processing. A focal point is an entry point that provides centralized management and control for other entry points for one or more network management categories.

**Note:** If a focal point is not available to receive an alert from the device, the alert is held (stored) by the device.

Entry points that communicate with a focal point make up that focal point’s *sphere of control*. If a focal point explicitly defines the entry points in its sphere of control and initiates communication with those entry points, it is an *explicit focal point*. If a focal point is designated by its entry points, which initiate communication with the focal point, the focal point is an *implicit focal point*. The focal point for the router can be either an explicit or implicit focal point.

Routers configured as branch extender nodes have additional flexibility. As with conventional network nodes, the focal point can directly establish an explicit relationship with the branch extender node. Also as with conventional network nodes, you can configure one or more implicit focal points at the branch extender node.
Unlike conventional network nodes, branch extender nodes can alternatively learn of the focal point from its network node server. When the network node server establishes a relationship with the focal point, either explicitly or implicitly, it will notify all its served end nodes, including served branch extender nodes, of the focal point name.

If the session between the router entry point and its primary focal point fails, the router can initiate a session with a designated backup focal point. Before initiating a session with a backup focal point, the router entry point makes an attempt to reestablish communication with its primary focal point if the router has been assigned session re-establishment responsibility. If that attempt fails, the router switches to the backup focal point.

**Note:** The router will attempt to establish a session with the backup focal point, or will attempt to re-establish the session with the primary focal point, only if the router has an alert to send.

After switching to a backup focal point, the router will periodically attempt to re-establish its session with the primary focal point. The interval between attempts is doubled each time an attempt fails until a maximum interval of one day is reached. From that point on, the attempt is performed daily.

**Notes:**
1. If the focal point is explicit and the explicit focal point retains the re-establishment responsibility for itself, this retry mechanism is disabled.
2. If the focal point is explicit and assigns re-establishment responsibility to the router, the router will attempt to reestablish communication until the next restart of APPN in the router.

The router entry point communicates with the focal point through an LU 6.2 session. Multiple-domain support (MDS) is the mechanism that controls the transport of management services requests and data between these nodes. The router network node does *not* support SSCP-PU sessions with focal points.

Management processes within the router’s control point are handled by its control point management services (CPMS) component. The CPMS component within the router network node collects unsolicited problem management data from resources within the router’s domain and forwards this data to the appropriate focal point.

**Supported Message Units**
The router network node uses the following message units for sending and receiving management services data, including alert messages from domain ENs:

<table>
<thead>
<tr>
<th>Message unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-MSU</td>
<td>Control point management services unit. This message unit is generated by CPMS and contains alert information forwarded by the router entry point. CPMS passes CP-MSU message units to MDS.</td>
</tr>
<tr>
<td>MDS-MU</td>
<td>Multiple-domain support message unit. This message unit is generated by MDS. It encapsulates the CP-MSU for transport between nodes.</td>
</tr>
</tbody>
</table>
SNMP Capabilities for APPN MIBs

An operator or application at an SNMP network management station can query objects in the APPN MIBs (using the SNMP `get` and `get_next` commands) to retrieve APPN status information and node statistics. A subset of APPN MIB objects can be modified using the SNMP `set` command. The APPN MIBs can be accessed only using SNMP.

Topology Database Garbage Collection

Information flows between APPN NNs to inform the NNs about network resources. Each NN keeps a topology database consisting of the names and characteristics of those resources. When a resource is eliminated from the network, it can also be deleted from each NN topology database. When a NN detects that a resource in its topology database is obsolete, the node will broadcast information stating that the resource should be garbage-collected. If NNs receiving this information support Enhanced Garbage Collection, they should delete that resource from their topology database. The record is not actually garbage-collected until the next garbage collection cycle. A NN examines each resource in its topology database once a day.

Configurable Held Alert Queue

The configurable held alert queue function allows you to configure the size of the held alert queue. If a focal point is not available, the held alert queue saves APPN alerts. When a focal point becomes available, the held alerts are sent. If more alerts arrive than can be held, the oldest alerts are discarded.

**Note:** If you configure a large value for the Held Alert Queue Size, the extra memory should be accounted for. You can do this by letting the tuning algorithm automatically calculate the Maximum Shared Memory value. See [APPN Node Tuning](#) for additional information about the node tuning algorithm.

Implicit Focal Point

A focal point is a node with centralized management responsibility. The managing node can contact the managed node (router) and establish a management session. The managing node is then an explicit focal point. When the name of the managing node is configured at the router and the router can initiate a management session, the managing node is an implicit focal point. You can configure a single, primary implicit focal point with up to eight backup implicit focal points, where each focal point is a fully qualified network name. The router will attempt to contact each focal point in order until a successful management session is established.

If the management session is with a backup implicit focal point, the device will periodically attempt to reestablish its session with the primary implicit focal point. The interval between attempts is doubled each time an attempt fails until a maximum interval of one day is reached. From that point on, the attempt is performed daily.

**Note:** If an explicit focal point initiates a management session with a device, it will cause a session with an implicit focal point to terminate.
**Enterprise Extender Support for HPR over IP**

Enterprise Extender support for HPR over IP allows HPR/APPN applications to run over an IP backbone network and still take advantage of APPN Class of Service. HPR over IP encapsulates HPR data into a UDP/IP packet for delivery over the IP network.

**Supported DLCs**

Table 2 shows the DLC ports supported by the device over APPN:

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Standard</th>
<th>HPR</th>
<th>ISR</th>
<th>DLUR¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Version 2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Ethernet IEEE 802.3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>TR 802.5</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Serial PPP</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Serial FR (bridged and routed)²</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Frame Relay BAN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Serial LAN bridging</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>SDLC</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>X.25 CCITT X.25</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DLSw</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>APPN/PPP/ISDN</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>APPN/FR/ISDN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>APPN/PPP/V.25 bis</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>APPN/PPP/V.34</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>LANE Forum compliant</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>HPR over IP</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>100Mbps Ethernet</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>100Mbps TR 802.5</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Router Configuration Process**

This section describes the router configuration process and includes details about parameters.

**Configuration Changes That Require the APPN Function to Restart**

- Network ID of the network node
- Control point name of the network node
- XID number (of network node) for subarea connection
- Adjacent node type (of link station)
- Change of node function (EBN, BN, NN)

---

1. This column refers to the port providing the connection to the downstream PU (DSPU).
2. Use bridged format when you have two devices connected by Frame Relay and one of them does not have APPN. Otherwise, use routed format because of improved performance.
Any parameters under the following options:
- High-Performance Routing (HPR) at the node level
- Dependent LU Requester (DLUR) at the node level
- Connection network
- Class of service
- Node tuning
- Node management
- Focal points
- Mode name mappings
- Delete TN3270E parameters
- Routing lists
- CoS mapping tables

See “APPN Dynamic Reconfiguration Support” on page 275 for details on dynamic changes you can make to your APPN configuration.

Configuration Requirements for APPN
APPN routing is configured on the individual adapters supporting the DLC desired. To use APPN routing, at least one of the following DLCs must be configured and enabled:

- LAN ports:
  - Token-ring
  - Ethernet
- Serial ports configured with:
  - PPP
  - Frame relay
  - X.25
  - SDLC
  - Dial circuits over ISDN
  - Dial circuits over V.25 bis
  - Dial circuits over V.34
- DLSw
- ATM
- HPR over IP

Configuring the Router as an APPN Network Node
You can configure the router as an APPN network node in one of three ways, depending on the level of connectivity you desire with other nodes.

- Minimum configuration
- Initiate connections configuration
- Controlling connections configuration

Minimum Configuration
This group of APPN configuration steps:

- Allows the network node to accept any request it receives from another node to establish a connection.
- Restricts the network node from initiating connections with other nodes.

If you choose the minimum configuration steps, adjacent nodes must define connections to the router network node to ensure connectivity. Because APPN nodes can initiate CP-CP sessions with the router network node, these nodes do not need to be defined in the router’s configuration. In general, when configuring APPN on the router, you can simplify the task considerably by allowing the router network node to accept connection requests from any node. Configuring the
Using APPN

network node in this manner eliminates the need to define information about adjacent nodes, except in the following cases:

- The adjacent node is a LEN end node. LEN end nodes do not support CP-CP sessions, so information about such nodes and their LU resources must be configured on the router network node.
- You want the router network node to be able to initiate a CP-CP session with an adjacent APPN node.

In these cases, you must specify information about the adjacent node when enabling APPN routing on the specific port you are using to connect to the adjacent node, and should follow the configuration steps described in [Initiate Connections Configuration].

Use the following procedure for minimum configuration steps:

1. If you are configuring APPN using a DLSw port:
   a. Enable bridging on the node
   b. Enable DLSw on the node
   c. Define the DLSw port with a locally administered MAC address for DLSw.
2. Enable APPN routing on the port.
   
   Note: Because Service Any is enabled by default, the node accepts any request for a connection that it receives from another node.
3. Enable the APPN Network Node.
4. Configure the following parameters:
   - Network ID
   - Control point name
5. Define the XID number for subarea connections parameter for the APPN network node (optional).
6. Accept all other defaults.
7. Optionally do the following:
   - Modify High-Performance Routing parameters
   - Configure Dependent LU Requester
   - Define connection networks
   - Define new CoS names or mode name mappings
   - Tune the performance of this node
   - Perform node service trace diagnostics
   - Collect statistics for this network node

Notes:

1. APPN routing must be defined and enabled on the specific ports you configure the router network node to use.
2. Bridging and DLSw must still be enabled on the specific adapter ports you desire the device network node to use.

Initiate Connections Configuration

This group of APPN configuration steps:

- Allows the network node to accept any request it receives from another node to establish a connection.
- Enables the network node to initiate connections with other nodes that you specify, including LEN end nodes.
Because APPN nodes can initiate CP-CP sessions with the router network node, these nodes do not need to be defined in the router’s configuration, except in the following cases:

- The adjacent node is a LEN end node. LEN end nodes do not support CP-CP sessions, so information about such nodes and their LU resources must be configured on the router network node.
- You want the router network node to be able to initiate a CP-CP session with an adjacent APPN node.

If neither of these cases apply to your configuration, you should follow the configuration steps described in “Minimum Configuration” on page 21.

Use the following procedure for initiate connections configuration:

1. If you are configuring APPN using a DLSw port:
   a. Enable bridging on the node
   b. Enable DLSw on the node
   c. Define the DLSw port with a locally administered MAC address for DLSw.

2. Select the ports over which to initiate connections to adjacent nodes. The following are the DLC port types supported by APPN:
   - Token-ring LAN port
   - Ethernet LAN port
   - Frame-relay serial port
   - PPP serial port
   - X.25
   - SDLC
   - DLSw
   - IP port

3. Enable APPN routing on APPN ports with the `enable APPN routing on this port` parameter.

   **Note:** Because Service Any is enabled by default, the node accepts any request for a connection that it receives from another node.

4. Define APPN link stations on the selected DLC ports for the adjacent nodes to which this network node may initiate a connection.

   **Note:** Link stations do not have to be defined on every port, only those over which you want to initiate connections to adjacent nodes.

5. Enable the APPN network node.

6. Configure the following parameters for the APPN network node:
   a. Network ID
   b. Control point name

7. Define the XID number for subarea connections parameter for the APPN network node (optional).

8. Accept all other defaults

9. Optionally do the following:
   - Modify High-Performance Routing parameters
   - Configure Dependent LU Requester
   - Define connection networks
   - Define new CoS names or mode name mappings
   - Tune the performance of this node
   - Perform node service trace diagnostics
   - Collect statistics for this network node
Controlling Connections Configuration

This group of APPN configuration steps:
- Allows the network node to accept requests only from nodes that you specify.
- Enables the network node to initiate connections with other nodes that you specify, including LEN end nodes.

This configuration provides a higher level of security because you explicitly define which APPN nodes may communicate with this router network node. A connection request from an adjacent node will be accepted only if its fully qualified CP name parameter has been configured on this network node. This group of configuration steps optionally enables you to have a secure link with each adjacent node by configuring the session level security feature for each link.

Use the following procedure for the controlling connections configuration:

1. Select ports over which you desire to establish connections to adjacent nodes from the following DLC port types supported by APPN:
   - Token-ring LAN port
   - Ethernet LAN port
   - Frame-relay serial port
   - PPP serial port
   - X.25
   - DLSw
   - SDLC
   - IP port

2. Define ports selected as direct APPN ports with the following parameters:
   - Enable APPN routing on this port
   - Disable the Service any port parameter

3. If you are configuring APPN using a DLSw port:
   - Enable bridging on the node
   - Enable DLSw on the node.
   - Define the DLSw ports with the following parameter:
     - Define a locally administered MAC address for DLSw
     - Disable the Service any node parameter

4. Enable APPN routing on the port.

5. Define APPN link stations on the selected DLC ports for the adjacent nodes:
   - that may initiate a connection to this network node.
   - which you desire this router network node to initiate a connection.

Specify the following link station parameters:
- Fully Qualified CP name of adjacent node (required)
- Any required addressing parameters for adjacent node
- And optionally:
  - CP-CP Session Level Security
  - Security Encryption Key

6. Enable the APPN network node.

7. Configure the following parameters for the APPN network node:
   - Network ID
   - Control point name

8. Define the XID number for subarea connections parameter for the APPN network node (optional):

9. Accept all other defaults.

10. (Optional) Configure the following router network node options:
    - Modify High-Performance Routing parameters
    - Configure Dependent LU Requester
• Define connection networks
• Define new CoS names or mode name mappings
• Tune the performance of this node
• Perform node service trace diagnostics
• Collect statistics for this network node

Configuring Branch Extender
To configure Branch Extender, set the following configuration parameters as appropriate for your network.
1. Use the set node command to:
   a. Answer 1 for Branch Extender to the Enable Branch Extender or Border Node question. If you answer 0, none of the following Branch Extender questions will appear.
   b. Answer Full, Partial, or None to the Enable Branch Awareness Support question, depending on whether you want to limit the flow of topology information about the TGs between NNs and BrNNs.
   c. Answer yes or no to the Permit search for unregistered LUs question depending on whether or not you want to allow searches from the backbone for LUs that were not registered with the network node server.
   d. Your answer to the Branch uplink question will determine the default for the analogous link level question.
2. Use the add link command to:
   a. Answer yes to the Branch uplink question if you want the router to appear as an end node on this link. An end node is for links to network nodes in the backbone. Note that this question doesn't appear and is forced to yes if you have defined the adjacent link station to be a network node on one of the earlier configuration prompts. Answer no if you want the router to appear as a network node on this link. A network node is for links to end nodes
   b. The Is uplink to another Branch Extender node question is asked only if this link has been defined as a limited resource and has also been defined as a Branch Extender uplink. Answer yes if the adjacent node is another Branch Extender.
   c. The Preferred network node server question is asked only if the adjacent node is a network node and CP-CP sessions are supported on this link. Since you can only have a single preferred network node server you won't be prompted for this question once it has been set to yes on any link.

Configuring Extended Border Nodes
To configure extended border node you must configure one or more of these parameters:
• Set node
• Add port
• Add link
• Add routing_list
• Add cos_mapping_table

Set node
The previously existing prompt used to enable branch extender has been expanded to allow you to choose the branch extender function, the extended border node function, or neither. Only if you enable the extended border node function will any of the other extended border node prompts appear.
Subnetwork visit count is the first prompt. This parameter defines the maximum number of topology subnetworks a session may span. The value defined here is used as the default value for the extended border node. You can specify different values for the subnetwork visit count when adding ports, links, or routing lists.

Cache search time is the next node level prompt. This specifies the number of minutes the extended border node will retain information on multi-subnetwork searches. The intention is for this to be the primary mechanism for limiting the size of this cache. However, the next parameter can also be used to control the size of this cache.

Maximum search cache size is next. This controls the same data structure controlled by the previous parameter. If set to zero, the maximum size is unlimited. Entries will be discarded only after the search cache time has expired. If you prefer to have a fixed maximum size for the search cache then specify that here. If this maximum is reached before any entries exceed the time limit the least recently entries are discarded.

List dynamics is the next prompt, and it allows you to control how the extended border node determines possible next hops when attempting to locate resources (LUs). The temporary list of possible next hop CPs is built dynamically by the operational code whenever the border node is attempting to locate a resource. This parameter specifies sources of next hop CP names the extended border node may use to build this temporary dynamic list of CP names.

After the temporary list is built, it is always ordered so that configured next-hop CPs are first followed by CPs associated with similarly named known resources. Additional reordering may be performed. Once all the reordering is complete, the extended border node starts searching for the target resource one CP after another.

Note that once the extended border node actually locates a resource it will remember the next hop CP and always use that next hop CP for that particular resource, ignoring the routing lists. Entries from this table of located resources can be quite long lived. They are discarded if the table reaches its maximum size, a later search to that CP fails to locate the resource, or if search from that LU comes from a different CP.

The list dynamics parameter is set to one of the following values. It is possible to respecify this value for individual routing lists when, and if, you configure individual routing lists.

**None**

The LU name of the destination resource is compared to the LU names configured in the routing lists. The routing list with the best LU name match is selected, and the next hop CP names from that configured list are placed in the dynamically built list. This is the only source of possible next hop CP names when list dynamics is set to none.

Note that if an LU name does not appear in a routing list the LU will not be reachable by the extended border node when this list dynamics parameter is set to none.

**Limited**

This augments the list of next hop CP names obtained from the best match configured routing list with CP names obtained from the extended border node’s knowledge of existing resources and topology. These additional CP names are obtained by:

- Adding all native extended border nodes
• Adding all non-native, adjacent extended border nodes and network nodes with NETIDs that match the NETID of the destination resource.

• Examining the table of resources already known to the extended border node due to the receipt of a find or found GDS variable. These resources are cached in the Directory Services database. For any entries where the Netid of the cached LU is the same as the destination of the current search, add the NNs of the cached LU to the list of next-hop CPs. None of these dynamically obtained next-hop CP names are permanently saved with the configuration data. The list is recreated whenever a resource needs to be located.

**Full**  This functions the same as Limited, except the restriction on matching NETIDs is removed when adding all non-native, adjacent extended border nodes and network nodes.

If *list optimization* is enabled, the reordering process described on page 23 is repeated a second time and the CP names obtained from configured data are also eligible to be reordered.

If *load balance* across parallel inter-subnet boundaries is enabled, the router will attempt to balance the number of sessions across two or more parallel inter-subnet exit points. The relevant configuration has two or more routers serving as EBN exit points in one subnet, with the same number in the other subnet. Each router has an inter-subnet TG to a different router in the other subnet, forming two or more parallel links. (Note that these are not parallel TGs between any two routers.)

To enable this load balancing function, you must configure routing lists in each EBN router, so that sessions for different destination LU names have different preferred exit EBNs. You also configure the preferred inter-subnet boundary and can set backup paths.

**Add port**

If extended border node is enabled, two additional prompts are presented when you invoke the add port menu item. Both of these new items establish the default for analogous parameters at the link level. The values of these parameters at the link level determine link station behavior.

*Subnetwork visit count* is the first of these, and describes the same concept as defined at the node level. When a port is first configured this parameter is initialized to the node setting. With this parameter you allow individual ports to deviate from the node level setting.

*Adjacent subnetwork affiliation* is controlled by the other new extended border node prompt. This allows you to define whether or not the adjacent node is in the same network as the extended border node. The value specified here will be used as the default value for all links through the port. Allowed values are:

**Native**  Adjacent node is in the same topology subnetwork as the extended border node.

**Non-native**  Adjacent node is not part of the extended border node’s topology subnetwork.

**Negotiable**  Adjacent node may or may not be in the same topology subnetwork depending upon how the adjacent node is defined. The adjacent node is in
Using APPN

the extended border node’s topology subnetwork unless the adjacent node’s corresponding link definition is one of:

- Non-native
- Negotiable and the adjacent node has a different network name
- Negotiable and the adjacent node has defined the link as non-native

Add link

If extended border node is enabled the same two additional prompts are presented when you invoke the add link menu item as were previously presented under add port.

Subnetwork visit count and adjacent subnetwork affiliation are the same concept as defined at the port level. They are initialized to the corresponding port setting when a link is first configured. You change the value here if you want different links to have different values even though they are on the same port.

Add Routing Lists

Note: Routing lists are not supported for 2210 12x models.

A configured routing list allows you to explicitly define one or more possible next hop CPs for one or more destination resources (LUs). A wildcard character “*” may be used when defining the LU names to reduce the amount of configured data. You can also vary some of the node level defaults for a given routing list.

You can define multiple routing lists. Typically a group of LUs with similar routing requirements would be configured into a single routing list. Additional groups of LUs, each group with its own routing requirements, would be configured into additional routing lists.

There are limits on the number of LU names and number of CP names used in routing lists. These limits vary according to the model router you have. See Table 38 on page 208 for the configuration command detail. Limits have been set to allow as much flexibility as possible in various environments. The ability of the router to handle the specification of many routing lists, each with many LU names and CP names, is limited by the availability of configuration nonvolatile memory, router memory, and APPN shared memory. See “APPN Node Tuning” on page 33 for a discussion of the APPN tuning parameters which control the amount of shared memory.

Recall from the discussion under the set node prompt that configured routing lists are never modified by operational code. When the extended border node uses a given routing list it copies the next hop CP names into a temporary routing list. This temporary dynamic routing list is augmented with dynamic entries as allowed by your configuration setting of the list dynamics parameter. This temporary list is short lived, and is discarded once the destination resource is found or the list is exhausted.

The routing list name is the first prompt you see when adding or modifying a routing list. This name is not used by the operational code at all. It’s purpose is to allow you to identify a specific routing list if you want to modify it or delete it at some later time.

Subnetwork visit count and list optimization are the next two prompts, and follow the same concept as the analogous parameters defined at the node level. A new
routing list initializes these values with the current node level settings. You change these values for individual routing lists as your requirements dictate.

*Destination LU* prompt(s) are next. Here you may configure at least one, and optionally more, destination resources. Any of the FQLU names may be prematurely terminated with a trailing wildcard "***" to identify a group of LUs. You may not imbed a "***" in the middle of an FQLU name.

One of your routing lists may specify a standalone "***" as one of the destination LUs. If this is done, then that routing list is known as the default routing list, and it will be used by the extended border node for all destination LUs that do not better match the LUs specified in the other routing lists. This list is also used to find LUs when *INAUTHENTIC NETID* is indicated.

When modifying an existing routing list with many LU names the process of stepping through the LU names could be quite tedious. There are a number of shortcut keys defined to help speed stepping through an existing list of names. Those shortcut keys are defined in the section with the configuration command detail.

*Routing CP* prompts are the last part of entering a routing list. Here you supply the names of one or more CPs that may know how to reach the configured list of LUs. Along with each CP name you may configure an optional subnetwork visit count. This allows you to specify a different maximum number of subnetworks a session may traverse for different CPs.

In addition to explicitly configuring FQCP names there are a couple of keywords defined that equate to the local node’s CP name, all native extended border nodes, etc. See the section with configuration command detail for those keywords.

As with the LU name list, the same shortcut keys are available to speed stepping through an existing CP name list.

**Add CoS Mapping Table**

*Note:* CoS mapping tables are not supported for 2210 12x models.

The class of service mapping table allows for the conversion of non-native CoS names to native CoS names and vice versa. Non-native networks using the same CoS names as the extended border node’s native network need not have a CoS mapping table defined. If only some of the non-native CoS names differ from the native CoS names, then only those that differ should be configured in a CoS mapping table.

A given CoS mapping table may apply to a single or multiple non-native networks. You may configure multiple CoS mapping tables as necessary.

There are limits on the number of non-native network names used in CoS mapping tables. These limits vary according to the model router you have. See Table 39 on page 212 for the configuration command detail. Limits have been set to allow as much flexibility as possible in various environments. The ability of the router to handle the specification of many CoS mapping tables, each with many non-native network names and CoS name pairs, is limited by the availability of configuration nonvolatile memory, router memory, and APPN shared memory. See "APPN Node Tuning" on page 33 for a discussion of the APPN tuning parameters which control the amount of APPN shared memory.
Using APPN

**Cos mapping table name** is the first prompt. As with the analogous name for routing lists, this parameter is not used by the operational code. It’s purpose is to allow you to refer to a specific CoS mapping table so that you can modify or delete it. Different CoS mapping tables must have different names, but a given CoS mapping table may have an identical name as a routing list.

Non-native CP name(s) are prompted for next. These are use to specify the non-native network(s) that this CoS mapping table applies to.

As with LU names in a routing list, you may prematurely terminate any of the FQCP names at any point with a trailing wildcard “**” . This allows you to specify a range of non-native FQCP names in one or more non-native networks. You may not imbed a wildcard in the middle of a FQCP name.

One CoS mapping table in the extended border node may have a standalone wildcard “**” as one of the non-native CP names. Such a table is known as the default CoS mapping table, and will be the table used by the extended border node whenever no other table has a CP name that matches the non-native network.

**CoS name pairs** are the final part of configuring a CoS mapping table. Here you are prompted for one or more pairs of CoS names. Each CoS name pair consists of a native CoS name followed by the corresponding CoS name used in the non-native network.

The extended border node uses this table to translate from native to non-native networks and vise versa. If you need to map multiple native CoS names into a common non-native CoS name you should configure one CoS name pair for each possible mapping. Similarly you may need to map multiple non-native CoS names into a common native CoS name, and that too can be accomplished by configuring a CoS name pair for each possible mapping. If there are multiple possible mappings in a table the extended border node will use the first exact mapping found.

Each CoS mapping table may have one CoS name pair where the non-native CoS name is a wildcard “**”. This is the default CoS mapping entry for that table, and it is used to translate all unrecognized non-native CoS names into a single native CoS name. Each CoS mapping table may have one of these default CoS mapping entries. You can never code a “**” as the native CoS name.

High-Performance Routing

See **Table 2 on page 20** for a list of ports that support HPR.

See **Configuration Requirements for APPN on page 21** for information about configuring the protocols that support APPN and HPR routing over direct DLCs on the router. In the case of HPR parameters such as retry and path switch timers, the configuration is done at the node level and is not specified on individual adapters.

DLUR

See **Table 2 on page 20** for a list of ports that support DLUR.

Configuring Focal Points

Focal points can be explicit or implicit. Explicit focal points are configured at the focal point itself. No configuration at the router is required.
Implicit focal points on the other hand are configured at the router. You configure
them with the command `add focal_point`. Add the primary implicit focal point first. If
you add another focal point, it is known as the first backup implicit focal point. If you
add yet another, it is known as the second backup implicit focal point. Up to eight
backup implicit focal points may be added for a total of 9.

To delete a focal point use the command `delete focal_point`. You will be prompted
for the name of the focal point to delete. When the name is deleted, the remaining
focal points retain their relative position with each other. Subsequent focal points
will be added at the end of the list.

There is no way to insert a focal point in the middle of the list. You must delete
them one at a time and then re-enter the entire list.

**Configuring Held Alert Queue Size**

To configure the size of the held alert queue enter the command `set management`
and answer the Held Alert Queue Size question. The queue defaults to a size of 10
alerts, and valid values are from 0 through 255 alerts.

As you increase the size of the held alert queue, additional memory is needed. If
you set it to a high value, you may want to adjust the Maximum Shared Memory
value. See [APPN Node Tuning](#) on page 33 for additional information.

**Defining Transmission Group (TG) Characteristics**

When you configure APPN on the router, you can specify the Transmission Group
(TG) characteristics for the link station that defines a connection between the router
network node and an adjacent node. These characteristics, such as the security of
a link or its effective capacity, are used by APPN when calculating an optimum or
least-weight route between nodes in the APPN network.

APPN on the router uses a set of default TG characteristics for each port (or DLSw
port). These defaults, defined by the `default TG characteristics` parameter apply to
all the TGs for link stations defined on a port unless they are overridden for a
particular link station by the `modify TG characteristics` parameter.

These default TG characteristics are also used for dynamic link stations established
when an adjacent node requests a connection with the router network node, but
does not have a predefined link station definition on the router network node. The
`Service any node` parameter must be enabled.

You can change the following parameters using the router `talk 6>` interface as well
as the Configuration Program:

- time cost
- byte cost
- user-defined TG characteristics 1 - 3
- effective capacity
- propagation delay
- security

**Calculating APPN Routes Using TG Characteristics**

The APPN route calculation function uses a CoS definition for TGs which is a table
containing rows of TG characteristic ranges. Each row defines a given range for
each of the eight TG characteristics and the corresponding TG weight for that row.
APPN starts at the top of the table and continues down the table until all eight of
the TG characteristic parameter values fit within the ranges given for that row. APPN then assigns the weight of that row as the TG weight for that link. There is also a CoS definition for nodes that calculates a node’s weight. The route calculation function continues until it has found the path with the least combined weight of TGs and nodes. This is the least weight route.

As an example of how TG characteristics are used to influence the selection of a route through an APPN network node, suppose that a route from network node router A to network node router D can pass through either network node router B or router C. In this example, router A defines serial port PPP connections to both router B and router C. However, the connection from router A to router B is a 64-kbps link, while the connection from router A to router C is a slower-speed 19.2-kbps link.

To ensure that the higher-speed connection from router A to router B is viewed as the more desirable path for routing APPN interactive traffic, the effective capacity TG characteristic for the link station associated with this path would be modified. In this case, the default value for effective capacity is X'38', which correctly represents a link speed of approximately 19.2-kbps. However, the effective capacity would be changed to X'45' to properly represent the 64-kbps link. Since the effective capacity for the TG from router A to router B is now X'45', this path is assigned a lower weight in the CoS file for interactive traffic. Consequently, the connection from router A to router B is represented as more desirable than the connection from router A to router C.

You can also change the TG characteristics if you purposefully want to favor certain TGs for route selection. In addition to the five architected TG characteristics, there are also three user-defined TG characteristics. You may define these user-defined TG characteristics in order to bias the route selection calculation in favor of certain paths.

**Note:** For DLSw ports, the TG characteristics that you define effect only the selection of routes between APPN nodes over these DLSw ports. These characteristics have no direct effect on any intermediate routing performed by DLSw on behalf of the APPN.

**CoS Options**

You can use a template to create new user-defined CoS names and associated definitions for TGs and nodes which can be used with new mode names or mapped to existing mode names.

In addition you can create new mode names that can be mapped to existing CoS names.

Each CoS definition file is identified by a CoS name and contains an associated transmission priority and a table of ranges of acceptable TG and node characteristics that APPN compares against actual TG and node characteristics to determine weights for TGs and nodes from which APPN calculates the least weight route for the session. Using the Configuration Program you can:

- View a CoS definition file:
  - View the transmission priority
  - View a list of node row references along with their corresponding weights
  - View a list of TG row references along with their corresponding weights

- Select standard or ATM CoS tables as templates to define a new user-defined CoS definition file with a new CoS name:
– Import an IBM-defined CoS definition file to use as a template
– Import a previously exported user-defined CoS definition file to use as a template

• Define the minimum and maximum ranges for the user-defined TG characteristics within an IBM-defined CoS definition.

Note: In an IBM-defined CoS definition you can edit only the user-defined TG characteristic ranges.

Using Configuration Program or talk 6 you can:
• Use standard CoS tables or the Enhanced CoS tables (for ATM).
• Define a new mode name and its mapping to a CoS name.
• Change a mode name to CoS name mapping:
  – Re-map an IBM-defined mode name to a different CoS name.
  – Re-map a previously specified user-defined mode name to a different CoS name.

Refer to the discussion of Topology and Routing Services in the IBM SNA APPN Architecture Reference for a description of standard and ATM CoS tables.

APPN Node Tuning

The performance of the router APPN network node can be tuned in two ways:

• By manually setting the values of the **maximum shared memory**, **percent of APPN shared memory to be used for buffers**, and the **maximum cached directory entries** tuning parameters using the Configuration Program or talk 6 option of the command line interface.

  See the Web router support pages for a tool you can use to estimate the memory required for APPN and other router components.

• By selecting values for the **maximum number of ISR sessions**, **maximum number of adjacent nodes** and other parameters shown in Table 9 on page 112, and having the tuning algorithm automatically calculate the **maximum shared memory** and **maximum cached directory entries** tuning parameter values.

  Use the Configuration Program to invoke the tuning algorithm.

The **maximum shared memory** parameter affects the amount of storage available to the APPN network node for network operations. You can allow the router to choose a general-purpose default for this value based on its installed memory.

The **maximum cached directory entries** parameter affects the amount of directory information that will be stored or cached to reduce the time it takes to locate a resource in the network.

In general, tuning the APPN network node involves a trade-off between node performance and storage usage. The better the performance, the more storage required.

Tuning Notes

1. The tuning parameter settings should reflect anticipated growth in your network.
2. If you define connection networks within your APPN network and you anticipate that most end nodes will initiate LU-LU sessions with other end nodes on the same connection network, you should set the **maximum number ISR sessions** parameter to a smaller value (1). Using connection networks in this manner reduces the shared memory requirements for the router network node because most LU-LU sessions will not flow through the APPN component in the router.
Using APPN

3. Because the maximum shared memory parameter affects storage allocation within the router, you should use care when explicitly defining this parameter. Use the auto-configured default unless you do a more careful analysis using the router storage tool.

Node Service (Traces)

The APPN Node Service (Traces) option allows you to start any APPN trace through talk 6 or the Configuration Program. The traces are activated when the configuration file is applied to the router. The traces will continue to be active until they are stopped when a new configuration that stops the traces is applied to the router.

Note: Running traces on the router can affect its performance. Traces should be started only when needed for node service and should be stopped as soon as the required amount of trace information is gathered.

The APPN traces are grouped into the following 5 categories:
• Node-level traces specify traces concerning the overall APPN network node.
• Inter-process signals traces specify component-level traces concerning signals between APPN components.
• Module entry and exit traces specify component-level traces concerning the entry and exit of APPN modules.
• General traces specify component-level traces concerning the APPN components.
• Miscellaneous traces specify trace information about DLC transmissions and receptions.

You can now enable/disable all trace flags through Talk 6 using the Turn all trace flags off question asked under the set trace command or by using the Configuration Program. See page 138 for more information.

You can now filter the data link control transmissions and receptions trace data by either message type or by specifying the maximum length of data per packet to trace. See Table 15 on page 135 for information.

Accounting and Node Statistics

Intermediate sessions are LU-LU sessions that pass through the APPN network node, but whose endpoints (origin and destination) lie outside of the network node. Information about intermediate sessions is generated by the ISR component in the network node and falls into two categories:
• Intermediate session names and counters
• Route selection control vector (RSCV) data for intermediate sessions

Enabling the Collect intermediate session information parameter instructs the router to collect session names and counters for all active intermediate sessions. Enabling the Save RSCV information for intermediate sessions parameter instructs the router to collect RSCV data for active intermediate sessions. The RSCV data is useful for monitoring session routes. In both cases, you can retrieve the data on active sessions by issuing SNMP get and get-next commands for variables in the APPN Management Information Base (MIB).

The Collect intermediate session information function defaults to being disabled. You can enable it using the Configuration Program or using the Talk 6 set
management command. Once enabled, you can control it, including disabling and re-enabling, using SNMP set commands to the APPN accounting MIB.

Note: This function can use a significant amount of APPN memory. You should configure APPN with the needed memory before you enable the collection of ISR information.

For accounting purposes, you can maintain records of intermediate sessions passing through the network node. The data records can be created and stored in router memory. SNMP must be used to retrieve data from accounting records stored in the router’s local memory.

Notes:
1. You can enable collection of active intermediate session data (session counters and session characteristics) in SNMP MIB variables explicitly or implicitly.
   To enable collection explicitly, set the Collect intermediate session information parameter to yes.
   To enable collection implicitly, set Create intermediate session records to yes. This setting will override the setting of Collect intermediate session information.
2. Configuration changes to the APPN accounting parameters made using the Talk 6 interface will not take effect until the router or the APPN function on the router is restarted. You can make changes interactively, however, by issuing SNMP set commands to modify the APPN MIB variables associated with the configuration parameters. Refer to the Software User’s Guide for a list of these MIB variables.
3. Data on intermediate session RSCVs is obtained by examining the BIND request used to activate a session between two LUs. RSCV data is not collected for sessions that have already been established because the BIND information for those sessions is not available.
4. Intermediate session data is not collected for HPR sessions since intermediate sessions are not part of HPR. If the router contains an ISR/HPR boundary, intermediate session data is collected when it flows across that boundary.

**DLUR Retry Algorithm**

If communication between DLUR and DLUS is broken, the following algorithm is used to reestablish communication:

If Perform retries to restore disrupted pipe is No:
- If DLUR receives a non-disruptive UNBIND (sense code of X’08A0 000A’), DLUR waits indefinitely for a DLUS to reestablish the broken pipe.
- If the pipe fails for any other reason than a non-disruptive UNBIND, DLUR attempts to reach the primary DLUS once. If this is unsuccessful, DLUR attempts to reach the backup DLUS. If DLUR is unable to reach the backup DLUS, it waits indefinitely for a DLUS to reestablish the broken pipe.

If Perform retries to restore disrupted pipe is Yes, DLUR will attempt to reestablish the pipe based on the following configuration parameters:
- Delay before initiating retries
- Perform short retries to restore disrupted pipe
- Short retry timer
- Short retry count
- Perform long retries to restore disrupted pipe
- Long retry timer

There are two cases that determine the retry algorithm:
For the case of receiving a non-disruptive UNBIND:
1. Wait for the amount of time specified by the Delay before initiating retries parameter. This delay allows time for an SSCP takeover, where the pipe would be reestablished by a new DLUS without action on the DLUR’s part.
2. Attempt to reach the primary DLUS.
3. If unsuccessful, attempt to reach the backup DLUS.
4. If the attempt to reach the backup DLUS is unsuccessful, DLUR will retry as described in Step 6 to Step 8 as long as the DSPU is requesting ACTPU.
5. Wait for the amount of time specified by the Long retry timer parameter.

   **Note:** If Perform long retries to restore disrupted pipe is No, no further retries will be attempted.
6. Attempt to reach the primary DLUS.
7. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS.

**Example:**
- Assume the following parameter values:
  - Delay before initiating retries = 120 sec
  - Perform short retries to restore disrupted pipe = yes
  - Short retry timer = 60 sec
  - Short retry count = 2
  - Perform long retries to restore disrupted pipe = yes
  - Long retry timer = 300 sec
- Pipe activation fails.
- Wait 120 seconds (the value of Delay before initiating retries).
- Retry the primary DLUS and, if this fails, retry the backup DLUS.
- If retry fails, wait 300 seconds (the value of Long retry timer), retry the primary DLUS and if this retry fails, retry the backup DLUS.
- If retries fail, continue to retry the primary and backup DLUS, waiting 300 seconds between retry sequences, for as long as the DSPU is requesting ACTPU.

For all other cases of pipe failure, DLUR will try the primary DLUS and then the backup DLUS immediately. If this fails, DLUR will:
1. Wait for the amount of time specified by the minimum of the Short retry timer and the Delay before initiating retries parameters.
2. Attempt to reach the primary DLUS.
3. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS.
4. If pipe activation continues to fail, DLUR will retry as described in steps 6 to 8 for the number of times specified in the Short retry count.
   If the Short retry count is exhausted, DLUR will retry as defined in steps 6 to 8 as long as the DSPU is requesting ACTPU.
5. Wait for the amount of time specified by the Long retry timer parameter.

   **Note:** If Perform long retries to restore disrupted pipe is No, no further retries will be attempted.
6. Attempt to reach the primary DLUS.
7. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS.

**Example:**
Assume the following parameter values:
- Delay before initiating retries = 120 sec
- Perform short retries to restore disrupted pipe = yes
- Short retry timer = 60 sec
- Short retry count = 2
- Perform long retries to restore disrupted pipe = yes
- Long retry timer = 300 sec
- Pipe activation fails.
- Retry the primary and backup DLUS immediately.
- If this retry fails, wait 60 seconds (the value of Short retry timer).
- Retry the primary DLUS. If this retry fails, retry the backup DLUS. This is attempt #1 of the Short retry count.
- If this fails, wait 60 seconds (the value of Short retry timer).
- Retry the primary DLUS, and then the backup DLUS. This is attempt #2 Short retry count. Short retry count is now exhausted.
- If the retry still fails, wait 300 seconds (the value of Long retry timer). Then retry the primary DLUS.
- As long as the retry fails, continue to retry the primary and the backup DLUS, waiting 300 seconds between retry sequences, for as long as the DSPU is requesting ACTPU.

**APPN Implementation on the Router Using DLSw**

The router also supports APPN over DLSw for connectivity to nodes through a remote DLSw partner. An example is shown in Figure 2. This support allows customers with DLSw networks to reach APPN without needing an external DLSw router. It also allows remote TN3270 servers to reach the host through subarea DLSw links.

**Note:** It is recommended to use APPN over direct DLCs when available instead of APPN over DLSw. However, local DLSw is the only way that a remote TN3270 server can use SDLC or X.25 QLLC subarea links to reach the host.

**Figure 2. Data Flow in an APPN Configuration Using DLSw Port**

APPN configuration restrictions using DLSw:
- Only one DLSw logical port per router
- Use of a locally administered MAC address
- HPR is not supported on DLSw ports
- DLSw ports cannot be members of connection networks
Using APPN

- Parallel TGs are not supported on DLSw ports

See [Configuring the Router as an APPN Network Node on page 21](#) to configure APPN using DLSw.

**How APPN Uses DLSw ports to Transport Data**

When APPN is configured on the router to use the Data Link Switching (DLSw) port, DLSw provides a connection-oriented interface (802.2 LLC type 2) between the APPN component in the router and APPN and SNA nodes attached to a remote DLSw partner.

When configuring a DLSw port for APPN on the router, you assign the network node a unique MAC address and one or more SAP addresses that enable it to communicate with DLSw. The MAC address for the network node is locally administered and must not correspond to any physical MAC address in the DLSw network. Multiple SAP addresses are required only when you are configuring the TN3270 server to reach the host through DLSw and you need more than one dependent PU.

**APPN Frame Relay BAN Connection Network Implementation**

The implementation of an APPN Frame Relay BAN connection network allows you to define an APPN Frame Relay port that supports the bridged Frame Relay format (BAN) to a connection network.

A shared-access transport facility (SATF) is a transmission facility, such as token-ring or Ethernet, in which nodes attached to the SATF can achieve any-to-any connectivity. This any-to-any connectivity allows direct connections between two nodes, eliminating routing through intermediate network nodes and the corresponding data traversing the SATF many times. TGs must be defined on each node to all other nodes in order to achieve this direct connectivity.

The SATF shown in [Figure 3](#) illustrates that the APPN NN in the router must define a link station to each node on the token-ring in order to initiate a connection to each node on the token-ring. The APPN NN must know the DLCI address for the Frame Relay link and the MAC address of each node on the token-ring. If the nodes on the token-ring want to initiate a connection to the APPN NN, they must define a link station in the APPN NN in the device and specify:

- BAN DLCI MAC address if the device connecting the token-ring to the frame relay network is performing the BAN function
- The Boundary Node Identifier MAC address if the device connecting the token-ring to the Frame Relay network is a bridge

![Figure 3. Logical View with Frame Relay Bridged Frame/BAN Connection Network Support](#)

**Note:** In this diagram and in all the following Frame Relay BAN diagrams, the APPN resides in the 2210.
Defining connections between all possible pairs of nodes attached to the SATF results in a large number of definitions and a large number of topology database update flows on the network. APPN allows nodes to become members of a connection network to represent their attachment to the SATF.

Figure 4 shows all nodes as members of the same connection network. Nodes use the connection network to establish communication with all other nodes, removing the necessity of creating connections to all other nodes on the SATF. To become a member of a connection network, an APPN node’s port must be attached to a connection network by defining a connection network interface. When the port is activated, a connection network TG is created by the APPN component to a Virtual Routing Node (VRN). This TG identifies the direct connection from the port to the connection network. The CP name of the VRN is the connection network name.

Since the connectivity is represented by a TG from a given node to a VRN, normal topology and routing services (TRS) can be used by the network node server to calculate the direct path between any two nodes attached to the connection network. DLC signaling information is returned from the destination node during the normal locate process to enable the origin node to establish a connection directly to the destination node.

The following are limitations on using APPN Frame Relay BAN connection networks:

- The same connection network can be defined on only one SATF.
- All Frame Relay ports belonging to the same connection network on the router must use the same DLCI number to connect to the Frame Relay network.
- When bridging is used instead of BAN, all Frame Relay ports belonging to the same connection network on the router must have the same BNI MAC address/SAP pair defined.
- CP-CP sessions cannot be established over links established through a connection network.

Sample APPN Frame Relay BAN Connection Network Definitions

Example 1
Using APPN

Example 2

Notes:
1. The same DLCI number must be specified on both ports.
2. The BDA address must be defined on the connection network definition.
3. The BNI address on both ports can be the same or different.
4. If the APPN node initiates the connection to the device, the APPN port that gets chosen for the connection is dependent upon which port responds first to the test frame.

Example 3

Notes:
1. This configuration requires two connection network definitions since there are two SATFs.
2. The DLCI number specified on the ports can be the same or different.
Using APPN

3. The BDA MAC address must be defined on the connection network definition.
4. The BNI MAC address specified on the ports can be the same or different.

Example 4

Figure 8. Single Connection Network using Bridging with One Frame Relay Port

Notes:
1. The BDA address is not defined on the connection network definition.

Example 5

Figure 9. Single Connection Network Using Bridging with Multiple Frame Relay Ports

Notes:
1. The same DLCI number must be specified on both ports.
2. The same BNI MAC address/SAP pair must be specified on both ports.
3. No BDA MAC address is specified on the connection network definition.
4. If the APPN node initiates the connection to the device, the APPN port chosen for the connection depends upon which port responds first to the test frame.

Example 6
Using APPN

Notes:
1. This configuration requires two connection network definitions since there are two SATFs.
2. The DLCI number specified on the ports can be the same or different.
3. The BDA MAC address is not defined on the connection network definition.
4. The BNI MAC address/SAP pair specified on the ports can be the same or different.

Port Level Parameter Lists
Use the following tables to configure APPN ports:

- “Port Configuration” on page 142
- “Port Definition” on page 152
- “Port Default TG Characteristics” on page 157
- “Port default LLC Characteristics” on page 163

Link Level Parameter Lists
Use the following tables to configure APPN link stations:

- “HPR Defaults” on page 165
- “Link Station - Detail” on page 167
- “Modify TG Characteristics” on page 184
- “Modify Dependent LU Server” on page 186
- “Modify LLC Characteristics” on page 187
- “Modify HPR Defaults” on page 190

LU Parameter List
Use the following table to configure an LU:

- “LEN End Node LU Name” on page 192
Node Level Parameter Lists

Use the following tables to configure an APPN node:

- "Local node basic characteristics" on page 97
- "High Performance Routing (HPR)" on page 104
- "HPR Timer and Retry Options" on page 104
- "Dependent LU Requester" on page 106
- "Connection Network - Detail" on page 193
- "TG Characteristics (Connection Network)" on page 199
- "APPN COS - Additional port to CN" on page 204
- "Node Level Traces" on page 113
- "Interprocess Signals Traces" on page 124
- "Module Entry and Exit Traces" on page 128
- "General Component Level Traces" on page 130
- "APPN Node Management" on page 138
- "TN3270E" on page 215
- Table 38 on page 208
- Table 39 on page 212

APPN Configuration Notes

The following examples show special parameters to consider when configuring various features to transport APPN traffic.

Note: These examples show sample output. The output you see may not appear exactly like the output shown here.

Note: In some configuration examples, the results of a talk 6 list command may show more configuration than is actually presented in the sample. However, the sample will show all of the configuration that is unique.

Configuring a Permanent Circuit Using ISDN

This example is a configuration of a permanent circuit using Frame Relay over ISDN from node 21 to node 1.

Note: You configure a permanent circuit by setting the idle timer value to 0.

************************************************************************
**** Configuring a PERMANENT circuit via ISDN from NN21 to NN1
**** Using Frame Relay over ISDN
************************************************************************

Config on 6
Circuit configuration
FR Config 1 all

Base net = 3
Destination name = 2210-01
Circuit priority = 8
Destination address: subaddress = 99195551234:

Inbound destination name = 2210-01
Inbound dst address: subaddress = 99195551000:

Inbound calls = allowed
Idle timer = 0 (fixed circuit)
SelfTest Delay Timer = 150 ms
Using APPN

FR Config> ex

************************************************************************
**** Verify that a FR PVC is defined to NN1. This is required for APPN
************************************************************************

Config> 6
Circuit configuration
FR Config>en
Frame Relay user configuration
FR Config>li perm

Maximum PVCs allowable = 64
Total PVCs configured = 1

<table>
<thead>
<tr>
<th>Circuit Name</th>
<th>Circuit Number</th>
<th>Type in bps</th>
<th>CIR</th>
<th>Burst</th>
<th>Excess</th>
</tr>
</thead>
<tbody>
<tr>
<td>2210-21-16</td>
<td>2</td>
<td>Permanent</td>
<td>16</td>
<td>64000</td>
<td>0</td>
</tr>
</tbody>
</table>

- circuit is required and belongs to a required PVC group

FR Config>ex
Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING, (S)DLC, (Y)25, (O)LTW, (A)TM, [IP] [] ? f
Interface number(Default 0): [0] ? 6
Port name (Max 8 characters) [FR006] ?
Enable APPN on this port (Y)es (N)o [Y] ?
Port Definition
Service any node: (Y)es (N)o [Y] ?
Limited resource: (Y)es (N)o [N] ?
High performance routing: (Y)es (N)o [Y] ?
Maximum BTU size (768-2044) [2044] ?
Percent of link stations reserved for incoming calls (0-100) [0] ?
Percent of link stations reserved for outgoing calls (0-100) [0] ?
Local SAP address (04-EC) [4] ?
Support bridged formatted frames: (Y)es (N)o [N] ?
Edit TG Characteristics: (Y)es (N)o [N] ?
Edit LLC Characteristics: (Y)es (N)o [N] ?
Edit HPR defaults: (Y)es (N)o [N] ?
Write this record? [Y] ?
The record has been written.

APPN config>add li
APPN Station
Port name for the link station [ ] ? fr006
Station name (Max 8 characters) [ ] ? tonn1isdn
Station name (Max 8 characters) [ ] ? tonn1is
Limited resource: (Y)es (N)o [N] ?
Activate link automatically (Y)es (N)o [Y] ?
DLCI number for link (16-1007) [16] ?
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0] ?
High performance routing: (Y)es (N)o [Y] ?
Edit Dependent LU Server: (Y)es (N)o [N] ?
Allow CP-CP sessions on this link (Y)es (N)o [Y] ?
CP-CP session level security (Y)es (N)o [N] ?
Configure CP name of adjacent node: (Y)es (N)o [N] ?
Edit TG Characteristics: (Y)es (N)o [N] ?
Edit LLC Characteristics: (Y)es (N)o [N] ?
Edit HPR defaults: (Y)es (N)o [N] ?
Write this record? [Y] ?
The record has been written.
APPN config>ex

APPN config>li all
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN21
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
DLUR:
  DLUR ENABLED: YES
  PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
  CN NAME: NETB.MVSC
  PORT INTERFACES

COS:
  COS NAME
  BATCH
  BATCHSC
  CONNECT
Using APPN

Configuring APPN Over Dial on Demand Circuits

APPN is supported over dial on demand circuits for the following DLC types:

- APPN/PPP/ISDN
- APPN/FR/ISDN
- APPN/PPP/V.25 bis
- APPN/PPP/V.34

Refer to the Software User’s Guide for additional information about dial on demand circuits.

PU 2.1 Node Considerations

When configuring an APPN link station for PU 2.1 nodes over a Dial on Demand link, you should specify yes for the limited resource link station parameter. This allows APPN to:

- Consider this link as a viable link to be used for route computation, even though the link is not actually active. The link will automatically become active during LU-LU session activation for a session needing to use it.
- Deactivate the link station when there are no active sessions using this link.

You should not configure CP-CP sessions over a dial on demand link. CP-CP sessions are persistent sessions. That is, they should remain active as long as the link is active. Since the active session count will not go to zero in this case, the link will remain active.

Note:
1. Idle timer = 0 gives a fixed circuit
2. Frame relay PVC is defined
3. This is the ISDN port
4. This is the link station
Using APPN

**Note:** If you specify yes for the `limited resource` parameter for a PU 2.1 node, you must specify an adjacent CPNAME and a TG number in the range of 1 to 20.

**PU 2.0 Node Considerations**

When configuring an APPN link station for PU 2.0 nodes over a Dial on Demand link, you can specify yes for the `limited resource` link station parameter. This allows APPN to deactivate the link station when there are no active sessions using it.

**Note:** If `limited resource` is yes, link activation for this link station must be initiated by either the DSPU (the PU 2.0) or by VTAM.

**Considerations When Using DLUR for T2.0 or T2.1 Devices**

For T2.0 or T2.1 nodes utilizing DLUR for dependent session traffic, an SSCP-PU and an SSCP-LU session must be active in order to establish an LU-LU session. These sessions are included in the session count for the link to the DSPU. Therefore, if `limited resource` is yes, the link will remain active as long as the SSCP-PU session is active or LU-LU sessions are active over this link.

If you specify no for the `limited resource` parameter, link deactivation is controlled by the node that initiated the connection.

If the link to the DSPU was activated due to the DSPU calling into the DLUR node or the DLUR node calling out to the DSPU (i.e. the link station to the DSPU has been configured in the router and `activate link automatically` is yes), when the active session count goes to zero the link is deactivated by APPN DLUR only if the DSPU requested DACTPU. In this case, if the DLUS sends a DACTPU request to DLUR, DLUR will deactivate the SSCP-PU session. However, it will not deactivate the link to the DSPU. DLUR will attempt to reestablish the SSCP-PU session to the DLUS or the backup DLUS until it is successful or until the DSPU no longer needs this session.

If the link to the DSPU was activated by the DLUS and the session count goes to zero, the link is deactivated by APPN DLUR only if the DLUS sends a DACTPU request to DLUR.

The following is a dial on demand configuration example. This configuration is similar to the ISDN permanent connection except:

- You must specify that the link is a limited resource.
- You must define the adjacent CP name.
- You must specify a TG number.

You configure both sides of the communication link the same way.

**Note:** If you allow CP-CP sessions on this link, the link will not disconnect.

```
* 6
Gateway user configuration
Config>
*************************************************************************
**** This is the NN6 configuration for a NN6----NN15 dial on demand link.
**** The NN15 config will look just like this.
**** interface 9 is a Dial On Demand link with destination = NN15
*************************************************************************
Confign 9
Circuit configuration
FR Config>li all

Base net = 6
Destination name = 2210-15
Circuit priority = 8
```
Inbound destination name = 2210-15
Inbound calls = allowed
Idle timer = 60 sec
SelfTest Delay Timer = 150 ms
FR Config>ex

***************************************************************************
**** Configure APPN Port for the Interface
***************************************************************************

Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (I)OKEN RING,
(S)DLC, (X)25, (D)Lsw, (A)TM, (IP) ? p
Interface number(Defualt 0): [0 ] ? 9
Port name (Max 8 characters) [PPP009 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
Service any node: (Y)es (N)o [Y ] ?
Limited resource: (Y)es (N)o [Y ] ?
**** note that limited resource = YES
High performance routing: (Y)es (N)o [Y ] ?
Maximum BTU size (768-2044) [2044 ] ?
Local SAP address (04-EC) [4 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.

***************************************************************************
**** Configure the linkstation for the DOD link to NN15
***************************************************************************

APPN config>add li
APPN Station
Port name for the link station [ ] ? ppp009
Station name (Max 8 characters) [ ] ? to15dod
**** < note limited resource= YES
TG Number (1-20) [1 ] ?
**** < note TG number is required input for limited resource
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node [0 ] ?
High performance routing: (Y)es (N)o [Y ] ?
Allow CP-CP sessions on this link (Y)es (N)o [Y ] ?
**** < Be sure to NOT allow CP-CP sessions, or link won’t hang up
Fully-qualified CP name of adjacent node (netID.CPname) [ ] ? stfnet.NN15
**** < Adjacent node name required for limited resource links
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>li all

NODE:
NETWORK ID: STFNET
CONTROL POINT NAME: NN6
XID: 00000
APPN ENABLED: YES
MAX SHARED MEMORY: 4096
MAX CACHED: 4000
DLUR:
DLUR ENABLED: YES
PRIMARY DLUS NAME: NETB.MVSC

CONNECTION NETWORK:
---------------------------------------
| CN NAME | LINK TYPE | PORT INTERFACES |
---------------------------------------
| BATCH | COS | COS NAME |
| BATCHSC | BATCHSC | |
| CONNECT | CONNECT | |
| INTER | INTER | |
| INTERSC | INTERSC | |

Chapter 1. Using APPN 47
Configuring WAN Reroute

WAN reroute lets you set up an alternate route so that if a primary link fails, the router automatically initiates a new connection to the destination through the alternate route.

You can use any type of link as the alternate link and any type of link as the primary link. The alternate link does not need to be connected to the same end point as the primary link.

If HPR is used on the primary link and alternate link, when the primary link fails, HPR’s Non-disruptive Path Switch function will automatically reroute traffic to the alternate link without disrupting end user sessions.

In this configuration example, the router performing the WAN reroute function is configured with two APPN link station definitions; one link station is defined over the primary interface and the other is over the alternate interface. The destination router needs to have APPN enabled on the port. If the destination router has a link station defined, that link station should not try to bring up the connection in order to avoid extra traffic.
In this example, Frame Relay is the primary route from NN22 to NN6.

*************************************************************************
**** The configuration is NN22---primary FR
**** ---Alternate WRR to NN6
*************************************************************************
****
**** This is the NN22 configuration
*************************************************************************
Ifc 0 Token Ring CSR 6000000, vector 28
Ifc 1 WAN Frame Relay 1 CSR B1620, CSR2 800000, vector 93
Ifc 2 WAN PPP CSR B1640, CSR2 800000, vector 92
Ifc 3 ISDN Basic CSR 0, vector 0
Ifc 4 PPP Dial Circuit 2 CSR 0, vector 0 (Disabled)
Ifc 5 PPP Dial Circuit CSR 0, vector 0 (Disabled)
Ifc 6 Frame Relay Dial Circuit CSR 0, vector 0 (Disabled)
*************************************************************************
* Ifc 4 is the ALTERNATE with Ifc 1 configured as PRIMARY.
* Note that interface 4 should be 'Disabled' here.
* Wan Reroute function will 'Enable' it when the
* Primary fails
*
* NN6 (2210-06) is going the be the destination of the Wan Reroute
*************************************************************************
Config>n 4
Circuit configuration
FR Config>li
   Base net = 3
   Destination name = 2210-06
   Circuit priority = 8
   Destination address: subaddress = 99199991201:
   Outbound calls = allowed
   Idle timer = 0 (fixed circuit)
   SelfTest Delay Timer = 150 ms
Config>ex
*************************************************************************
**** Configure the Wan Reroute Primary and Alternate circuit
*************************************************************************
Config>fea wan 4
WAN Restoral user configuration
WRS Config>en wrs
WRS Config>add alt
Alternate interface number [0] ? 4
Primary interface number [0] ? 1
WRS Config>li all
WAN Restoral is enabled.
Default Stabilization Time: 0 seconds
Default First Stabilization Time: 0 seconds
[No Primary-Secondary pairs defined]
Primary Interface 1st Subseq TOD Revert Back
Alternate Interface Enabled Stab Start Stop
----------------- ---------------------- ------- ---- ---- ------- -------
1 - WAN Frame Re 4 - PPP Dial Circuit No dflt dflt Not Set Not Set
*************************************************************************
* Set Default and first stabilization times
*
Using APPN

**********************************************************************

WRS Config> set default firs 30
WRS Config> set def stab 10
WRS Config> li all
WAN Restoral is enabled.
Default Stabilization Time: 10 seconds
Default First Stabilization Time: 30 seconds
[No Primary-Secondary pairs defined]

Primary Interface Alternate Interface Enabled Stab Stab Start Stop
---------------------------------------------------------------
1 - WAN Frame Re 4 - PPP Dial Circuit No dflt dflt Not Set Not Set

WRS Config> en alt
Alternate interface number [0 ] ? 4
WRS Config> 

**********************************************************************

*Configure APPN PORTS and LINKSTATIONS for the
+ALTERNATE and PRIMARY interfaces

Config>p appn
APPN user configuration
APPN config>add p 5
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)thernet, (T)OKEN RING,
(S)DLC, (X)25, (D)Lsw, (A)TM, (I)P [ ] ? p
Interface number(Defaul 0): [0 ] ? 4
Port name (Max 8 characters) [PPP004 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
Service any node: (Y)es (N)o [Y ] ?
Limited resource: (Y)es (N)o [N ] ?
High performance routing: (Y)es (N)o [Y ] ?
Maximum BTU size (768-2044) [2044 ] ?
Local SAP address (04-EC) [4 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>add li 6
APPN Station
Port name for the link station [ ] ? ppp004
Station name (Max 8 characters) [ ] ? toNN6WRR
Limited resource: (Y)es (N)o [N ] ?
Activate link automatically (Y)es (N)o [Y ] ?
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node [0 ] ?
High performance routing: (Y)es (N)o [Y ] ?
Allow CP-CP sessions on this link (Y)es (N)o [Y ] ?
CP-CP session level security (Y)es (N)o [N ] ?
Configure CP name of adjacent node: (Y)es (N)o [N ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>add li 6
APPN Station
Port name for the link station [ ] ? fr001
Station name (Max 8 characters) [ ] ? tonNlpri
Activate link automatically (Y)es (N)o [Y ] ?
DLCI number for link (16-1007) [16 ] ? 421
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node [0 ] ?
High performance routing: (Y)es (N)o [Y ] ?
Allow CP-CP sessions on this link (Y)es (N)o [Y ] ?
CP-CP session level security (Y)es (N)o [N ] ?
Configure CP name of adjacent node: (Y)es (N)o [N ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>li all
NODE:
NETWORK ID: STFNET

50 MRS V3.4 Protocol Reference V2
CONTROL POINT NAME: NN22
XID: 000000
APPN ENABLED: YES
MAX SHARED MEMORY: 4096
MAX CACHED: 4000
DLUR:
DLUR ENABLED: NO
PRIMARY DLUS NAME:
CONNECTION NETWORK:

CN NAME | LINK TYPE | PORT INTERFACES
--------|-----------|-----------------

COS:
COS NAME
--------
BATCH
BATCHSC
CONNECT
INTER
INTERSC
CPVCMD
SNASVCMG

MODE NAME | COS NAME
----------|-----------

PORT:

<table>
<thead>
<tr>
<th>INF</th>
<th>PORT NAME</th>
<th>LINK TYPE</th>
<th>HPR</th>
<th>SERVICE</th>
<th>PORT NUMBER</th>
<th>PORT TYPE</th>
<th>ENABLED</th>
<th>ANY ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>TR000</td>
<td>IBMTRNET</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>

**** < this is the Primary port
1   FR001   | FR   | YES | YES | YES

**** < this is the alternate port
4   PPP004 | PPP  | YES | YES | YES

STATION:

<table>
<thead>
<tr>
<th>STATION</th>
<th>PORT</th>
<th>DESTINATION</th>
<th>HPR</th>
<th>ALLOW</th>
<th>ADJ NODE</th>
<th>CP-CP</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TONN25</td>
<td>FR001</td>
<td>132</td>
<td>YES</td>
<td>YES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TONN31</td>
<td>FR001</td>
<td>141</td>
<td>YES</td>
<td>NO</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TONN103</td>
<td>FR001</td>
<td>153</td>
<td>YES</td>
<td>NO</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**** < this is the alternate to NN6

| TONN6WRR | PPP004| 00000000 | YES | YES | 0        |      |      |

**** < this is the Primary to NN1

| TONN1PRI | FR001| 121       | YES | YES | 0        |      |      |

LU NAME:

<table>
<thead>
<tr>
<th>LU NAME</th>
<th>STATION NAME</th>
<th>CP NAME</th>
</tr>
</thead>
</table>

APPN config> ex

************************************************************************
************************************************************************
Config>
************************************************************************
************************************************************************
Config>
************************************************************************
************************************************************************
**** The configuration is NN22---primary FR
**** ---Alternate WRR to NN6
****
** This is the NN6 configuration which is the destination side for the
* NN22 Wan Reroute
* interface 17 has the ISDN lid for 2210-22 so when NN22 calls into NN6,
* it will map to interface 17
*
************************************************************************

Config> n 17
Circuit configuration
FR Config> fea 11 all

<table>
<thead>
<tr>
<th>Base net</th>
<th>= 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination name</td>
<td>= 2210-22</td>
</tr>
<tr>
<td>Circuit priority</td>
<td>= 8</td>
</tr>
<tr>
<td>Inbound destination name</td>
<td>= 2210-22</td>
</tr>
<tr>
<td>Inbound calls</td>
<td>= allowed</td>
</tr>
<tr>
<td>Idle timer</td>
<td>= 0 (fixed circuit)</td>
</tr>
<tr>
<td>SelfTest Delay Timer</td>
<td>= 150 ms</td>
</tr>
</tbody>
</table>

FR Config> ex
**** on this side, the interface must be ENABLED all the time
Using APPN

Config> ena in 17
Interface enabled successfully

************************************************************************
* Define the APPN PORT; NN22 will call into NN6 and dynamically create
* the linkstation when NN22 does a Wan Reroute.
************************************************************************

Config> p appn
APPN user configuration
APPN config> add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (T)HERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)Lsw, (A)TM, (IP) [ ] ? p
Interface number (Default 0): [0] ? 17
Port name (Max 8 characters) [PPP017] ?
Enable APPN on this port (Y)es (N)o [Y] ?
Port Definition
Service any node: (Y)es (N)o [Y] ?
Limited resource: (Y)es (N)o [N] ?
High performance routing: (Y)es (N)o [Y] ?
Maximum BU size (768-2044) [2044] ?
Local SAP address (04-EC) [4] ?
Edit TG Characteristics: (Y)es (N)o [N] ?
Edit LLC Characteristics: (Y)es (N)o [N] ?
Edit HPR defaults: (Y)es (N)o [N] ?
Write this record? [Y] ?
The record has been written.

APPN config> li al

NODE:
NETWORK ID: STFNET
CONTROL POINT NAME: NN6
XID: 00000
APPN ENABLED: YES
MAX SHARED MEMORY: 4096
MAX CACHED: 4000
DLUR:
DLUR ENABLED: YES
PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:

-------------------------------------------------------------
CN NAME   LINK TYPE PORT INTERFACES
-------------------------------------------------------------

COS:
COS NAME
--------

BATCH
BATCHSC
CONNECT
INTER
INTERSC
CPSCMVCG
SNSCMVG
USRNOT

MODE:
MODE NAME COS NAME
---------------------

USRBAT USRBAT
USRNOT USRNOT

PORT:
NUM  PORT  LINK HPR SERVICE PORT
INTR  NAME  TYPE ENABLED ANY ENABLED
------------------------------------------------------
0   TR000  IBMTRNET YES YES YES
1   PPP001  PPP YES YES YES
2   SS  SDLC NO YES YES
3   SDLC NO YES NO
4   PPP YES YES NO
5   TR005  IBMTRNET YES YES YES
254  DLS NO YES NO
17  PPP017  PPP YES YES YES

STATION:
STATION NAME PORT DESTINATION HPR ALLOW ADJ NODE TYPE
-----------------------------------------------
TONN1  TR000  0004CAE75055 YES YES 1
TONN2  TR000  550020004020 YES YES 1
TONN9  TR000  0004CAE9551D YES YES 1
TOPC4  TR000  0004CA941684 YES YES 1
TOVTTM1 TR000  400000003888 YES YES 1
Using APPN

Chapter 1. Using APPN

Configuring WAN Restoral

The following example shows APPN over a primary PPP link. For APPN, no unique definitions are needed. Both sides of the communication link are enabled for WAN restoral and are similarly configured.

*************************************************************************
*** Configuration of NN6 with a Wan Restoral link to NN35
*** interface 1 is the primary, interface 8 is the Secondary
*** NN35 must also have Wan Restoral configured for its primary/secondary
*** interfaces
*** Note that for APPN, there are NO unique definitions needed.
*************************************************************************

Circuit configuration
FR Config> li al

Base net = 6
Destination name = 2210-35
Circuit priority = 8

Inbound destination name = 2210-35
Inbound calls = allowed
Idle timer = 0 (fixed circuit)
SelfTest Delay Timer = 150 ms

FR Config> ex
Config> fea wan
WAN Restoral user configuration
WRS Config> li all

WAN Restoral is enabled. Yes
Default Stabilization Time: 0 seconds
Default First Stabilization Time: 0 seconds

Primary Interface Secondary Interface Secondary Enabled
----------------------- ----------------------- --------
1 - WAN PPP 8 - PPP Dial Circuit Yes

WRS Config> ex
Config> p appn
APPN user configuration
APPN config> li al

NODE:
NETWORK ID: STFNET
CONTROL POINT NAME: NN6
XID: 000000
APPN ENABLED: YES
Using APPN

MAX SHARED MEMORY: 4096
MAX CACHED: 4000
DLUR:
DLUR ENABLED: YES
PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
<table>
<thead>
<tr>
<th>CN NAME</th>
<th>LINK TYPE</th>
<th>PORT INTERFACES</th>
</tr>
</thead>
</table>

COS:
<table>
<thead>
<tr>
<th>COS NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>BATCH</td>
</tr>
<tr>
<td>BATCHSC</td>
</tr>
<tr>
<td>CONNECT</td>
</tr>
<tr>
<td>INTER</td>
</tr>
<tr>
<td>INTERSC</td>
</tr>
<tr>
<td>CPSVCMG</td>
</tr>
<tr>
<td>SNASVCMG</td>
</tr>
<tr>
<td>USRBAT</td>
</tr>
<tr>
<td>USRNOT</td>
</tr>
</tbody>
</table>

MODE:
<table>
<thead>
<tr>
<th>MODE NAME</th>
<th>COS NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>USRBAT</td>
<td>USRBAT</td>
</tr>
<tr>
<td>USRNOT</td>
<td>USRNOT</td>
</tr>
</tbody>
</table>

PORT:
<table>
<thead>
<tr>
<th>INF NUMBER</th>
<th>PORT NAME</th>
<th>LINK</th>
<th>HPR</th>
<th>SERVICE</th>
<th>ANY</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>TR000</td>
<td>IBMTRNET</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>

**** < This is the port that will get backed up

1  PPP001  PPP  YES | YES | YES |
2  SS       SDLC  NO | YES | YES |
3  SDLC     SDLC  NO | YES | NO  |
4  PPP      PPP  YES | YES | NO  |
5  TR005    IBMTRNET | YES | YES |
254 DLS     NO | YES | NO  |
17  PPP017  PPP  YES | YES | YES |
9  PPP009   PPP  YES | YES | YES |

STATION:
<table>
<thead>
<tr>
<th>STATION NAME</th>
<th>PORT NAME</th>
<th>DESTINATION</th>
<th>HPR</th>
<th>ALLOW</th>
<th>ADJ NODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TONN1</td>
<td>TR000</td>
<td>0004AC4E7505</td>
<td>YES</td>
<td>YES</td>
<td>1</td>
</tr>
<tr>
<td>TONN2</td>
<td>TR000</td>
<td>5500200004020</td>
<td>YES</td>
<td>YES</td>
<td>1</td>
</tr>
<tr>
<td>TONN9</td>
<td>TR000</td>
<td>0004AC4E9510</td>
<td>YES</td>
<td>YES</td>
<td>1</td>
</tr>
<tr>
<td>TOPC4</td>
<td>TR000</td>
<td>0004AC9416B4</td>
<td>YES</td>
<td>YES</td>
<td>1</td>
</tr>
<tr>
<td>TOVTAM1</td>
<td>TR000</td>
<td>400000003888</td>
<td>YES</td>
<td>YES</td>
<td>1</td>
</tr>
</tbody>
</table>

**** < this linkstation will get backed up

<table>
<thead>
<tr>
<th>STATION NAME</th>
<th>PORT NAME</th>
<th>DESTINATION</th>
<th>HPR</th>
<th>ALLOW</th>
<th>ADJ NODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TONN35</td>
<td>PPP001</td>
<td>000000000000</td>
<td>YES</td>
<td>YES</td>
<td>0</td>
</tr>
<tr>
<td>TO15DOD</td>
<td>PPP009</td>
<td>000000000000</td>
<td>YES</td>
<td>NO</td>
<td>0</td>
</tr>
</tbody>
</table>

LU NAME:
<table>
<thead>
<tr>
<th>LU NAME</th>
<th>STATION NAME</th>
<th>CP NAME</th>
</tr>
</thead>
</table>

APPN config>ex
Config>
*logout
Connection closed.

Note:
1  WAN restoral is enabled on both sides.
2  Port that will get backed up
3  Link station that will get backed up

Configuring V.25 bis

The following is a sample V.25 bis configuration that could be used when APPN traffic uses PPP over V.25 bis:

Config> list device
Ifc 0 Token Ring  CSR 6000000, vector 28
Ifc 1 WAN PPP    CSR 81620, CSR2 00D00, vector 93
Ifc 2 WAN V.25bis CSR 81640, CSR2 00E00, vector 92
Config> set data v25 2.
Config> list device
Ifc 0 Token Ring                CSR 6000000, vector 28
Ifc 1 WAN PPP                   CSR 81620, CSR2 80000, vector 93
Ifc 2 WAN V.25bis              CSR 81640, CSR2 80000, vector 92

Config> add v25
Assign address name (1-23) chars []? brown
Assign network dial address (1-30 digits) []? 555-1211
Assign address name (1-23) chars []? gray
Assign network dial address (1-30 digits) []? 555-1212
Config> list v25
Address assigned name  Network Address
--------------------- ---------------
brown 555-1211
gray 555-1212

Config> add device dial
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use net 3 command to configure circuit parameters
Config> net 3
Circuit configuration
Circuit config: 3>list all.
Base net = 0
Destination name =
Circuit priority = 8
Outbound calls = allowed
Inbound calls = allowed
Idle timer = 60 sec
SelfTest Delay Timer = 150 ms

Circuit config: 3>set net
Base net for this circuit [0]? 2
Circuit config: 3>set idle 0
Circuit config: 3>set dest
Assign destination address name []? brown
Circuit config: 3>list all

Base net = 2
Destination name = brown
Circuit priority = 8
Destination address: subaddress = 555-1211
Outbound calls = allowed
Inbound calls = allowed
Idle timer = 0 (fixed circuit)
SelfTest Delay Timer = 150 ms

Circuit config: 3>ex
Config> net 2
V.25bis Data Link Configuration
V25bis Config> list all
V.25bis Configuration
Local Network Address Name = Unassigned
No local addresses configured
Non-Responding addresses:
Retries = 1
Timeout = 0 seconds
Call timeouts:
Command Delay = 0 ms
Connect = 60 seconds
Disconnect = 2 seconds
Cable type = RS-232 DTE
Speed (bps) = 9600
V25bis Config> set local
Local network address name []? gray
V25bis Config> list all
V.25bis Configuration
Using APPN

Local Network Address Name = gray
Local Network Address = 555-1212

Non-Responding addresses:
Retries = 1
Timeout = 0 seconds

Call timeouts:
Command Delay = 0 ms
Connect = 60 seconds
Disconnect = 2 seconds

Cable type = RS-232 DTE
Speed (bps) = 9600
V25bis Config>

Note:
1. A non-zero value for Idle Timer results in a dial-on-demand link
2. A zero value results in a leased link

Configuring V.34

The following is a sample V.34 configuration that could be used when APPN traffic uses PPP over V.34:

Config> list device
Ifc 0 Token Ring
Ifc 1 WAN PPP
Ifc 2 WAN PPP
Config> set data v34
Config> list device
Ifc 0 Token Ring
Ifc 1 WAN PPP
Ifc 2 WAN PPP

Config> add v34
Assign address name [1-23] chars []? brown
Assign network dial address [1-30 digits] []? 555-1211
Config> add v34
Assign address name [1-23] chars []? gray
Assign network dial address [1-30 digits] []? 555-1212
Config> list v34

Address assigned name Network Address
--------------------- ---------------
default_address 9999999
brown 555-1211
grey 555-1212

Config> add device dial
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters

Config> net 3
Circuit configuration
Circuit config: 3> set all
Base net = 0
Destination name =
Circuit priority = 8
Outbound calls = allowed
Inbound calls = allowed
Idle timer = 60 sec
Self Test Delay Timer = 150 ms

Circuit config: 3> set net
Base net for this circuit [0]? 2
Circuit config: 3> set idle 0
Circuit config: 3> set dest
Assign destination address name []? brown
Circuit config: 3> set all
Base net = 2
Destination name = brown
Circuit priority = 8
Destination address: subaddress = 555-1211
Outbound calls = allowed
Inbound calls = allowed
Idle timer = 0 (fixed circuit)
SelfTest Delay Timer = 150 ms

Circuit config: 3>ex
Config>net 2
V.34 Data Link Configuration
V.34 System Net Config 2>list all
V.34 System Net Configuration:
Local Network Address Name = default_address
Local Network Address = 9999999
Non-Responding addresses:
Retries = 1
Timeout = 0 seconds
Call timeouts:
Command Delay = 0 ms
Connect = 60 seconds
Disconnect = 2 seconds
Modem strings:
Initialization string = at&f&s1l1&d2&c1x3
Speed (bps) = 115200

V.34 System Net Config 2>set local
Local network address name []? gray
V.34 System Net Config 2>list all
V.34 System Net Configuration:
Local Network Address Name = gray
Local Network Address = 555-1212
Non-Responding addresses:
Retries = 1
Timeout = 0 seconds
Call timeouts:
Command Delay = 0 ms
Connect = 60 seconds
Disconnect = 2 seconds
Modem strings:
Initialization string = at&f&s1l1&d2&c1x3
Speed (bps) = 115200

Notes:
1. A non-zero value for Idle Timer results in a dial-on-demand link
2. A zero value results in a leased link

Configuring APPN Over ATM

The following sample configures APPN over ATM.

Notes:
1. When PVCs are configured, the link station must be defined on both APPN nodes wanting to use the PVC. The link station must be defined with Activate link automatically= yes.
2. When parallel TGs over ATM are configured, the adjacent node name and TG number must be defined in both nodes for each link station.
Using APPN

Note: When defining parallel TGs if using dynamic TG number assignment, either ALL of the links or NONE of the links must be defined between the two nodes.

```
add po
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING, (S)DLC, (X)25, (D)Ls,w,(A)TM, (IP) [ ]? atm 1
Interface number (Default 0): [0]?
Port name (Max 8 characters) [ATM006]?

WARNING!! You are changing an existing record.
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o [Y]?
Maximum BTU size (768-2048) [2048]?
Percent of link stations reserved for incoming calls (0-100) [0]?
Percent of link stations reserved for outgoing calls (0-100) [0]?
Local ATM Address (hex) [99998888777766]?
Local SAP address (04-EC) [4]?
Enable Incoming Calls (Y)es (N)o [N]?
ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
Shareable Connection Network Traffic (Y)es (N)o [N]?
Shareable Other Protocol Traffic (Y)es (N)o [N]?
Broadband Bearer Class: 0 = CLASS_A, 1 = CLASS_C, 2 = CLASS_X [2]?
Best Effort Indicator (Y)es (N)o [N]?
Forward Traffic Peak Cell Rate (1-16777215) [131750]?
Forward Traffic Sustained Cell Rate (1-16777215) [131750]?
Forward Traffic Tagging (Y)es (N)o [Y]?
Forward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2, 3 = CLASS_3, 4 = CLASS_4 [0]?
Backward Traffic Peak Cell Rate (1-16777215) [460800]?
Backward Traffic Sustained Cell Rate (1-16777215) [39168]?
Backward Traffic Tagging (Y)es (N)o [Y]?
Backward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2, 3 = CLASS_3, 4 = CLASS_4 [0]?
Call out anonymously (Y)es (N)o [N]?
LDAP Retry Count (1-255) [3]?
LDAP Timer Period (1-255 seconds) [1]?
Limited resource timer for HPR (1-2160000 seconds) [180]?
Would you like TG characteristics updated to recommended values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

```
nada205 APPN config> add li atm006 2
APPN Station
Station name (Max 8 characters) [ ]? tograya
WARNING!! You are changing an existing record.
Limited resource: (Y)es (N)o [N]?
Activate link automatically (Y)es (N)o [Y]?
Virtual Channel Type (0 = PVC, 1 = SVC) [0]?
Destination ATM Address [39999999999999000999990103168902259411]?
VPI (0-255) [0]?
VCI (0-65535) [70]?
ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
Shareable Connection Network Traffic (Y)es (N)o [N]?
Shareable Other Protocol Traffic (Y)es (N)o [N]?
Remote SAP (04-EC) [4]?
Adjacent node type: 0 = APPN network node, 1 = APPN end node or Unknown node type, 2 = LEN end node [0]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
LDAP Retry Count (1-255) [3]?
LDAP Timer Period (1-255 seconds) [1]?
Would you like TG characteristics updated to recommended values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```
nada205 APPN config>add link atm006
APPN Station
Station name (Max 8 characters) [ ]? tograya
WARNING!! You are changing an existing record.
Limited resource: (Y)es (N)o [N]?
Activate link automatically (Y)es (N)o [Y]?
Virtual Channel Type (0 = PVC , 1 = SVC) [0]? 1
Destination ATM Address [3999999999999903168902259411]? /SF580000
/4/SF590000
Limited resource: (Y)es (N)o [N]?
Best Effort Indicator (Y)es (N)o [N]?
Forward Traffic Peak Cell Rate (1-16777215) [30000]? 30000
Forward Traffic Sustained Cell Rate (1-16777215) [20000]? 20000
Forward Traffic QOS Class: 0 = CLASS_A, 1 = CLASS_C, 2 = CLASS_X [2]?
Backward Traffic Peak Cell Rate (1-16777215) [30000]? 30000
Backward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2, 3 = CLASS_3, 4 = CLASS_4 [0]?
Call out anonymously (Y)es (N)o [N]?
ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
Shareable Connection Network Traffic (Y)es (N)o [N]?
Shareable Other Protocol Traffic (Y)es (N)o [N]?
Remote SAP(04-EC) [4]?
Adjacent node type: 0 = APPN network node, 1 = APPN end node or Unknown node type, 2 = LEN end node [0]?
TG Number (0-20) [0]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
LDLC Retry Count(1-255) [3]? 3
LDLC Timer Period(1-255 seconds) [1]? 1
Would you like TG characteristics updated to recommended values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

nada205 APPN config>

Notes:
1. Define an APPN port with link type ATM
2. Define an APPN link station
3. Define a PVC
4. Define an SVC

Configuring APPN Using SDLC

APPN supports the following SDLC stations:
- Primary point-to-point
- Secondary point-to-point
- Negotiable point-to-point
- Primary multipoint
- Secondary point-to-point (multi-APPN link stations)

Using the talk 5 command interface for SDLC, you can:
- Enable/disable a SDLC link
- Update SDLC station parameters.

In order to activate an APPN connection to the remote SDLC link station, you must configure and activate the APPN SDLC link station in the router. This enables the APPN link station in the router to receive an activation XID from the remote SDLC link station. This is different from other DLC types, such as Token ring or Ethernet, whose APPN link stations do not need to be explicitly defined for APPN in the router since APPN has the capability to dynamically define these types of link stations.
Using APPN

Refer to the Software User’s Guide for additional information about SDLC network layer configuration.

***********************************************************************
* The following examples show how to configure different SDLC stations. *
***********************************************************************
*Configuring a Primary Point-To-Point SDLC Station:*

Config> set data sdlc 1

SDLC user configuration
SDLC 1 Config> set link role primary
SDLC 1 Config> list link

Link configuration for: LINK_1 (ENABLED)

Role: PRIMARY Type: POINT-POINT
Duplex: FULL Modulo: 8
Idle state: FLAG Encoding: NRZ
Clocking: INTERNAL Frame Size: 2048
Speed: 64000 Group Poll: 00
Cable: RS-232 DCE

Timers: XID/TEST response: 2.0 sec
        SNRM response: 2.0 sec
        Poll response: 0.5 sec
        Inter-poll delay: 0.2 sec
        RTS hold delay: DISABLED
        Inter-frame delay: DISABLED
        Inactivity timeout: 30.0 sec

Counters: XID/TEST retry: 8
          SNRM retry: 6
          Poll retry: 10

SDLC 1 Config> ex

Config> CTRL p

* restart

Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6

Config> appn

APPN user configuration
APPN config> add port sdlc

APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?  
Enable APPN on this port (Y)es (N)o [Y]?  
Port Definition
Service any node: (Y)es (N)o [Y]?  
Edit TG Characteristics: (Y)es (N)o [N]?  
Write this record? [Y]?  
The record has been written.

APPN config> list port sdlc001

PORT:  
Interface number(DLSw = 254): 1
PORT enable: YES
Service any node: YES
Link Type: SDLC
MAX BTU size: 2048
MAX number of Link Stations: 1
Percent of link stations reserved for incoming calls: 0
Percent of link stations reserved for outgoing calls: 0
Cost per connect time: 0
Cost per byte: 0
Security:(0 = Nonsecure, 1 = Public Switched Network
            2 = Underground Cable, 3 = Secure Conduit,
            4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
               3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 2
Effective capacity: 45
First user-defined TG characteristic: 128
Second user-defined TG characteristic: 128
Third user-defined TG characteristic: 128

APPN config> add link sdlc001

APPN Station
Station name (Max 8 characters) [ ]? TOSECSTN
Activate link automatically (Y)es (N)o [Y]?
Using APPN

Station address(1-fe) [C1]?
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config> list link toseeccstn

STATION:
    Port name: SDLC001
    Interface number(DLSw = 254): 1
    Link Type: SDLC
    Station address: C1
    Activate link automatically: YES
    Allow CP-CP sessions on this link: YES
    CP-CP session level security: NO
    Fully-qualified CP name of adjacent node:
    Encryption key: 0000000000000000
    Use enhanced session security only: NO
    Cost per connect time: 0
    Cost per byte: 0
    Security: 0 = Nonsecure, 1 = Public Switched Network
            2 = Underground Cable, 3 = Secure Conduit,
            4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
    Propagation delay: 0 = Minimum, 1 = Lan, 2 = Telephone,
            3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 2
    Effective capacity: 45
    First user-defined TG characteristic: 128
    Second user-defined TG characteristic: 128
    Third user-defined TG characteristic: 128
    Predefined TG number: 0

APPN config> act

***********************************************************************
* Configuring a Secondary Point-To-Point SDLC Station:               
*--------------------------------------------------------------------
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role secondary
SDLC 1 Config> set link cable rs-232 dte
SDLC 1 Config> list link **(will show link configuration)**

SDLC 1 Config> add station
Enter station address (in hex) [C1]?
Enter station name [SDLC_C1]?
Include station in group poll list ([Yes] or No): no
Enter max packet size [2048]?
Enter receive window [7]?
Enter transmit window [7]?

SDLC 1 Config> list station all
Address Name Status Max BTU Rx Window Tx Window
--------- -------- ---------- ------- --------- ---------
C1 SDLC_C1 ENABLED 2048 7 7

SDLC 1 Config> ex
Config> CTRL p
* restart
Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6
Config> p appn
APPN user configuration
APPN config> add port sdlc
APPN Port
    Interface number(Default 0): [0] ? 1
    Port name (Max 8 characters) [SDLC001]?
    Enable APPN on this port (Y)es (N)o [Y]?
    Port Definition
    Service any node: (Y)es (N)o [Y]?
    Edit TG Characteristics: (Y)es (N)o [N]?
    Write this record? [Y]?
The record has been written.

APPN config> list port sdlc001 **(will show port definitions)**
APPN config> add link sdlc01
APPN Station
    Station name (Max 8 characters) [ ]? TOPRISTN
    Activate link automatically (Y)es (N)o [Y]?
    (Note: "Y" to accept activation from the primary or negotiable station)
Using APPN

Station address(1-fe) [C1]?  
Adjacent node type: 0 = APPN network node, 1 = APPN end node  
2 = LEN end node, 3 = PU 2.0 node [0]?  
Edit Dependent LU Server: (Y)es (N)o [N]?  
Allow CP-CP sessions on this link (Y)es (N)o [Y]?  
CP-CP session level security (Y)es (N)o [N]?  
Configure CP name of adjacent node: (Y)es (N)o [N]?  
Edit TG Characteristics: (Y)es (N)o [N]?  
Write this record? [Y]?

The record has been written.

APPN config>list link topristn **(will show link station definitions)
APPN config>act

***********************************************************************
* Configuring a Negotiable Point-To-Point SDLC Station: 3
***********************************************************************

Config> set data sdlc 1
Config> m 1
SDLC user configuration
SDLC 1 Config> set link role negotiable
SDLC 1 Config>list link **(will show link configuration)
SDLC 1 Config>ex
Config> CTRL p
* restart

Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?  
Enable APPN on this port (Y)es (N)o [Y]?  
Port Definition  
Service any node: (Y)es (N)o [Y]?  
Edit TG Characteristics: (Y)es (N)o [N]?  
Write this record? [Y]?

The record has been written.

APPN config>list port sdlc001 **(will show port definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) []? TOREMSTN  
Station address(1-fe) [C1]?  
(Non: CI may be used if this station is becoming a secondary station)  
Adiacent node type: 0 = APPN network node, 1 = APPN end node  
2 = LEN end node, 3 = PU 2.0 node [0]?  
Edit Dependent LU Server: (Y)es (N)o [N]?  
Allow CP-CP sessions on this link (Y)es (N)o [Y]?  
CP-CP session level security (Y)es (N)o [N]?  
Configure CP name of adjacent node: (Y)es (N)o [N]?  
Edit TG Characteristics: (Y)es (N)o [N]?  
Write this record? [Y]?

The record has been written.

APPN config>list link toremstn **(will show link station definitions)
APPN config>act

***********************************************************************
* Configuring a Primary Multipoint SDLC Station: 4
***********************************************************************

Config> set data sdlc 1
Config> m 1
SDLC user configuration
SDLC 1 Config> set link role primary
SDLC 1 Config> set link type multipoint
SDLC 1 Config>list link **(will show link configuration)
SDLC 1 Config>ex
Config> CTRL p
* reload

Are you sure you want to reload the gateway? (Yes or [No]): yes

* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?  
Enable APPN on this port (Y)es (N)o [Y]?  
Port Definition  
Service any node: (Y)es (N)o [Y]?
Maximum number of link stations (1-127) ? 2
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config> list port sdlc001
**(will show port definitions)

APPN config> add link sdlc001

APPN Station
Station name (Max 8 characters) [ ]? TOSTNC1
Activate link automatically (Y)es (N)o [Y]?
Station address(1-fe) [C1]?
(Note: C1 must match to the remote secondary station)
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config> list port sdlc001
**(will show port definitions)

APPN Station
Station name (Max 8 characters) [ ]? TOSTNC1
Activate link automatically (Y)es (N)o [Y]?
Station address(1-fe) [C1]?
(Note: C1 must match to the remote secondary station)
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config> list port sdlc001
**(will show port definitions)

APPN Station
Station name (Max 8 characters) [ ]? TOSTNC2
Activate link automatically (Y)es (N)o [Y]?
Station address(1-fe) [C2]?
(Note: C2 must match to the remote secondary station)
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config> list port sdlc001
**(will show port definitions)

APPN Station
Station name (Max 8 characters) [ ]? TOSTNC2
Activate link automatically (Y)es (N)o [Y]?
Station address(1-fe) [C2]?
(Note: C2 must match to the remote secondary station)
Using APPN

| Adjacent node type: 0 = APPN network node, 1 = APPN end node |
| 2 = LEN end node, 3 = PU 2.0 node [0] |
| Edit Dependent LU Server: (Y)es (N)o [N] |
| Allow CP-CP sessions on this link (Y)es (N)o [Y] |
| CP-CP session level security (Y)es (N)o [N] |
| Configure CP name of adjacent node: (Y)es (N)o [N] |
| Edit TG Characteristics: (Y)es (N)o [N] |
| Write this record? [Y] |

APPN config>
list link tostnc1 **(will show link station definitions)
APPN config>
add link sdlc001
APPN Station
Station name (Max 8 characters) []? TOSTNC2
Activate link automatically (Y)es (N)o [Y]?
Station address(1-fe) [C2]?
(Note: C2 must match to the remote secondary station)
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
list link tostnc2 **(will show link station definitions)
APPN config>

Note:
1. Configuring a primary point-to-point SDLC station
2. Configuring a secondary point-to-point SDLC station
3. Configuring a negotiable point-to-point SDLC station
4. Configuring a primary multipoint SDLC station
5. Configuring secondary point-to-point (multi APPN link stations)

Configuring APPN Over X.25

This example shows APPN configuration for an X.25 port and two link stations. One
link station is a PVC and one is an SVC. The SVC is configured as a limited
resource. The SVC will be activated when needed and brought down when it is not.

Boats Config>
appn
APPN user configuration
Boats APPN config>
add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING, (S)DLC, (X)25, (D)LsW, (A)TM, (IP)[ ]? x
Interface number(Defa ult 0):[0]?: 2
Port name (Max 8 characters)[X25002]?
Enable APPN on this port (Y)es (N)o[Y]?
Port Definition
Service any node: (Y)es (N)o[Y]?
Maximum number of link stations (1-65535)[65535]?
Percent of link stations reserved for incoming calls (0-100)[0]?
Percent of link stations reserved for outgoing calls (0-100)[0]?
Edit TG Characteristics: (Y)es (N)o[N]?
Write this record?[Y]?
The record has been written.

Boats APPN config>
add link
APPN Station
Port name for the link station[ ]? x25002
Station name (Max 8 characters)[ ]? x25svc1
Limited resource: (Y)es (N)o[N]?
Y
Activate link automatically (Y)es (N)o[N]?
Link Type (0 = PVC, 1 = SVC)[0]?: 1
DTE Address [0]?: 2222
Adjacent node type: 0 = APPN network node, 1 = APPN end node or Unknown node type
2 = LEN end node, 3 = PU 2.0 node[1]?
Edit Dependent LU Server: (Y)es (N)o[N]?
Allow CP-CP sessions on this link (Y)es (N)o[Y]?
N
CP-CP session level security (Y)es (N)o[N]?
Configure CP name of adjacent node: (Y)es (N)o[N]?
Using APPN

Chapter 1. Using APPN

65
Using APPN

Encryption key: 0000000000000000
Use enhanced session security only: NO
Cost per connect time: 0
Cost per byte: 0
Security: (0 = Nonsecure, 1 = Public Switched Network,
    2 = Underground Cable, 3 = Secure Conduit,
    4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
Propagation delay: (0 = Minimum, 1 = Lan, 2 = Telephone,
    3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3
Effective capacity: 45
First user-defined TG characteristic: 128
Second user-defined TG characteristic: 128
Third user-defined TG characteristic: 128
Predefined TG number: 0

Boats APPN config>li all

NODE:
NETWORK ID: STFNET
CONTROL POINT NAME: BOATS
XID: 00000
APPN ENABLED: YES
MAX SHARED MEMORY: 4096
MAX CACHED: 4000

DLUR:
DLUR ENABLED: NO
PRIMARY DLUS NAME:

CONNECTION NETWORK:
CN NAME    LINK TYPE PORT INTERFACES
-------------------------------------------------------------

COS:
COS NAME
--------
BATCH
BATCHSC
CONNECT
INTER
INTERSC
CPSVCMG
SNASVCMG

MODE NAME COS NAME
---------------------

PORT:

<table>
<thead>
<tr>
<th>INF</th>
<th>PORT NAME</th>
<th>LINK TYPE</th>
<th>HPR</th>
<th>SERVICE</th>
<th>ANY</th>
<th>PORT ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>X25002</td>
<td>X25</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>TR005</td>
<td>IBMTRNET</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>

STATION:
STATION NAME PORT DESTINATION HPR ALLOW ADJ NODE
NAME NAME ADDRESS ENABLED CP-CP TYPE
-------------------------------------------------------------
X25SVC1  X25002  2222 NO NO 1
X25PVC1  X25002  1 NO YES 1

LU NAME:

LU NAME STATION NAME CP NAME
------------------------------------------------------------

Boats APPN config>ex

Boats Config>n 2
X.25 User Configuration
Boats X.25 Config>li all

X.25 Configuration Summary

Node Address: 1111
Max Calls Out: 4
Inter-Frame Delay: 0 Encoding: NRZ
Speed: 64000 Clocking: External
MTU: 2048 Cable: V.35 DTE
Lower DTR: Disabled
Default Window: 2 SVC Idle: 30 seconds
National Personality: GTE Telenet (DCE)
PVC
low: 1 high: 4
Inbound low: 0 high: 0
Two-Way low: 10 high: 20
Outbound low: 0 high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400
X.25 National Personality Configuration

Follow CCITT: on  OSI 1984: on  OSI 1988: off
Request Reverse Charges: off  Accept Reverse Charges: off
Frame Extended seq mode: off  Packet Extended seq mode: off
Incoming Calls Barred: off  Outgoing Calls Barred: off
Throughput Negotiation: off  Flow Control Negotiation: off
Suppress Calling Addresses: off
DDN Address Translation: off
Call Request Timer: 20 decaseconds
Clear Request Timer: 18 decaseconds (1 retries)
Reset Request Timer: 18 decaseconds (1 retries)
Restart Request Timer: 18 decaseconds (1 retries)
Min Recall Timer: 10 seconds
Min Connect Timer: 90 seconds
Collision Timer: 10 seconds
T1 Timer: 4.00 seconds  N2 timeouts: 20
T2 Timer: 0.00 seconds  DP Timer: 500 milliseconds
Standard Version: 2  Network Type: CCITT
Disconnect Procedure: passive
Window Size  Frame: 7  Packet: 2
Packet Size  Default: 128  Maximum: 256

X.25 protocol configuration

<table>
<thead>
<tr>
<th>Prot</th>
<th>Window</th>
<th>Packet-size</th>
<th>Idle</th>
<th>Max</th>
<th>Station</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>-&gt; APPN</td>
<td>7</td>
<td>128</td>
<td>1024</td>
<td>0</td>
</tr>
</tbody>
</table>

X.25 PVC configuration

Prtcl  X.25 address  Active Enc  Window  Pkt_len  Pkt-chan
30  (APPN)  6666  NONE  2  128  1

X.25 address translation configuration

IF #  Prot #  Active Enc  Protocol  -> X.25 address
2  30 (APPN)  NONE  appn  -> 6666

Configuring APPN Over Frame Relay

The following example shows configuration of APPN over Frame Relay.

nada207 Config> p appn
APPN user configuration
nada207 APPN config> add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING, (S)DLC, (X)25, (D)Lsw, (A)TM, (IP) [ ]
f Interface number (Default 0): [0]? 4
Port name (Max 8 characters) [FR004]? 
Enable APPN on this port (Y)es (N)o [Y]? 
Port Definition
Service any node: (Y)es (N)o [Y]? 
High performance routing: (Y)es (N)o [Y]? 
Maximum BTU size (768-2048) [2048]? 
Percent of link stations reserved for incoming calls (0-100) [0]? 
Percent of link stations reserved for outgoing calls (0-100) [0]? 
Local SAP address (04-EC) [4]? 
Support bridged formatted frames: (Y)es (N)o [N]? 
Edit TG Characteristics: (Y)es (N)o [N]? 
Edit LLC Characteristics: (Y)es (N)o [N]? 
Edit HPR defaults: (Y)es (N)o [N]? 
Write this record? [Y]? 
The record has been written.
nada207 APPN config> add link
APPN Station
Port name for the link station []? fr004
Station name (Max 8 characters) []? tonn
Activate link automatically (Y)es (N)o [Y]? 
DLCI number for link (16-1007) [16]? 
Adjacent node type: 0 = APPN network node, 1 = APPN end node or Unknown node type, 2 = LEN end node, 3 = PU 2.0 node [1]? 0
High performance routing: (Y)es (N)o [Y]? 
Edit Dependent LU Server: (Y)es (N)o [N]? 
Allow CP-CP sessions on this link (Y)es (N)o [Y]? 
CP-CP session level security (Y)es (N)o [N]?
Using APPN

- Configure CP name of adjacent node: (Y)es (N)o [N]?
- Edit TG Characteristics: (Y)es (N)o [N]?
- Edit LLC Characteristics: (Y)es (N)o [N]?
- Edit HPR defaults: (Y)es (N)o [N]?
- Write this record? [Y]?

The record has been written.
nada207 APPN config>act
nada207 APPN config>exit
nada207 Config>write
Config Save: Using bank B and config number 2

Configuring APPN Over Frame Relay BAN

The following example shows configuration of APPN over Frame Relay BAN.

nada207 Config>p appn
APPN user configuration
nada207 APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)Lsw, (A)TM, (IP) [ ] ?f
Interface number (Default 0): [0] 4
Port name (Max 8 characters) [FR004]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
- Service any node: (Y)es (N)o [Y]?
- High performance routing: (Y)es (N)o [Y]?
- Maximum BTU size (768-2048) [2048]?
- Percent of link stations reserved for incoming calls (0-100) [0]?
- Percent of link stations reserved for outgoing calls (0-100) [0]?
- Local SAP address (04-EC) [4]?
- Support bridged formatted frames: (Y)es (N)o [N]?
- Boundary node identifier (hex-noncanonical) [4FFF00000000]?

41235fad
Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config>add link
APPN Station
Port name for the link station []? fr004
Station name (Max 8 characters) []? tonn
Activate link automatically (Y)es (N)o [Y]?
DLCI number for link (16-1007) [16]?
Support bridged formatted frames: (Y)es (N)o [N]?
MAC address of adjacent node (hex-noncanonical) [000000000000]?
3456
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type
2 = LEN end node, 3 = PU 2.0 node [1] 0
High performance routing: (Y)es (N)o [Y]?
Edit Dependent LU Server: (Y)es (N)o [N]?
- Allow CP-CP sessions on this link (Y)es (N)o [Y]?
- CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config>act
nada207 APPN config>exit
nada207 Config>write
Config Save: Using bank B and config number 2

Configuring Enterprise Extender Support for HPR Over IP

Using APPN

- Configure CP name of adjacent node: (Y)es (N)o [N]?
- Edit TG Characteristics: (Y)es (N)o [N]?
- Edit LLC Characteristics: (Y)es (N)o [N]?
- Edit HPR defaults: (Y)es (N)o [N]?
- Write this record? [Y]?

The record has been written.
nada207 APPN config>act
nada207 APPN config>exit
nada207 Config>write
Config Save: Using bank B and config number 2

Configuring Enterprise Extender Support for HPR Over IP

Using APPN
Using APPN

(S)DLC, (X)25, (D)LSw, (A)TM, (I)P []? ip
Port name (Max 8 characters) [IP255]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o [Y]?
Maximum BTU size (768-2048) [768]?
UDP port number for XID exchange (1024-65535) [11000]?
UDP port number for low priority traffic (1024-65535) [11004]?
UDP port number for medium priority traffic (1024-65535) [11003]?
UDP port number for high priority traffic (1024-65535) [11002]?
UDP port number for network priority traffic (1024-65535) [11001]?
IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
Local SAP address (04-EC) [4]?
LDLC Retry Count(1-255) [3]?
LDLC Timer Period(1-255 seconds) [15]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

****3.3.3.3 is the router's internal IP address
APPN config>add link
APPN Station
Port name for the link station []? ip255
Station name (Max 8 characters) []? tonn
Activate link automatically (Y)es (N)o [Y]?
IP address of adjacent node [0.0.0.0]? 3.3.3.3
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type [0]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Remote SAP(04-EC) [4]?
IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
LDLC Retry Count(1-255) [3]?
LDLC Timer Period(1-255 seconds) [15]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>

Configuring Connection Networks over HPR over IP

Configuring an Extended Border Node

Spurs APPN config>p app
Spurs APPN config=set node
Enable APPN (Y)es (N)o [N]? y
Network ID (Max 8 characters) [STFDDD3]?
Control point name (Max 8 characters) [SPURS]?
Enable branch extender or extended border node
Using APPN

(0=Neither, 1=Branch Extender, 2=Border Node)[2]?
Subnet visit count(1-255) [3]?
Cache searches for (0-255) minutes [8]?
Maximum number of searches to cache (0(unlimited)-32765) [0]?
Dynamic routing list updates (0=None, 1=Full, 2=Limited) [1]?
Enable routing list optimization (Y)es (N)o [Y]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
Spurs APPN config=act
APPN is not currently active
Spurs APPN config=add rout
Routing list name []? list1
Subnet visit count (1-255) [3]?
Dynamic routing list updates (0=None, 1=Full, 2=Limited) [1]?
Enable routing list optimization (Y)es (N)o [Y]?
Destination LUs found via this list:
(netID.LUname)[ ]? net1=net1
(netID.LUname)[ ]?
Routing CPs (with optional subnet visit count):
(netID.CPname ?) [ 3]? net2.router2
(netID.CPname ?) [ 3]?
Write this record? (Y)es (N)o [Y]?
The record has been written.

Spurs APPN config=add cos
COS mapping table name []? cos1
Non-native network (netID.CPname) []?net2.router2
Non-native network (netID.CPname) []?
Native and non-native COS name pair [ ]? #inter
Native and non-native COS name pair [ ]?
Write this record? (Y)es (N)o [Y]?
The record has been written.
Chapter 2. Using TN3270

This section introduces TN3270 and summarizes the TN3270E server function implemented in IBM routers. It includes the following topics:

- "Overview"
- "General TN3270E Server Configuration" on page 75
- "Example Configurations" on page 87

Overview

Many companies today are consolidating their WAN traffic onto IP-only backbones. Companies are also simplifying their workstation configurations and attempting to run only the TCP/IP protocol stack at the desktop. However, most of these companies still require access to SNA application hosts.

TN3270 meets these requirements by allowing you to run IP from the desktop over the network and attach to your SNA host through a TN3270 server. The clients connect to the server using a TCP connection. The server provides a gateway function for the downstream TN3270 clients by mapping the client sessions to SNA dependent LU-LU sessions that the server maintains with the SNA host. The TN3270 server handles the conversion between the TN3270 data stream and an SNA 3270 data stream.

To deploy a TN3270 solution, you install TN3270 client software on desktop workstations and TN3270 server software in one of several places discussed below. Client software is available from IBM and many other vendors, and runs on top of the TCP/IP stack in the workstation. A given client product provides one of two possible levels of standards support:

- Base TN3270 client
  These clients conform to RFC 1576 (TN3270 Current Practices) and/or RFC 1646 (TN3270 Extensions for LU name and Printer Selection).

- TN3270E client
  These clients conform to RFC 1647 (TN3270 Enhancements), and RFC 2355 (TN3270 Enhancements).

A server implementation that can support TN3270E clients is called a TN3270E server.

Placement of the TN3270 Server Function

The TN3270 server function can be placed in a variety of products and positions within a network, including:

- In the SNA host itself
  IBM and several other vendors provide host TN3270 server software that sits on top of the host TCP/IP stack and connects within the host to VTAM.

- In a router or in the network
  IBM and other vendors provide TN3270 server function in networking hardware products. You can place these products directly adjacent to the SNA host, or at any position in the network where you have SNA connectivity to the host. If you

---

3. You can also find small, dedicated TN3270 client products that represent printers.
are using IBM routers and your host is running APPN, you can use Enterprise Extender technology to place the server at any position where you have IP connectivity to the host.

- In a software product in the network
  IBM and other vendors provide TN3270 server software products that you install on mid-range servers that use operating systems such as AIX, OS/2, or Windows/NT. You can place these products at any position in the network where you have SNA connectivity to the application host.

The choice of TN3270 server product and network position is a complex one, involving such factors as:

- Host capacity and cycle impact
- Price for performance and capacity
- Availability
- Impact of server failure
- Scalability

IBM routers provide a high-performing TN3270E server implementation that scales to large networks. By combining this implementation with the Network Dispatcher feature, you can implement server redundancy and load sharing in large TN3270 installations. You can also place an IBM router out into an SNA or IP network away from the data center and get the same advantages of scalability, incremental addition, and reduced impact of server failure.

**TN3270E Server Function**

**Standards Compliance**
The IBM router implementation of TN3270E server supports these RFCs:

- **RFC 1576**  TN3270 Current Practices
- **RFC 1646**  TN3270 Extensions for LU names and Printers
- **RFC 1647**  TN3270 Enhancements
- **RFC 2355**  TN3270 Enhancements (obsoletes RFC 1647)

It can handle both base TN3270 and TN3270E clients at the same time.

**Host Connectivity**
The path from a TN3270 client to the SNA host consists of two pieces:

- A TCP connection over IP from the client to the server
- An SNA LU-LU session from the server to the host

The form of the SNA connection from the server to the host depends on how the server represents PUs and dependent LUs. When you are using an IBM router as your TN3270 server, you can configure either of two different ways to establish links and represent PUs and LUs to VTAM:

- Using SNA subarea links
  You configure this way when you are not running APPN at the host (even though the router is still APPN-capable). You configure a separate DLC-layer link to the host for every PU (maximum of 255 LUs per PU). Multiple PUs require multiple parallel host links. SNA frames arriving at the router on one of these links flow directly to the corresponding internal PU.

  Subarea host links must be a single DLC-layer hop to the product providing the SNA subarea boundary function. Typically, this product is either NCP running in a FEP (front-end processor), or is VTAM itself in the host. The subarea link from
the router can traverse bridges or other DLC-layer forwarding mechanisms (such as protocol converters or external DLSw routers). IBM routers support the following link types for subarea host attachment (where the link type is available on a given router product):

- Token-Ring: physical, ATM LAN emulation, or channel LSA
- Ethernet: physical, ATM LAN emulation, or channel LSA
- FDDI: physical only
- Frame relay PVCs: bridged or routed RFC 1490/2427 formats
- DLSw (note that local DLSw can provide access to SDLC and QLLC upstream links)

- Using an APPN Dependent LU Requester (DLUR) link

You configure this way when you are running APPN with its Dependent LU Server (DLUS) function at the host. At the DLUR router, you configure one or more DLUS(es) to support the TN3270 internal dependent PUs (and any external dependent PUs that may exist). A router running DLUR can either be directly connected to the DLUS host, or can be located remotely across several APPN links. Only one link is required to carry the first or only hop of the DLUR-DLUS "pipe", even if you are defining multiple local PUs (to have more than 255 total LUs). SNA frames arriving on the DLUR-DLUS pipe flow to the DLUR function, which redirects them to the correct internal or external PU.

When you are using DLUR, you can route through an APPN network using either ISR or HPR routing to reach the host. IBM routers support the following link types as the “first hop” APPN link to the host (where the link type is available on a given router product):

- Token-Ring: physical, ATM LAN emulation, or channel LSA
- Ethernet: physical, ATM LAN emulation, or channel LSA
- FDDI: physical only
- Frame relay PVCs: bridged or routed RFC 1490/2427 formats
- ATM (native, not LAN emulation): HPR only
- Channel MPC+: HPR only
- PPP
- SDLC: ISR only
- X.25: ISR only
- DLSw: ISR only
- IP (Enterprise Extender): HPR only

Note especially that when using DLUR and HPR routing, you can place a TN3270E server across an IP network from the SNA application host. Enterprise Extender maintains session-level class of service and transmission priority across the IP network.

If an LU-LU session exists when the TN3270 client disconnects from the TN3270 server, an UNBIND or TERM-SELF request will be sent to the host to terminate the LU-LU session. The default is UNBIND cleanup. The local PU or link station must be configured appropriately for TERM-SELF to flow. TERM-SELF should be configured if a session manager (front end) application is being used to get to applications such as TSO or CICS.

**SNA Management Support**

From a VTAM or NetView/390 operator console, you can control the links, PUs, and LUs involved with TN3270. For LUs, when a TN3270 client connects in, the router reports the client’s IP address and TCP port number to VTAM on its session.
Using TN3270

activation flows (via CV64). VTAM console display commands such as "/D NET,ID=(lu name),E" have the ability to display the TCP/IP address information associated with particular LUs. This permits problem determination for TN3270 clients from a VTAM operator console.

VTAM support for receiving and displaying client IP addresses is in CS for OS/390 V2R6 base code. It was also PTF'd to CS for OS/390 V2R5 (VTAM APAR OW31454, TCP/IP APAR PQ12574).

In addition to enabling this console support, APPN generates SNA alerts for a variety of error configurations, and can forward alerts from other SNA devices. There are no alerts specific to the TN3270 server function, but alerts that the router itself generates may relate to SNA resources involved with TN3270.

SNMP MIB and Trap Support
IBM routers support an Internet Draft version of both of these standard MIBs for TN3270 server function:

- TN3270 Base MIB (now RFC 2561)
- TN3270 Response Time MIB (now RFC 2562)

IBM router support for these MIBs includes the ability to:

- View server configuration, status, and statistics
- Set up client groups for response time collection
- View the mapping of LU names from VTAM name to local name to client IP address
- View the mapping of client IP addresses to VTAM LU names
- Collect response time data for current client groups

In addition, the following enterprise-specific MIB shows the reasons why clients were not able to successfully connect to the TN3270 server:

- IBM TN3270 Connection Rejection

These TN3270-related MIBs supplement the extensive IBM router MIB support for APPN and SNA resources.

TN3270 Host On-Demand Client Caching
Some IBM router products (currently the 2216 and 2212) support a "Web Server Cache" function, where they can sit in front of an HTTP server and offload the server by caching Web objects and serving them up to requesting clients. Among the objects these routers can cache are Java applets that provide TN3270 client function.

Host On-Demand (HOD) Client Caching allows one of these routers or the IBM Network Utility to cache TN3270 client function applets from an HOD host Web server and serve them to client browsers upon request. The browsers then launch the TN3270 terminal emulation applets. These applets connect to an SNA host either through the router’s TN3270 server function, or through some other TN3270 server.

Host On-Demand support is packaged with the TN3270 server function, but you configure the two independently. The router can cache HOD clients but not be configured as a TN3270 server. Likewise, the router can be a TN3270 server with no HOD caching enabled. The Web Server Cache router code loads that do not include TN3270 server function (only on 2216 and 2212) can also cache HOD client applets if so configured.
Because the HOD client cache function is completely separate from the Server function, it is not further discussed in this chapter. See the chapter entitled “Configuring and Monitoring IBM eNetwork Host On-Demand Client Cache” in the Using and Configuring Features publication, for more information on this function.

General TN3270E Server Configuration

This section covers general information about configuring TN3270 server support. For specific example configurations, see “Example Configurations” on page 87.

Loading the TN3270 Server Code

Depending on your router type and configuration method, you may have to take extra steps to load APPN and TN3270 code and be able to access their command-line configuration and monitoring prompts:

- Install a router code load that includes both APPN and TN3270. The protocols are loaded when the router boots.

For details about the load add command, see the chapter entitled “The CONFIG Process (CONFIG - Talk 6) and Commands” in the Software User’s Guide.

Configuring TN3270 under the APPN Protocol

In the IBM router implementation of TN3270 server, all SNA functions are bundled within the APPN protocol. This means that even when you are configuring SNA subarea host attachment and your SNA host is not running APPN, you must use the configuration and console services of the APPN protocol. In particular:

- You must go through the APPN protocol at the command line and at the Configuration Program to configure ports, links, and TN3270 server functions
- You must go through the APPN protocol at the command line to use TN3270 monitoring commands
- You must configure APPN at the node level

When you configure SNA subarea support, the router does in fact still function as an APPN network node, but only on links to other APPN nodes. If the only ports and links you configure are those for SNA subarea host attachment, then the APPN function itself does not run.

Server IP Address

To enable the TN3270 server function, you must configure an IP address to which the TN3270 clients will connect. The IBM router TN3270 implementation supports only a single server IP address (but multiple destination TCP ports). The address you configure for TN3270 must match one of the following addresses you configure for IP, otherwise TN3270 will not initialize.

- An interface address
  You can assign any number of addresses to an interface. The interface can be either physical or a virtual “loopback” interface. Physical interface addresses are active only when the associated interface is up, but loopback interface addresses are always active.
- The internal address
  This is a single address that represents the entire router and is active independent of the state of any particular interface.

When you choose the IP address for the TN3270 function, you must consider that administrative users also need to be able to establish regular Telnet sessions, to bring up remote router consoles.
Using TN3270

TN3270 is the same (23), so unless you want one or the other sets of users to use a non-default destination port, you must set aside different IP addresses for Telnet and TN3270 users.

If you are using router code V3.4 or higher, the recommended procedure is to define a loopback interface and use one of the IP addresses on that interface as your TN3270 server IP address. If you are using router code before V3.4, you need to choose either to use a physical interface address for TN3270 and leave the internal address for Telnet, or vice versa. One important consideration in this choice is whether you have multiple parallel TN3270 servers, each of which needs the same server address but different Telnet addresses for maintenance.

Server TCP Ports

When you configure the server IP address, you also specify a destination TCP port number to which the TN3270 clients will connect. You must provide at least one port number as part of server's general configuration (TN3270E config> set command, Configuration Program TN3270E Server/General panel). Optionally, you can configure additional TCP ports for the TN3270 server to “listen” on (TN3270E config> add port command, Configuration Program TN3270E Server/Ports panel).

The following are reasons you might want to configure more than one server TCP port:

- Segregate "E" and “non-E” clients
  The TN3270 protocol requires an E-capable server to initiate certain negotiations with clients. Some old non-E clients fail instead of simply ignoring these negotiations. You can configure the router so that it treats clients connecting to a given destination port as non-E clients, and does not send them the offending request. You then configure the non-E clients to attach to that port.

- Map clients to SNA resources using a port number
  Many clients cannot request an SNA resource by name, but they all connect to a destination TCP port. When you configure a destination port, you associate an LU pool with that port number (there is a global default pool if you do not specify a particular one). Clients that connect to this port and do not specify an LU name will be assigned an LU from this pool.

- Disable IP address mapping for some clients
  If you have globally enabled the mapping of client IP addresses to LU or LU pool names, the router chooses the LU using the IP address mapping rules rather than using the port to LU pool association. You may want to have a set of clients that are exempt from this mapping (note that clients who fail to match the configured mappings are refused a connection). You can configure a destination port so that when a client connects to that port, IP address mapping is ignored. When you select this option, the LU pool associated with that port is used instead to choose the LU.

- Map clients to SNA resources using port-specific IP address mapping
  If you have globally enabled the mapping of client IP addresses to LU or LU pool names, you may want to have different IP mapping rules apply to different sets of clients. When you configure an IP mapping table entry, you can specify a destination TCP port number (the default is “all ports”). When you do so, only the clients that connect to that port number are checked against that mapping entry.
Defining PUs

You must always define dependent PUs in the router, to contain the LUs that the router associates with incoming TN3270 client TCP connections. Each PU you define must have a corresponding PU definition in VTAM.

If you are using DLUR for your host connection, the internal PUs you define each appear to have an “inside the box” logical link to the DLUR function. This logical link is always active when APPN and TN3270 are active. DLUR may at the same time be serving other dependent PUs external to the router.

You need to define only as many PUs as you need to contain your LUs, where each PU can have 255 LUs. If you are defining more than one local PU, you distinguish them by specifying different local node IDs. To configure a local PU for DLUR using the command line, use the `add local-pu` command. From the Configuration Program, select Local PUs from under the TN3270E Server protocol in the Navigation window.

If you are using subarea links for your host connection, each link is bound to an associated internal PU. The router creates this internal PU automatically when you configure a subarea link; you do not explicitly configure internal PUs the way you do with DLUR. The link associated with each PU is a real external link which can go up or down. Some users distribute the LUs that are in a single pool across multiple subarea PUs, so that if one link fails there may be another available to service client reconnection attempts.

To configure a subarea link using the command line, use the `add link` command. Respond yes to the question “Solicit SSCP session?”, and no to the question “Does link support APPN function?” From the Configuration Program, select Interfaces from under the APPN protocol in the Navigation Window, then click on the Link stations column heading. If you are configuring more than one subarea link under the same physical port, you must enable that port to support multiple PUs. You distinguish the PUs by local node ID as well as by local addressing information such as the SAP address.

Defining LUs

When a TN3270 client is fully connected, its TCP connection is paired with an SNA LU representation in the server. VTAM also has a representation for the same LU. Each of these LU representations has a name, and it is possible but not necessary for the server LU name to match the VTAM LU name. Since a typical TN3270 configuration involves thousands of LUs to satisfy as many potential clients, various schemes have been developed to ease the burden of configuring LUs and to make it possible for the server and VTAM names to match.

The IBM router implementation of TN3270 server currently supports the following LU definition methods. See the sections that follow for a detailed description of each method. All these methods are available regardless of whether your host link attachment is DLUR or subarea.

- Static in the router, static in the host
  
  With this method, you configure LUs in the router either individually by name or in groups using name seeds. You define corresponding LUs in VTAM by hand using the same or different LU names. The PU ID and LU’s NAU addresses are what relate the router’s LUs to VTAM’s LUs.

- Static in the router, dynamic in the host (DDDLU - Dynamic Definition of Dependent LUs)
Using TN3270

With this method also, you configure LUs in the router either individually by name or in groups using name seeds. In VTAM, you code model LU definitions and associate them with the dependent PUs defined in the router. When a TN3270 client connects to the router, the router selects an LU and sends its configured information about that LU to VTAM (both NAU address and name). Passing the router LU name in this manner is referred to as “name pushing”. VTAM creates the LU definition dynamically, using either its own name seed or the LU name “passed” by the router.

When a TN3270 client disconnects, the router sends a notification of this event. Later levels of VTAM have the ability to destroy the dynamic LU. Earlier versions do not destroy the LU but simply deactivate it pending usage by another client. Dynamic creation and deletion make it possible to have the same named LU be served by any of a number of parallel load-balanced TN3270 servers.

- Dynamic in the router, static in the host (HIDLU - Host-Initiated Dynamic LUs)
  
  With this method, you are not required to configure LUs in the router. You simply configure on a PU basis that a PU supports host-initiated dynamic LUs. In VTAM, you define PUs and LUs by hand as normal. When you activate the LUs at VTAM, the ACTLUs cause the router to dynamically create corresponding LUs using the VTAM LU name. The dynamic LUs are treated as explicit LUs or are placed into implicit LU pools based on whether you configure a pool name for the HIDLU-capable PU.

You can choose any of these LU definition methods, based on the size of your network configuration, level of router and VTAM code, LU naming requirements, and server load balancing requirements. You can combine HIDLU with the other methods by configuring some LUs in the router and allowing the rest to be dynamically created, even within the same PU.

Configured LUs

You need to configure LUs in the router unless you are using Host-Initiated Dynamic LUs. You can configure individual LUs or groups of LUs. Normally, you configure individual LUs when you want to fully specify the LU name and fix it at a particular NAU address. You configure groups of LUs when you have a large number of similar LUs to define and you want the router to generate the LU names.

To configure an individual LU from the command line, use the `add lu` command. You specify the name of the PU (or subarea link) for the LU, and the LU's name, type, and NAU address. To configure an individual LU from the Configuration Program, select LUs from under the TN3270E Server protocol in the Navigation Window, then click on the LUs column heading.

To configure a group of LUs from the command line, use the `add implicit-pool` command. This command defines a group of LUs under a single PU and places them in a pool. You can use this command several times to place different groups of LUs in the same pool, such as LUs from different PUs.

Each time you add a group, you specify the name of the PU, name of the pool, and LU type information. Instead of a single NAU address, you specify either a range of addresses, or the number of LUs you want to add. At initialization time, the router fixes the NAU addresses for configured individual LUs, then assigns the remaining addresses in the range, or number of addresses, to LUs in the group.

Instead of a single LU name, for a group you specify an LU name mask. When the router initializes, it assigns LU names by suffixing this mask with the LU's NAU
address in decimal (not padded with leading zeros). For example, a mask of "@LU1A" might result in the LU names @LU1A1, @LU1A2, and so forth.

If you specify a NAU address range, the router generates names appending the NAU address starting with the bottom of the range going to the top, as just shown with @LU1A. If you specify the number of LUs instead of an NAU address range, the router generates names starting with NAU 2, incrementing up to 255, and ending with 1. For example, a mask of @LU2A for 10 LUs would generate the names @LU2A2, @LU2A3, ..., @LU2A11. The server code starts with 2 for migration consistency with prior code releases that did not support the NAU value 1. To see the exact names the router generates for LUs under a particular PU, use the Talk 5 TN3270 list pu name command.

To configure a group of LUs from the Configuration Program, you must first name the target pool by selecting Pools from under the TN3270E Server protocol in the Navigation Window. Then select LUs from the Navigation window and click the Implicit Pool column heading.

**Dynamic Definition of Dependent LUs (DDDLU)**

As summarized in Defining LUs, you may use DDDLU to avoid duplicate definition of LUs in both VTAM and the router. DDDLU allows you to configure LUs in one place only, the router. In VTAM, you only need to define one or more PUs depending on the number of LUs you need. Implementation of DDDLU also eliminates the effort of VTAM definitions and maintenance for future LU definition requirements.

**Creating LUs at VTAM**

When a TN3270E client requests a connection using one of the LUs defined in the router, the router sends a Reply PSID NMVT command to VTAM on the SSCP-PU session. In this command, the router sends the following information:

- Local NAU address of the LU
- Router name for the LU
- Power on/off indicator
- Device type and model number of the device
- Other optional device-dependent information

On receipt of this NMVT, VTAM sees from the PU definition that there is no definition for the LU in question. VTAM then uses the PU definition and the information in the NMVT to choose a model LU statement and create an LU definition.

The name that VTAM chooses for the dynamic LU is driven by an exit routine for Selection of Definitions for Dependent LUs (SDDLU). If you use the standard IBM-supplied user exit routine, VTAM constructs a name using the LUSEED value on the PU statement, suffixed by the NAU address. You must also code the LUGROUP operand to specify a model major node. These operations are described in VTAM Network Implementation Guide, SC31-8370, under the section entitled “Defining Dependent LUs Dynamically”.

If you want VTAM to use the LU name that the router sends in the Reply PSID NMVT command, you must replace the standard SDDLU user exit with one available from the IBM router support download Web pages. This routine ignores the LUSEED operand and simply uses the name pushed from the router. To download this routine from the 2216 Web pages, for example, go to...
Using TN3270

http://www.networking.ibm.com/support/downloads/2216, select the link to “APPN/TN3270 Files”, and select the user exit package. The package is common to all IBM routers.

Deleting LUs from VTAM
When a TN3270 client disconnects from the router, it sends VTAM another Reply PSID NMVT indicating that the device has powered off. VTAM can then delete the dynamically created LU. This frees up storage and makes the name available for reuse.

VTAM support for dynamic LU deletion on client disconnect is in the base code of CS for OS/390 V2R6, and is PTF’d to CS for OS/390 V1R3 and above with APAR OW29773.

Dynamic LUs and Network Dispatcher
IBM’s Network Dispatcher (ND) can provide a TCP load balancing function when installed between clients and two or more TN3270 servers. The IBM router version of ND and TN3270 Server work together so that ND sends new client connections to the least busy TN3270 server. Previously, when using ND to load balance between TN3270 servers going to the same VTAM, you could not have LUs that needed a fixed VTAM LU name. This is because ND could route the client TCP connection to any of the servers, but you could not have duplicate LU names active at VTAM at the same time.

With LU name pushing and deletion, you can configure the desired LU name at all the potential TN3270 servers. When the client connects in, the server that ND selects sends the name to VTAM for dynamic creation. When the client disconnects, VTAM can delete it. This makes it available to be created again through whichever TN3270 server ND selects the next time the client connects in.

Additional Details
The following example shows a VTAM PU definition for DDDLU. Note that several static LUs that require specific LU names and 3270 printers on specific ports are also defined under the same switched major node.

Example:

```
DDDPU VBUILD TYPE=SWNET
DDDPU PU ADDR=02, x
   IDBLK=077, x
   IDNUM=22160, x
   PUTYPE=2, x
   USSTAB=US327X, x
   LUGROUP=GROUP1, x
   LUSEED=DDLU###, x
   DLOGMOD=D4C32XX3

SALE01 LU LOCADDR=98, x
   DLOGMOD=D4C32XX3, x
   LOGAPPL=CICSA

SALEPRT LU LOCADDR=99, x
   LOGMODE=SAL3287, x
   LOGAPPL=CICSA
```

1 In this sample definition, the LU ‘SALE01’ was requested to be on LOCADDR=98 because of specific requirements. Therefore, this specific LU is defined under this ’DDDPU’ to meet the requirements.

2 In this definition, the printer must also be on a specific address. This especially happens for some SNA applications (e.g. CICS). The application for the sales department needs a printer on address 99, with LOGMODE=SAL3287, and it needs to be connected to application CICSA when it is activated.
For users who wish to write their own or modify one of the VTAM SDDLU exit routines, the router sends LU information in the Reply PSID NMVT as follows:

- SV10, subfield 11 contains one of the device and model type values listed in Table 3.
- SV86, subfield 00 contains IBMTN3270LUNAME to indicate an LU name is being pushed up.
- SV86, subfield 10 contains the actual LU name in EBCDIC.

An example of these subvectors follows:

```
191000 161103130012F3F2F7F0F0F0F2 (3270 device - mod 2)
1086 1100C2D4E3D5F3F2F7F0B3E4D5C1D4C5 {IBMTN3270LUNAME} (LU name is AAAABBBB)
0A10C1C1C1C1C2C2C2C2 (LU name is AAAABBBB)
```

<table>
<thead>
<tr>
<th>Device/Model</th>
<th>NMVT Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>3270 mod 2 display</td>
<td>3270002</td>
</tr>
<tr>
<td>3270 mod 3 display</td>
<td>3270003</td>
</tr>
<tr>
<td>3270 mod 4 display</td>
<td>3270004</td>
</tr>
<tr>
<td>3270 mod 5 display</td>
<td>3270005</td>
</tr>
<tr>
<td>3270 printer</td>
<td>3270P</td>
</tr>
<tr>
<td>SCS printer</td>
<td>SCSP</td>
</tr>
</tbody>
</table>

### Table 3. Device/model type Values

#### Host-Initiated Dynamic Definition of Dependent LUs (HIDLU)

As summarized in [Defining LUs on page 77](#), HIDLU removes the burden of configuring LUs in the router by having the router dynamically create LUs as they are activated from VTAM. This is essentially the opposite of DDDLU, where you configure the LUs in the router and dynamically create them in VTAM. HIDLU allows LUs to be defined in VTAM only. In the router you define only a PU, or as many PUs you need, but no LUs for these PUs.

When VTAM activates the PU and its LUs, the VTAM LU names are conveyed to the router in ACTLU commands in Control Vector 0E. LUs defined in this manner have the same name in both VTAM and the router.

To configure HIDLU in the router, you must still define local dependent PUs in the router either for DLUR or subarea links, as described in [Defining PUs on page 77](#). When you configure the DLUR PU or the subarea link, you simply indicate that Host-initiated dynamic LUs should be allowed for this PU. You also indicate whether these dynamic LUs are to be placed in a pool or not, by optionally specifying a pool name. If you do not specify a pool name, the LUs will be treated only as workstation LUs. If you do specify a pool name, you can indicate whether they are workstation or printer LUs. All pooled HIDLU LUs under a given PU must be in the same pool and have the same type. You can use the same pool name for multiple PUs if you want more than 255 LUs in the pool or you want the pool to span multiple subarea links.

If you place HIDLUs into a pool, you do not need to configure clients to explicitly request a particular LU. The clients can request an LU by pool name, using an IP address to pool mapping, or using a TCP port to pool mapping. You can also mix explicit LUs with HIDLU pooled LUs by configuring an individual LU under a PU that is configured with a host-initiated pool. When the ACTLU arrives for the configured individual LU, the router does not create a dynamic LU.
To configure HIDLU in VTAM, you must define the dependent LUs in the major node and specify INCLUD0E=YES on the PU statement. The INCLUD0E keyword is supported by VTAM V4R4 with APARs OW31805 and OW31436. For remote subarea connections through NCP, V7R6 is needed for INCLUD0E keyword support.

If the host is a DLUS and the PU is being serviced by a DLUR in another node, then CV0E of the ACTLU request may not be forwarded to the PU from the DLUR. In this case, the LUs will not be created dynamically. Once LUs have been created dynamically, they can only be removed by rebooting or manually deleting via configuration. If the LU names are changed in the host major node file after the LUs have been created dynamically, the local names in the router will not be changed.

Client to LU Mapping

When a TN3270 client connects to a server, the server must choose an LU to associate with that client, or deny the connection. There are a number of ways you can configure your clients and server to control which LUs will be chosen, and which clients will be denied. The IBM router implementation of TN3270 server supports the following methods:

- The client can request an individual LU name
- The client can request an LU pool name
- You can configure the router to map client IP addresses to configured individual LU or LU pool names
- You can configure the router to associate destination TCP port numbers with configured LU pool names

The following sections describe background concepts, how to configure each of these methods, and how they work.

Concepts

**LU Pools and Individual LUs:** As described above in “Configured LUs” on page 78, you can configure individual LUs or groups of LUs in the router. In addition, dynamic host-initiated LUs can be treated individually or in groups. An LU pool is simply a named group of LUs. For example, you might call a pool MYPOOLA.

The LUs in a pool can come from one or many different PUs. Except for host-initiated dynamic LUs, the LUs under a PU can be placed in multiple pools. The LUs that you place into a specific pool would typically have similar VTAM definitions and characteristics such as using the same USSMSG10. Using pools is your primary means to group similar LUs together and you will ultimately map a set of like TN3270 client end users to specific pools.

**The Global Default Pool:** There is always at least one pool defined to TN3270E Server, referred to as the Global Default Pool. You name this pool when you initially configure TN3270E Server, and by default it is named PUBLIC. Whatever you name the default pool, you can refer to that name in other parts of the server configuration using the special character string <DEFLT>. This permits you to later change the pool name in only one place without having to change all references to it. Note however that the string <DEFLT> has special meaning when used in an IP address mapping table entry, so you should be careful to understand that meaning when defining such mappings.
You may not need to have a default pool, but it will exist regardless. You do not, however, have to put any LUs into this pool.

**Explicit and Implicit LUs:** LUs in the TN3270 server can be divided into two categories, based on how clients are allowed to access them. Implicit LUs are always members of a pool, and clients can access them either by their individual name or by any of the methods that use pool names. You configure implicit LUs either by adding a group of them to a pool, or by adding individual ones to a pool. Explicit LUs are never members of a pool (even the global default pool), so they can be accessed only by clients requesting their individual name, or by IP address mappings to that name. The server function will never assign an explicit LU to a client that requests or is mapped to a pool name.

**Clients Requesting LU Names**

Client implementations that support RFCs 1646 or 2355 can request a resource name when they connect to a TN3270 server. In the IBM router server, this name is treated either as an individual LU name or as a pool name. In the client configuration, it may be called an LU name even though the same name is configured in the router as a pool name.

If your LU definition method involves different LU names at the router and at VTAM, the name passed by the client must match the router’s LU name, not the LU name in VTAM.

In the absence of IP address and TCP port mapping, the server attempts to satisfy the client’s request as follows:

- If the client requests a valid individual LU name and it is available, the LU is assigned. If it is not available, the server denies the connection.
- If the client requests a valid pool name and one LU in that pool is available, the LU is assigned. If there are no LUs available, the server denies the connection.
- If the name requested is invalid, the server denies the connection.

See the sections below for what happens when a client a name and one of the mapping methods also applies.

**Client IP Address to LU/Pool Mapping**

You can configure the router’s TN3270 server function to map client IP addresses either to individual LU names or to LU pool names. You may want to do this if your clients do not have the ability to request resource names, or you do not want to configure the clients individually. You may also want to use this function as a security mechanism, to deny connections to any clients that are not on the IP mapping access list.

To configure this mapping function, you first enable it globally as part of overall TN3270 server configuration. If you wish clients connecting to certain server TCP ports to be exempt from IP address mapping, you can disable this function on a port-by-port basis when you configure the ports. You then create a table of IP address mapping entries, each of which maps a set of IP addresses to a single LU or pool name. By default, a given entry applies to all server TCP ports, but you can specify that an entry should be used only for connections made to a certain destination TCP port. This allows you to have clients from different IP networks use the same set of port numbers but map to different LU pools based on both their network and the destination server port number.

The key fields in each mapping entry are: an IP address, and IP address mask, and an LU or LU pool name. The IP address mask indicates which bits of the configured
IP addresses are to be compared against the corresponding bits in the incoming client’s source IP address. This allows you to map either individual clients or entire subnets.

For example, if your mapping entry is defined as:

IP Address: 1.2.3.4
Subnet Mask: 255.255.255.255
Pool or LU: MYLU

If a TN3270 client connects in using IP address 1.2.3.4, then the TN3270E Server will assign MYLU to this client. Here we are mapping an individual IP address to an Individual LU. Specific clients can also be mapped to a pool.

If your mapping entry is defined as:

IP Address: 1.2.3.4
Subnet Mask: 255.255.255.0
Pool or LU: YOURPOOL

If a TN3270 client connects in using an IP address of 1.2.3.1, or 1.2.3.2, or 1.2.3.3,..., etc. then TN3270E Server will assign the client an LU from YOURPOOL. Since the subnet mask is 255.255.255.0, all clients in this subnet would match this mapping entry. Masks that are not 255.255.255.255 must be mapped to a pool rather than to an individual LU.

Suppose you define both of the above mapping entries. Note that client 1.2.3.4 would match both of these mapping entries. TN3270E Server will always use the most specific match first. In this example, the client would get mapped to the LU called MYLU.

Suppose again that both of the above mapping entries are defined and client 1.2.3.4 connects in. TN3270 will choose the most specific mapping entry and attempt to connect with the LU called MYLU. However, for some reason the server cannot successfully establish the session with MYLU; MYLU could already be in use, or it may not be activated by VTAM. After unsuccessfully attempting to connect to MYLU, the server normally scans the IP address mapping table to see if there is another less specific match for this client. In our example there is another match and TN3270E Server would connect the client to an LU from YOURPOOL.

There are cases where you may not want the router to use a less-specific match after a more specific match fails. To control this behavior, you can optionally configure an entry as the "final LU mapping connection attempt". If this yes/no flag is set, the server function does not look for less specific matches following a failed match on this entry.

The TN3270 server makes the following checks when a client connects to the router and does not pass in a specific name request:

1. If mapping is globally enabled, is mapping enabled on the destination port? If not, incoming requests are treated without using IP address mapping.
2. If so, try to match the incoming client IP address against the mapping entries in this order:
   a. entries for the specific destination port, most specific IP address first
   b. entries for all destination ports, most specific IP address first
3. If there is a match, try to pair the connection with the indicated LU or an LU in the indicated pool, honoring the LU type (workstation or printer) requested by the client
4. If there is a problem and this is not the “final” mapping entry, repeat for less specific matches. Continue until all matches are exhausted or the connection is satisfied, before denying the connection.

5. If there is no match at all, deny the connection

When a client connects in and makes a request for a specific name, the matching logic is different. In order to successfully connect, a mapping entry must exist whose IP address and mask match the client and whose resource name is the exact same as the name passed in by the client. If the client requests an individual LU name, that name must be in the mapping table, not just the name of a pool containing that LU. The server does not search the mapping table for the most specific IP address and mask match. If the connection to the LU/pool with the requested name cannot be satisfied, the server does not re-scan the mapping table for other matching entries.

You can use the TN3270 Talk 5 command list mapping to see the order in which mapping entries will be searched. You can put a specific IP address as a parameter to this command, to see only those mapping entries that apply to that IP address.

Here are a number of important additional considerations for constructing IP address mapping entries:

- If you have multiple entries that are equally specific, the most recently defined ones are used first.
- If the global default pool has the name PUBLIC and you configure a mapping entry with the name PUBLIC, the server connects incoming clients to LUs in that pool. If instead you configure a mapping entry with the name <DEFLT>, the server does not connect clients to the PUBLIC pool. Rather, it switches to TCP Port association rules and connects the client to the pool associated with the destination server port to which the client connected.
- The IP address mapping table is initially built by the TN3270E server with a default entry containing the IP address 0.0.0.0, subnet mask 0.0.0.0, and pool name <DEFLT>. This entry will match all incoming client addresses. As mentioned above, it will cause the server to map clients to LUs in the pool associated with the destination TCP port(s). If you prefer not to have this default entry in the LU Name Mapping Table, you can create a similar entry above it mapping to a named pool, and indicate that yours is the last to be searched. If the named pool is the global default pool, you can choose not to configure any LUs in that pool.
- The LU and pool names you configure in IP mapping entries must be configured in the router in order to become active. You cannot, for example, configure individual host-initiated dynamic LU names in IP mapping entries, since these names are not known to the router at initialization time. You can configure HIDLU pool names, however, since these are configured in the router.
- For individual workstation LUs with associated printers, both the workstation and printer LUs need to have an IP mapping table entry with the same client IP address.
- Specifying a port number in an IP address mapping table entry does not cause the TN3270 server to define the port and listen on it for client connections. You must configure the port explicitly (using `add port`) before a reference to it in this table will have any meaning.

**Server TCP Port to Pool Association**

You can configure the router’s TN3270 server function to map incoming client connections to LU pools based on the TCP port number to which the clients are
Connecting. You may want to do this if your clients do not have the ability to request resource names, or you do not want to configure the clients individually. You may also be migrating an existing network where clients already connect to different TCP port numbers based on application needs.

To configure TCP port to pool association, you specify a pool name with the port when you configure the port (see [Server TCP Ports on page 76]). Clients obviously each have to connect in through one of the defined ports and the server function assigns an LU based on what pool is associated with the port. If you do not specify a pool name for a port, or you give the special value <DEFLT>, the global default pool is associated with that port. This is the same pool you associate with the globally defined server port when you first configure the TN3270 server.

If a client connects in and does not pass a resource name, the TN3270 server function assigns an LU from the pool associated with the destination port. If no LUs are available, the connection is rejected.

If a client connects in and passes a specific LU or LU pool name, the following rules apply:

- If the port is associated with the exact same LU or pool name as that is passed in by the client, then the client will be connected with the LU or an LU from the pool (if available).
- If the port is defined with a null pool name or with the name <DEFLT>, the client will be connected to the specific LU or an LU from the pool that was passed in from the client as long as that exact LU or pool name is configured somewhere in the TN3270E server. An individual LU can be explicit or implicit. The LU or pool type (workstation or SCS printer or 3270 printer) must match the request. If the name is an LU name, it does not matter what pool, if any, the LU is grouped into.
- If neither of the above two conditions apply, or the specified LU(s) are not available, the connection is rejected.

The above description assumes IP mapping is disabled. If IP address mapping is enabled, then by default the IP address mapping function applies to all ports and will override TCP port to pool mapping. You can change this default behavior by disabling IP address mapping on a TCP port basis, as described earlier. Note also the special case where an IP address mapping entry with the <DEFLT> pool can cause LU allocation from the pool associated with the TCP port.

**Port and IP Address Mapping Combined**

It is possible to use a combination of both IP address mapping and TCP port to pool association. The following is an example of how one user combined these methods to meet their mapping needs.

- The user had IP address mapping enabled and had defined mapping entries to map specific client IP subnets to specific pools.
- The same end user’s clients realized a need to occasionally connect to a group of LUs that presented a different USSMSG10 logon screen.
- Since this was the same set of clients, they would be using the same IP addresses, so adding additional mapping entries to the IP address mapping table would not resolve their needs.
- The user defined a new pool of LUs, defined a new port and associated it with the new pool. Also, they defined this new port not to use the IP address mapping table since that would result in using the original pools.
The clients were then configured at the end user workstations to connect to the new port.

Load Balancing among Multiple PUs

It is common to define a large pool of LUs that reside in multiple PUs. Any pool with more than 255 LUs must include more than one PU. Spreading a pool’s LUs across multiple PUs can lessen the number of clients affected by any given link or PU failure. How the server allocates LUs from among these multiple PUs also determines how many clients are affected by a link or PU failure. For example, if the server allocated all the LUs in one PU before allocating any from the second PU, failure of the first might affect as many as 255 clients needlessly.

The IBM router implementation of TN3270 generally does round-robin allocation of LUs from among multiple PUs in a pool. All other things being equal, it will allocate LU1 from PU1, LU1 from PU2, and so on. At the same time the allocation algorithm favors those PUs that are currently active (avoiding the delay of an activation attempt), and it favors LUs that provide an exact match to the model type requested by the client.

The rules for LU selection are as follows:

- An exact match based on model type is always returned if found in an active PU.
- If an exact match can’t be found in an active PU, then an acceptable LU in an active PU will be returned before an exact match in an inactive PU.
- To be an “acceptable” match, the LU type (workstation, SCS printer, or 3270 printer) must match what the client is requesting. The model type for a workstation LU must give the same or a smaller screen size than that requested by the client. For example, if a client requested a mod 4, a mod 4 LU would be an exact match, and mod 3 or mod 2 LUs would be acceptable matches.

Based on whether an exact or acceptable match is found, PUs are moved on a list to provide general round-robin allocation while keeping less desirable PUs from always being searched first.

Example Configurations

This section contains sample VTAM and router command-line configurations for basic TN3270 server scenarios. For more advanced scenarios and Configuration Program information, see “Other Example Configurations” on page 92.

Configuring TN3270 using DLUR

If you are using DLUR to communicate with the host, the local PUs used by the TN3270E Server need to be configured in the host as DLUR internal PUs. The following code is an example of the host VTAM configuration:

```
PU30E7          PU    ADDR=12,
                 IDBLK=077, IDNUM=EEEE7, 1
                 MAXPATH=8,
                 ISTATUS=ACTIVE,
                 MODETAB=LMT3270,
                 USSTAB=STFTSNA2,
                 ANS=CONT,
                 MAXDATA=521,
                 IRETRY=YES,
                 MAXOUT=7,
                 DLOGMOD=G22NNE,
                 NETID=STFNET,
                 PASSLIM=5,
                 PUTYPE=2
```
Using TN3270

JCPATH7 PATH PID=1,
DLURNAME=VLNN01,
DLCADDR=(1,C,INTPU),
DLCADDR=(2,X,07711111)
JC7LU2 LU LOCADDR=2
JC7LU3 LU LOCADDR=3
JC7LU4 LU LOCADDR=4
JC7LU5 LU LOCADDR=5
JC7LU6 LU LOCADDR=6

Note: 07711111 represents the ID block/ID number of the local PU. The 077 part of this value is not configurable at the router.

The following example shows how to configure the router to use an upstream DLUR connection for TN3270, using the command line.

APPN config>
APPN config> set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [STFNET]?
Control point name (Max 8 characters) [VLNN2]?
Enable branch extender (Y)es (N)o [N]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
APPN config>
APPN config> set dlur
Enable DLUR (Y)es (N)o [Y]?
Fully-qualified CP name of primary DLUS [STFNET.MVS8]?
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds)[120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.
APPN config>
APPN config> tn3270e
TN3270E config> set
TN3270E Server Parameters
Enable TN3270E Server (Y/N) [Y]?
TN3270E Server IP Address[4.3.2.1]?
Port Number[23]?
Enable Client IP Address to LU Name Mapping (Y/N) [N]
Default Pool Name[PUBLIC]?
NetDisp Advisor Port Number[10008]?
Keepalive type:
0 = none,
1 = Timing Mark,
2 = NOP[2]?
Frequency (1 - 65535 seconds)[60]?
Automatic Logoff (Y/N)[N]?
Write this record?[Y]?
The record has been written.
TN3270E config> exit
APPN config>
APPN config> add loc
Local PU information
Using TN3270

Station name (Max 8 characters) []? link1
Fully-qualified CP name of primary DLUS[STFNET.MVS8] ?
Fully-qualified CP name of a backup DLUS[]?
Local Node ID (5 hex digits)[11111]?
Autoactivate (y/n)[Y]?
Write this record?[Y]?
The record has been written.

APPN config>tn3270
TN3270E config>add im
TN3270E Server Implicit definitions
Pool name (Max 8 characters)[<DEFLT>]? link1
LU Name Mask (Max 5 characters) [001LU]?
LU Type ( 1 - 3270 mod 2 display
2 - 3270 mod 3 display
3 - 3270 mod 4 display
4 - 3270 mod 5 display) [1]?
Specify LU Address Range(s) (y/n) [n]
Number of Implicit LUs in Pool(1-255) [50]?
Write this record?[Y]?
The record has been written.

TN3270E config>
TN3270E config>add lu
TN3270E Server LU Definitions
LU name(Max 8 characters) []? printer1
NAU Address (1-255) [0] 2
Station name (Max 8 characters) []? link1
Class:
1 = Explicit Workstation,
2 = Implicit Workstation,
3 = Explicit Printer,
4 = Implicit Printer[3]?
LU Type ( 5 - 3270 printer
6 - SCS printer) [5]?
Write this record?[Y]?
The record has been written.

TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP Frequency: 60
Automatic Logoff: N Timeout: 30
Enable IP Precedence: N
Link Station: link1
Local Node ID: 11111
Auto activate: YES
Implicit Pool Information
Number of LUs: 50
LU Mask: @01LU

LU Name | NAU addr | Class | Assoc LU Name | Assoc NAU addr
-----------------------------------------------
printer1 | 2         | Explicit Printer

TN3270E config>exit
APPN Config>exit

Config>
Config>ip
Internet protocol user configuration
IP config=11 all
Interface addresses
IP addresses for each interface:
**Using TN3270**

```
intf 0 9.1.1.20 255.0.0.0  Local wire broadcast, fill 1
intf 1                         IP disabled on this interface
intf 2                         IP disabled on this interface

Internal IP address: 4.3.2.1
```

**Routing**

**Protocols**

- BOOTP forwarding: disabled
- IP Time-to-live: 64
- Source Routing: enabled
- Echo Reply: enabled
- TFTP Server: enabled
- Directed broadcasts: enabled
- ARP subnet routing: disabled
- ARP network routing: disabled
- Per-packet-multipath: disabled
- OSPF: disabled
- BGP: disabled
- RIP: disabled

```
IP config>
* 
```

**Configuring TN3270E Using a Subarea Connection**

The following example shows how to configure the router to use an SNA subarea (non-APPN) upstream host connection for TN3270, using the command line. In this example, the router appears to VTAM as multiple downstream PUs.

```
Confign>p appn
APPN config> set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [STFNET]?
Control point name (Max 8 characters) [VLNN2]?
Enable branch extender (Y)es (N)o [N]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [000000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
APPN config>

APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)thernet, (T)oken Ring, (S)DLC, (X)25, (FD)I, (D)LsW, (A)TM, (I)P []?fr
Interface number(Defalut 0): [0]?: 2
Port name (Max 8 characters) [F00002]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
  Support multiple subarea (Y)es (N)o [N]? y
  All active port names will be of the form <port name sap>
  Service any node: (Y)es (N)o [Y]?
  High performance routing: (Y)es (N)o [Y]?
  Maximum BUU size (768-8136) [2048]?
  Percent of link stations reserved for incoming calls (0-100) [0]?
  Percent of link stations reserved for outgoing calls (0-100) [0]?
  Local SAP address (04-EC) [4]?
  Support bridged formatted frames: (Y)es (N)o [N]?
  Edit TG Characteristics: (Y)es (N)o [N]?
  Edit LLC Characteristics: (Y)es (N)o [N]?
  Edit HPR defaults: (Y)es (N)o [N]?
```
APPN config>add link
APPN Station
Port name for the link station [ ]? f00002
Station name (Max 8 characters) [ ]? suba1
  Activate link automatically (Y)es (N)o [Y]?
  DLCI number for link (16-1007) [16]? 23
  Adjacent node type: 0 = APPN network node,
  1 = APPN end node or Unknown node type,
  2 = LEN end node [0]?
  Solicit SSCP Session: (Y)es (N)o [Y]? y
    Local Node ID (5 hex digits) [00000]? 12345
  Local SAP address (04-EC) [4]? c
  Allow CP-CP sessions on this link (Y)es (N)o [Y]? n
    Configure CP name of adjacent node: (Y)es (N)o [N]?
  Edit TG Characteristics: (Y)es (N)o [N]?
  Edit LLC Characteristics: (Y)es (N)o [N]?
  Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>act
APPN config>APPN config>tn3270e
TN3270E config>set
TN3270E Server Parameters
  Enable TN3270E Server (Y/N) [Y]?
  TN3270E Server IP Address[4.3.2.1]?
  Port Number[23]?
  Enable Client IP Address to LU Name Mapping (Y/N) [N]
  Default Pool Name[PUBLIC]?
  NetDisp Advisor Port Number[10008]?
  Keepalive type:
  0 = none,
  1 = Timing Mark,
  2 = NOP[2]?
  Frequency ( 1 - 65535 seconds)[60]?
  Automatic Logoff (Y/N)[N]?
Write this record?[Y]?
The record has been written.
TN3270E config>exit
APPN config>
Write this record?[Y]?
The record has been written.

APPN config>tn3270
TN3270E config>add im
TN3270E Server Implicit definitions
  Pool name (Max 8 characters)[<DEFLT>]? subal
  Station name (Max 8 characters)[ ]? subal
  LU Name Mask (Max 5 characters) [@@01LU]?
  Specify LU Address Range(s) (y/n) [N]
  Number of Implicit LUs in Pool(1-255) [50]?
Write this record?[Y]?
The record has been written.
TN3270E config>

APPN config>add lu
TN3270E Server LU Definitions
  LU name(Max 8 characters) []? printer1
  NAU Address (1-255) [2]
  Station name (Max 8 characters) []? subal
  Class:
  1 = Explicit Workstation,
  2 = Implicit Workstation,
  3 = Explicit Printer,
  4 = Implicit Printer[3]?
Using TN3270

LU Type ( 5 - 3270 printer 
6 - SCS printer) [5]?
Write this record[Y]?
The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keppalive type: NOP Frequency: 60
Automatic Logoff: N Timeout: 30
Enable IP Precedence: N
Link Station: suba1
Local Node ID: 12345
Auto activate : YES
Implicit Pool Information
Number of LUs: 50
LU Mask: @01LU
LU Name NAU addr Class Assoc LU Name Assoc NAU addr
-----------------------------------------------
printer1 2 Explicit Printer

TN3270E config>exit
APPN Config>exit

APPN config>act

Other Example Configurations

The TN1 model of the Network Utility product was designed to be used as a
TN3270 server, and it shipped with example TN3270 configuration information that
can be helpful to users of the 2216, 2212, and 2210. This information is available
both in product publications and in example binary configuration files on the Web.

The publication Network Utility: Installation, Getting Started, and User’s Guide,
GA27-4167-02, documents the router configuration (usually both the command-line
and Configuration Program) and sample VTAM configurations for the following
network configurations:

- Subarea host connection through token-ring to an NCP (same for channel
gateway or OSA)
- Parallel subarea TN3270 servers load balanced by two Network Dispatcher
  routers
- DLUR host connection through token-ring to a Network Node
- DLUR host connection through Enterprise Extender to an IBM router or gateway
- Dynamic definition of dependent LUs (DDDLU)
- Host-initiated Dynamic LU Definition (HIDLU)
- Host On-Demand (HOD) Client Cache
- Subarea host connection over DLSw
- Subarea host connection over channel via LSA loopback

Some of the above configurations are supplemented on the Web by both
router-format and Configuration Program-format binary configuration files. Use your
browser to reach these as follows:

1. Open the Network Utility downloads page at:
   http://www.networking.ibm.com/support/downloads/networkutility
2. Follow the link to “Configuration Program” files
3. Find the code release you are using (the file contents have already been upgraded for each release)
4. Open the package named "Example Configuration Files"
Using TN3270
Chapter 3. Configuring and Monitoring APPN

This chapter describes the APPN configuration and monitoring commands. It includes the following sections:
- "APPN Configuration Command Summary"
- "APPN Configuration Command Detail" on page 96
- "APPN Dynamic Reconfiguration Support" on page 275

Accessing the APPN Configuration Process

Use the following procedure to access the APPN configuration process.

1. At the * prompt, enter talk 6. The Config> prompt is displayed. (If this prompt is not displayed, press Return again.)
2. Enter protocol appn. The APPN Config> prompt is displayed.
3. Enter an APPN configuration command.

APPN Configuration Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function Description</th>
<th>See page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxvii</td>
<td>36</td>
</tr>
<tr>
<td>Enable/Disable</td>
<td>Enables/disables the following: APPN 96 Dependent LU Requestor 97 Port port name</td>
<td>36</td>
</tr>
<tr>
<td>Set</td>
<td>Sets the following: Node 97 Traces 118 HPR 104 DLUR 108 Management 138 Tuning 112</td>
<td>37</td>
</tr>
<tr>
<td>Add</td>
<td>Adds or updates the following: Port port name 143 Link-station link station name 166 LU-Name LU name 192 Connection-network connection network name 193 Additional-port-to-connection-network 204 Mode 202 Focal_point 205 local-pu 205 Routing_list 208 COS_mapping_table 212</td>
<td>36</td>
</tr>
</tbody>
</table>
### APPN Configuration Command Detail

#### Enable/Disable

Use the `enable/disable` command to enable (or disable):

**Syntax:**

```
enable appn
[or disable] dlur
    port port name
```

---

Note: APPN will respond to a dynamic `reset` command at the interface level.
**Set**

Use the `set` command to set:

**Syntax:**

```
set node
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

**Table 5. Configuration Parameter List - APPN Routing**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Enable APPN</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables the router as an APPN network node. This parameter enables both APPN and HPR routing capability for this network node which consists of defining the Network ID and CP name for this node. APPN, however, must be enabled on the particular ports on which you desire to support APPN routing. Additionally, support for HPR must be enabled on the particular APPN ports desired and must be supported by the particular link stations on those ports. <strong>Note:</strong> HPR only supported on LAN, Frame Relay and PPP direct DLC ports.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Network ID (required)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>- First character: A to Z</td>
</tr>
<tr>
<td>- Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Note:</strong> A network identifier for an existing network, of which this router network node is to become a member, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new network IDs.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of the APPN network to which this network node belongs. The network ID must be the same for all network nodes in the APPN network. Attached APPN end nodes and LEN end nodes can have different network IDs.</td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

**Table 5. Configuration Parameter List - APPN Routing (continued)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Control point name (required)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>• First character: A to Z</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Note:</strong> An existing CP name that this node would be acquiring, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names.</td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of the CP for this APPN network node. The CP is responsible for managing the APPN network node and its resources. The CP name is the logical name of the APPN network node in the network. The CP name must be unique within the APPN network identified by the Network ID parameter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable branch extender or border node</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 (enable neither)</td>
</tr>
<tr>
<td>1 (enable branch extender)</td>
</tr>
<tr>
<td>2 (enable border node)</td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether branch extender function, border node function, or neither will be enabled on this node. If either function is enabled, appropriate additional questions will be asked.</td>
</tr>
</tbody>
</table>
### Table 5. Configuration Parameter List - APPN Routing (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Enable Branch Awareness Support</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 (Full), 1 (Partial), 2 (None)</td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>0 (Full)</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether you want to limit the flow of topology information regarding Branch Extender topology.</td>
</tr>
<tr>
<td><em>Full</em> means that the node will broadcast all Branch Extender TGs into the network when they are learned.</td>
</tr>
<tr>
<td><em>Partial</em> means that the node will not broadcast local Branch Extender topology, but will store and broadcast non-local Branch Extender topology.</td>
</tr>
<tr>
<td><em>None</em> means that the node will not broadcast local Branch Extender topology and it will ignore any Branch Extender topology received from the network and the node will not store or broadcast non-local Branch Extender topology.</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Permit search for unregistered LUs</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether this node (when acting as an End Node) can be searched for LUs even if the LUs were not registered with the network node server of the Branch Extender. If <em>yes</em> is specified, this node can be searched for LUs.</td>
</tr>
<tr>
<td><strong>Note:</strong> This question is asked only if <strong>Enable Branch Extender or Border Node</strong> parameter is set to <em>branch extender</em>.</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Subnet visit count</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 — 255</td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Specifies the node level default for the maximum number of subnetworks that a multi-subnetwork session may traverse. The default may be overridden as part of port, link, or routing list configuration.</td>
</tr>
<tr>
<td><strong>Note:</strong> This is the first of the questions asked only if border node has been enabled.</td>
</tr>
</tbody>
</table>
### Table 5. Configuration Parameter List - APPN Routing (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Cache searches for (0-255) minutes</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 - 255</td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Specifies how many minutes the BN retains information in the multi-subnet search cache once the search terminates.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Maximum number of searches in cache</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 - 32765 (0=unlimited)</td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Specifies the maximum number of entries in the multi-network search cache. Once this limit is reached, the oldest entries are discarded.  
**Note:** The primary mechanism for deletion of these entries is the cache search time value specified in cache searches for (0–255) minutes. |

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Dynamic routing list updates</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
</tbody>
</table>
| 0 (none) - No dynamic entries are added.  
1 (full) - All native border nodes, all adjacent non-native border and network nodes, and nodes that know of similarly named destination LUs are added.  
2 (limited) - All native border nodes, all adjacent non-native border nodes and network nodes **with the same NETID**, and nodes that know of similarly named destination LUs are added. |
| **Default**            |
| 2                      |
| **Description**        |
| Indicates the degree to which, if any, that a BN can supplement configured routing list data with topology data learned by the operational code. This supplemental data is not saved in SRAM. |
### Parameter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Enable routing list optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Indicates whether or not a BN may reorder the operational code's temporary copy of a subnetwork routing list so that entries that are more likely to be successful are found first.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Load balance across parallel inter-subnet boundaries</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies whether the router should attempt to balance the number of sessions across two or more parallel inter-subnet exit points when it is functioning as an EBN. The relevant configuration has two or more IBM routers serving as EBN exit points in one subnet, with the same number in the other subnet. Each router has an inter-subnet TG to a different router in the other subnet, forming two or more parallel links. (Note that these are not parallel TGs between any two routers.) To configure session load balancing among the parallel exit points: 1. Set this parameter to yes. 2. Configure routing lists (see 211) in each EBN router, so that sessions for different destination LU names have different preferred exit EBNs. You also configure the preferred inter-subnet boundary and can set backup paths. 3. Configure the routing lists with <strong>dynamic routing list updates</strong> set to <em>none</em>, and <strong>Enable routing list optimization</strong> set to <em>no</em>.</td>
</tr>
</tbody>
</table>
### Table 5. Configuration Parameter List - APPN Routing (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>XID number for subarea connection (see table notes)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
<th>A string of 5 hexadecimal digits</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>X’00000’</th>
</tr>
</thead>
</table>

#### Description
This parameter specifies a unique ID number (identifier) for the network node. The XID number is combined with an ID block number (which identifies a specific product) to form an XID node identification. Node identifications are exchanged between adjacent nodes when the nodes are establishing a connection. The router network node automatically appends an ID block number to this parameter during the XID exchange to create an XID node identification.

The ID number you assign to this node must be unique within the APPN network identified by Network ID parameter. Contact your network administrator to verify that the ID number is unique.

**Note:** Node identifications are normally exchanged between T2.1 nodes during CP-CP session establishment. If the network node is communicating with the IBM Virtual Telecommunications Access Method (VTAM) product through a T2.1 LEN node and the LEN node has a CP name defined for it, the XID number parameter is not required. If the adjacent LEN node is not a T2.1 node or does not have an explicitly defined CP name, the XID number parameter must be specified to establish a connection with the LEN node. VTAM versions prior to Version 3 Release 2 do not allow CP names to be defined for LEN nodes.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Use enhanced BATCH COS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
<th>Yes or No</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Yes</th>
</tr>
</thead>
</table>

#### Description
This parameter specifies whether to use the enhanced COS tables. The enhanced tables assign reasonable weights to ATM TGs based on cost, speed, and delay. For ATM, the order of preference is:

- Campus Best Effort (SVC or PVC)/Reserved PVC (WAN or Campus)
- Campus Reserved SVC
- WAN Best Effort (SVC or PVC)
- WAN Reserved SVC
Table 5. Configuration Parameter List - APPN Routing (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
</tbody>
</table>
| **Description**       | This parameter specifies whether to use the enhanced COS tables. The enhanced tables assign reasonable weights to ATM TGs based on cost, speed, and delay. For ATM, the order of preference is:  
- Campus Best Effort (SVC or PVC)/Reserved PVC (WAN or Campus)  
- Campus Reserved SVC  
- WAN Best Effort (SVC or PVC)  
- WAN Reserved SVC |

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
</tbody>
</table>
| **Description**       | This parameter specifies whether to use the enhanced COS tables. The enhanced tables assign reasonable weights to ATM TGs based on cost, speed, and delay. For ATM, the order of preference is:  
- Campus Reserved (SVC or PVC)  
- Campus Best Effort (SVC or PVC)/WAN reserved PVC  
- WAN Reserved SVC  
- WAN Best Effort (SVC or PVC) |

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
</tbody>
</table>
| **Description**       | This parameter specifies whether to use the enhanced COS tables. The enhanced tables assign reasonable weights to ATM TGs based on cost, speed, and delay. For ATM, the order of preference is:  
- Campus Reserved (SVC or PVC)  
- Campus Best Effort (SVC or PVC)/WAN reserved PVC  
- WAN Reserved SVC  
- WAN Best Effort (SVC or PVC) |
APPN Configuration Commands

Syntax:

```
set high-performance routing
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

**Table 6. Configuration Parameter List - High-Performance Routing (HPR)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Maximum sessions for HPR connections</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>1 to 65535</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter specifies the maximum number of sessions allowed on an HPR connection. An HPR connection is defined by the class of service (COS), the physical path (TGs), and the network connection end points.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

This parameter is applicable only when the router is the initiator of the BIND. If the number of sessions exceeds the specified value for this parameter, HPR will allocate another HPR (RTP) connection.

**Table 7. Configuration Parameter List - HPR Timer and Retry Options**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low transmission priority traffic</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>RTP inactivity timer</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>1 to 3600 seconds</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>180 seconds</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter specifies RTP’s inactivity interval for HPR connections that carry traffic with low transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Maximum RTP retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>0 to 10</td>
</tr>
<tr>
<td>Default Value</td>
<td>6</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with low transmission priority.</td>
</tr>
</tbody>
</table>
### Table 7. Configuration Parameter List - HPR Timer and Retry Options (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

#### Medium transmission priority traffic

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

Table 7. Configuration Parameter List - HPR Timer and Retry Options (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>High transmission priority traffic</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP inactivity timer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
<th>1 to 3600 seconds</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
<th>180 seconds</th>
</tr>
</thead>
</table>

| Description | This parameter specifies RTP's inactivity interval for HPR connections that carry traffic with high transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection. |

<table>
<thead>
<tr>
<th>Parameter</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum RTP retries</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
<th>0 to 10</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
<th>6</th>
</tr>
</thead>
</table>

| Description | This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with high transmission priority. |

<table>
<thead>
<tr>
<th>Parameter</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Path switch timer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
<th>0 to 7200 seconds</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
<th>180 seconds</th>
</tr>
</thead>
</table>

| Description | This parameter specifies the maximum amount of time that a path switch may be attempted on an HPR connection carrying traffic with high transmission priority. A value of zero indicates that the path switch function is to be disabled, and a path switch will not be performed. |

**Network transmission priority traffic**
### Table 7. Configuration Parameter List - HPR Timer and Retry Options (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>RTP inactivity timer</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 3600 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>180 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies RTP’s inactivity interval for HPR connections that carry traffic with network transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Maximum RTP retries</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>0 to 10</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>6</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with network transmission priority.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Path switch timer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>0 to 7200 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>180 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies the maximum amount of time that a path switch may be attempted on an HPR connection carrying traffic with network transmission priority. A value of zero indicates that the path switch function is to be disabled, and a path switch will not be performed.</td>
</tr>
</tbody>
</table>

**Syntax:**

```
set dlur
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].
### Table 8. Configuration Parameter List - Dependent LU Requester

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Enable dependent LU requester (DLUR) on this network node</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether a dependent LU requester is to be functionally enabled on this node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default fully-qualified CP name of primary DLUS (required when DLUR is enabled)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of up to 17 characters in the form of <code>netID.CPname</code>, where:</td>
</tr>
<tr>
<td><code>netID</code> is a network ID from 1 to 8 characters</td>
</tr>
<tr>
<td><code>CPname</code> is a CP name from 1 to 8 characters</td>
</tr>
<tr>
<td>Each name must conform to the following rules:</td>
</tr>
<tr>
<td>First character: A to Z</td>
</tr>
<tr>
<td>Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Note:</strong> An existing fully-qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the fully-qualified control point (CP) name of the dependent LU server (DLUS) that is used by default. The default primary server may be overridden on a link station basis. The default server is used for incoming requests from downstream PUs when a primary DLUS has not been specified for the associated link station.</td>
</tr>
</tbody>
</table>
### Table 8. Configuration Parameter List - Dependent LU Requester (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Perform retries to restore disrupted pipe</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies whether DLUR will attempt to reestablish the pipe to a DLUS after a pipe failure. If DLUR receives a non-disruptive UNBIND and this parameter is No, DLUR waits indefinitely for a DLUS to reestablish the broken pipe. If the pipe fails for any other reason and this parameter is No, DLUR attempts to reach the primary DLUS once. If this is unsuccessful, DLUR attempts to reach the backup DLUS. If this attempt also fails, DLUR waits indefinitely for a DLUS to reestablish the pipe.</td>
</tr>
</tbody>
</table>

See [DLUR Retry Algorithm](page 35) for a description of the retry algorithm.
### Table 8. Configuration Parameter List - Dependent LU Requester (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Delay before initiating retries</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 2 756 000 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>120 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies an amount of time for two different cases when the pipe between the DLUR and its DLUS is broken.</td>
</tr>
<tr>
<td>- For the case of receiving a non-disruptive UNBIND: This parameter specifies the amount of time the DLUR must wait before attempting to reach the primary DLUS. A value of 0 indicates immediate retry by the DLUR.</td>
</tr>
<tr>
<td>- For all other cases of pipe failure: The DLUR will try the primary DLUS and then the backup DLUS immediately. If this fails, DLUR will wait for the amount of time specified by the minimum of the short retry timer and this parameter before attempting to reach the primary DLUS.</td>
</tr>
<tr>
<td>See <a href="#">DLUR Retry Algorithm on page 35</a> for a complete description of the retry algorithm.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Perform short retries to restore disrupted pipe</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>If Perform retries to restore disrupted pipes is Yes, then the default value is Yes. Otherwise, the default is No.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>See <a href="#">DLUR Retry Algorithm on page 35</a> for a complete description of the retry algorithm.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Short retry timer</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 2 756 000 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>120 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>In all cases of pipe failure other than non-disruptive UNBIND, the minimum of Delay before initiating retries and this parameter specifies the amount of time DLUR will wait before attempting to reach the primary DLUS after an attempt to establish this connection has failed.</td>
</tr>
<tr>
<td>See <a href="#">DLUR Retry Algorithm on page 35</a> for a complete description of the retry algorithm.</td>
</tr>
</tbody>
</table>
### Table 8. Configuration Parameter List - Dependent LU Requester (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Short retry count</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 65 535</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>In all cases of pipe failure other than non-disruptive UNBIND, this parameter specifies the number of times the DLUR will attempt to perform short retries to reach the DLUS after an attempt to establish this connection has failed.</td>
</tr>
<tr>
<td>See <a href="#">DLUR Retry Algorithm</a> on page 35 for a complete description of the retry algorithm.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform long retries to restore disrupted pipe</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>If Perform retries to restore disrupted pipes is Yes, then the default value is Yes. Otherwise, the default is No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>See <a href="#">DLUR Retry Algorithm</a> on page 35 for a complete description of the retry algorithm.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long retry timer</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 2 756 000 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>300 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the time DLUR will wait when performing long retries.</td>
</tr>
<tr>
<td>See <a href="#">DLUR Retry Algorithm</a> on page 35 for a complete description of the retry algorithm.</td>
</tr>
</tbody>
</table>
### Table 8. Configuration Parameter List - Dependent LU Requester (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

**Syntax:**

```
set tuning
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

**Note:** You will have to re-boot in order for the changes you specify to take place.

### Table 9. Configuration Parameter List - APPN Node Tuning

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### Table 9. Configuration Parameter List - APPN Node Tuning (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### Table 9. Configuration Parameter List - APPN Node Tuning (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

| **Parameter**          | Maximum percent of ISR sessions using HPR data connections |
| **Valid Values**       | 0 to 100 percent |
| **Default**            | 0 percent |
| **Description**        | This parameter specifies the largest percentage of ISR sessions that use ISR to HPR mappings. This parameter is configurable using the Configuration Program only. |

| **Parameter**          | Percent adjacent nodes that function as DLUR PU nodes |
| **Valid Values**       | 0 to 100 percent |
| **Default**            | 0 percent |
| **Description**        | This parameter specifies the largest percentage of adjacent nodes allowed to function as adjacent DLUR PU nodes. This parameter is configurable using the Configuration Program only. |

| **Parameter**          | Maximum percent ISR sessions used by DLUR LUs |
| **Valid Values**       | 0 to 100 percent |
| **Default**            | 0 percent |
| **Description**        | This parameter specifies the largest percentage of ISR sessions used by DLUR LUs. This parameter is configurable using the Configuration Program only. |
### Table 9. Configuration Parameter List - APPN Node Tuning (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

**Table 9. Configuration Parameter List - APPN Node Tuning (continued)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Number of local-pus for TN3270E support</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the number of local PUs that are available for TN3270 support.</td>
</tr>
<tr>
<td>This parameter is configurable using the Configuration Program only.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of LUs for TN3270E</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the total number of LUs available for TN3270E support.</td>
</tr>
<tr>
<td>This parameter is configurable using the Configuration Program only.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum shared memory</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 - 16 777 215 KB</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Auto-configured (configure based on installed memory)</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the amount of shared memory within the router that is allocated to the APPN network node. APPN uses its shared memory allocation to perform network operations and to maintain required tables and directories.</td>
</tr>
<tr>
<td>You can either input a value in Kilobytes, or select to have the router pick a reasonable general purpose default value at boot time based on its installed memory. Note that the default value the router chooses is not based on the size of the APPN configuration. Default values assume you are running a medium-size APPN or TN3270 network, and some other non-trivial routing function. The default value may not fit if you also configure another extremely memory-intensive router function.</td>
</tr>
<tr>
<td>As you select the <em>auto-configured</em> value from the command-line prompt, you can see what this value will be if you boot the configuration on the router you are using. If you select this value from the Configuration Program, you must download and activate the configuration before you can see what the result will be.</td>
</tr>
<tr>
<td>This parameter is configurable using the Configuration Program and from the command line.</td>
</tr>
</tbody>
</table>
### Table 9. Configuration Parameter List - APPN Node Tuning (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

### Syntax:

```
set traces
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].
### Table 10. Configuration Parameter List - Trace Setup Questions

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Turn all trace flags off</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables trace flags.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Edit Node-Level Traces</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. See Table 11 on page 119 for the set of questions you will be asked if this option is enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Edit Interprocess Signals</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. See Table 12 on page 124 for the set of questions you will be asked if this option is enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Edit Module Entry and Exit</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. See Table 13 on page 128 for the set of questions you will be asked if this option is enabled.</td>
</tr>
</tbody>
</table>
Table 10. Configuration Parameter List - Trace Setup Questions (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Edit General</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. See Table 14 on page 130 for the set of questions you will be asked if this option is enabled.</td>
</tr>
</tbody>
</table>

Table 11. Configuration Parameter List - Node Level Traces

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Process management</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the management of processes within the APPN network node, including the creation and termination of processes, processes entering a wait state, and the posting of processes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Process to process communication</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about messages exchanged between processes in the APPN network node, including the queuing and receipt of such messages.</td>
</tr>
</tbody>
</table>
### Parameter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Locking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about locks that were obtained and released on processes in the APPN network node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Miscellaneous tower activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about miscellaneous activities within the APPN network node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>I/O to and from the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the flow of messages entering and exiting the APPN network node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Storage management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about any shared memory that was obtained and released by the APPN network node.</td>
</tr>
</tbody>
</table>
### Table 11. Configuration Parameter List - Node Level Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Queue data type management</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls in the APPN network node that manage general purpose queues.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Table data type management</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls in the APPN network node that manage general purpose tables, including calls to add table entries and calls to query tables for specific entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Buffer management</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about buffers in the APPN network node that were obtained and released.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Configuration control</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the activities of the configuration control component of the APPN network node. The configuration control component manages information about node resources.</td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

Table 11. Configuration Parameter List - Node Level Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Timer service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about requests for timer service from the APPN network node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Service provider management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the definition and enabling or disabling of services within the APPN network node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Inter-process message segmenting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the buffer transfer and freeing of chained messages within the APPN network node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Control of processes outside scope of this tower</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
<td>No</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the definition and activation of processes external to this APPN network node, such as when the node operator facility (NOF) defines the external process configuration control.</td>
</tr>
</tbody>
</table>
### Table 11. Configuration Parameter List - Node Level Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th>Distributed environment control</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about requests within the APPN network node that define subsystems and create environments.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th>Process to service dialogs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter enables or disables this APPN trace option. When enabled, this trace option causes the router trace facility to gather data about all calls within the APPN network node that open, close, or send data on a dialog.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th>AVL Tree Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls that manage AVL trees.</td>
</tr>
</tbody>
</table>
## APPN Configuration Commands

*Table 12. Configuration Parameter List - Inter-process Signals Traces*

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Address space manager</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the address space manager component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Attach manager</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the attach manager component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Configuration services</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the configuration services component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Dependent LU requester</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the dependent LU requester component.</td>
</tr>
</tbody>
</table>
### Parameter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory services</td>
<td>Yes, No</td>
<td>No</td>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the directory services component.</td>
</tr>
<tr>
<td>Half Session</td>
<td>Yes, No</td>
<td>No</td>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the half session component.</td>
</tr>
<tr>
<td>HPR Path Control</td>
<td>Yes, No</td>
<td>No</td>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the HPR path control component.</td>
</tr>
<tr>
<td>LUA RUI</td>
<td>Yes, No</td>
<td>No</td>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the LUA RUI component.</td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

#### Table 12. Configuration Parameter List - Inter-process Signals Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Management Services</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the management services component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Operator Facility</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the node operator facility component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Control</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the path control component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation Services</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the presentation services component.</td>
</tr>
<tr>
<td>Parameter Information</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Resource manager</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the resource manager component.</td>
</tr>
</tbody>
</table>

| **Parameter**          |
| Session connector manager |
| **Valid Values**       |
| Yes, No                |
| **Default Value**      |
| No                     |
| **Description**        |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the session connector manager component. |

| **Parameter**          |
| Session connector     |
| **Valid Values**       |
| Yes, No                |
| **Default Value**      |
| No                     |
| **Description**        |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the session connector component. |

| **Parameter**          |
| Session manager       |
| **Valid Values**       |
| Yes, No                |
| **Default Value**      |
| No                     |
| **Description**        |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the session manager component. |
### Table 12. Configuration Parameter List - Inter-process Signals Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Session services</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the session services component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Topology and routing services</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the topology and routing services component.</td>
</tr>
</tbody>
</table>

### Table 13. Configuration Parameter List - Module Entry and Exit Traces

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Attach manager</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the attach manager component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Half session</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the half session component.</td>
</tr>
</tbody>
</table>
### Table 13. Configuration Parameter List - Module Entry and Exit Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>LUA RUI</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the LUA RUI component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node operator facility</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the node operator facility component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation services</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the presentation services component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid transport protocol</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the rapid transport control component.</td>
</tr>
</tbody>
</table>
### Table 13. Configuration Parameter List - Module Entry and Exit Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Resource manager</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the resource manager component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Session manager</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the session manager component.</td>
</tr>
</tbody>
</table>

### Table 14. Configuration Parameter List - General Component Level Traces

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Accounting services</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the accounting services component.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Address space manager</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the address space manager component.</td>
</tr>
<tr>
<td>Parameter Information</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
APPN Configuration Commands

Table 14. Configuration Parameter List - General Component Level Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>HPR path control</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the HPR path control component.</td>
</tr>
</tbody>
</table>

| Parameter              |
| LUA RUI                |
| Valid Values           |
| Yes, No                |
| Default Value          |
| No                     |
| Description            |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the LUA RUI component. |

| Parameter              |
| Management services    |
| Valid Values           |
| Yes, No                |
| Default Value          |
| No                     |
| Description            |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the management services component. |

| Parameter              |
| Node operator facility |
| Valid Values           |
| Yes, No                |
| Default Value          |
| No                     |
| Description            |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the node operator facility component. |
### Table 14. Configuration Parameter List - General Component Level Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Path control</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the path control component.</td>
</tr>
</tbody>
</table>

| **Parameter**          |
| Problem determination services |
| **Valid Values**       |
| Yes, No                |
| **Default Value**      |
| No                     |
| **Description**        |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the problem determination component. |

| **Parameter**          |
| Rapid transport protocol |
| **Valid Values**       |
| Yes, No                |
| **Default Value**      |
| No                     |
| **Description**        |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the rapid transport control component. |

| **Parameter**          |
| Session connector manager |
| **Valid Values**       |
| Yes, No                |
| **Default Value**      |
| No                     |
| **Description**        |
| This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the session connector manager component. |
### APPN Configuration Commands

Table 14. Configuration Parameter List - General Component Level Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### Table 14. Configuration Parameter List - General Component Level Traces (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Topology and routing services</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the topology and routing services component.</td>
</tr>
</tbody>
</table>

### Table 15. Configuration Parameter List - Miscellaneous Traces

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Data link control transmissions and receptions</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>If this parameter is enabled, the APPN trace facility will trace all XIDs and PIUs transmitted and received by the APPN node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Trace RTP Headers</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>If this parameter is enabled, the APPN trace facility will trace all headers of RTP flows. This option is available only if Data link control transmissions and receptions is yes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Include payload in RTP trace</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>If this parameter is enabled, the APPN trace facility will trace the payload data in RTP flows. This option is available only if trace RTP headers is yes.</td>
</tr>
</tbody>
</table>
### Table 15. Configuration Parameter List - Miscellaneous Traces (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the Data</td>
<td>Yes, No</td>
<td>No</td>
<td>If this parameter is enabled, the APPN trace facility will filter the trace data according to the way you answer the following questions.</td>
</tr>
<tr>
<td>Truncate the data</td>
<td>Yes, No</td>
<td>No</td>
<td>If this parameter is enabled, the APPN trace facility will truncate the trace data. You will be asked to specify the <em>length to trace</em>.</td>
</tr>
<tr>
<td>Length to trace</td>
<td>1 - 3600</td>
<td>100</td>
<td>This parameter specifies the number of bytes of trace data to accumulate.</td>
</tr>
<tr>
<td>Trace Locates</td>
<td>Yes, No</td>
<td>No</td>
<td>If this parameter is enabled, the APPN trace facility will trace locates.</td>
</tr>
<tr>
<td>Parameter Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trace TDUs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes, No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If this parameter is enabled, the APPN trace facility will trace topology data updates.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Trace route setups</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>If this parameter is enabled, the APPN trace facility will trace route setups.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Trace CP Capabilities</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>If this parameter is enabled, the APPN trace facility will trace CP Capabilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Trace Session Control</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>If this parameter is enabled, the APPN trace facility will trace session control traffic.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Trace XIDs</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>If this parameter is enabled, the APPN trace facility will trace XIDs.</td>
</tr>
</tbody>
</table>
Syntax:
```
set management
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

### Table 16. Configuration Parameter List - APPN Node Management

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect intermediate session information</td>
<td>Yes, No</td>
<td>No</td>
<td>This parameter specifies whether the APPN node should collect data on intermediate sessions passing through this node (session counters and session characteristics). The data is captured in SNMP MIB variables for APPN.</td>
</tr>
<tr>
<td>Save RSCV information for intermediate sessions</td>
<td>Yes, No</td>
<td>No</td>
<td>This parameter specifies whether the APPN node should save the Route Selection control vector (RSCV) for an intermediate session. The data is captured in an associated SNMP MIB variable for APPN.</td>
</tr>
<tr>
<td>Create intermediate session records</td>
<td>Yes, No</td>
<td>No</td>
<td>This parameter enables or disables the creation of data records for intermediate sessions passing through this node. The records contain information about session counters and session characteristics. RSCV information is also included in the data records if the Save RSCV information for intermediate sessions parameter is enabled.</td>
</tr>
</tbody>
</table>

The session RSCV is carried in the BIND request used to activate a session between two LUs. It describes the optimum route through an APPN network for a particular LU-LU session. The session RSCV contains the CP names and TG associated with each pair of adjacent nodes along a route from an origin node to a destination node.
### Table 16. Configuration Parameter List - APPN Node Management (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

### Table 17. Configuration Parameter List - APPN ISR Recording Media

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

*Table 17. Configuration Parameter List - APPN ISR Recording Media (continued)*

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Maximum memory records per buffer</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 2000</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the maximum number of intermediate session records that may be stored in the memory buffer on the router.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory buffers full</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Stop recording (0), Wrap (1)</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Stop recording (0)</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the action to take when the memory buffer allocated to store intermediate session records becomes full. Select <strong>Stop recording</strong> to instruct the router to discard any new intermediate session records. Select <strong>Wrap</strong> to allow new records to overwrite existing records in the buffer. The oldest records in the buffer are overwritten first.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory record format</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>ASCII (0), Binary (1)</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>ASCII (0)</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the format in which intermediate session records are to be stored in the router’s local memory.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time between database updates</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>60 — 1440 minutes</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>60</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter sets the time in minutes between topology database updates.</td>
</tr>
</tbody>
</table>
Table 17. Configuration Parameter List - APPN ISR Recording Media (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td>• When you enable the collection of intermediate session records, the data associated with the records also is collected, by default, in SNMP.</td>
</tr>
<tr>
<td>• MIB variables for APPN. The MIB variables are updated, in this case, whether or not the Collect intermediate session information parameter (in Table 16 on page 138) has been enabled.</td>
</tr>
<tr>
<td>• Intermediate session data can be stored in router memory.</td>
</tr>
</tbody>
</table>

**Add**

Use the **add** command to add or update:

**Syntax:**

```plaintext
add  port
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 18. Configuration Parameter List - Port Configuration

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Link type</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Ethernet (E)</td>
</tr>
<tr>
<td>Token ring (T)</td>
</tr>
<tr>
<td>ATM (A)</td>
</tr>
<tr>
<td>DLSw (D)</td>
</tr>
<tr>
<td>PPP (P)</td>
</tr>
<tr>
<td>Frame relay (F)</td>
</tr>
<tr>
<td>SDLC (S)</td>
</tr>
<tr>
<td>X.25 (X)</td>
</tr>
<tr>
<td>IP</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the type of link associated with this port.</td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

**Table 18. Configuration Parameter List - Port Configuration (continued)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong> Interface number</td>
</tr>
<tr>
<td><strong>Valid Values</strong> 0 to 65533</td>
</tr>
<tr>
<td><strong>Default Value</strong> 0</td>
</tr>
<tr>
<td><strong>Description</strong> This parameter defines the physical interface number of the hardware interface to which this device is attached.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong> Port name</td>
</tr>
<tr>
<td><strong>Valid Values</strong> A string of 1 to 8 characters, where the first character is alphabetic and the 2nd through 8th characters are alphanumeric.</td>
</tr>
<tr>
<td><strong>Default Value</strong> A unique unqualified name that is automatically generated.</td>
</tr>
<tr>
<td>The name will consist of:</td>
</tr>
<tr>
<td>• TR (token-ring)</td>
</tr>
<tr>
<td>• EN (Ethernet)</td>
</tr>
<tr>
<td>• DLS (DLSw)</td>
</tr>
<tr>
<td>• IP255</td>
</tr>
<tr>
<td>• ATM</td>
</tr>
<tr>
<td>• FR (Frame Relay)</td>
</tr>
<tr>
<td>• X25 (X.25)</td>
</tr>
<tr>
<td>• SDLC (SDLC)</td>
</tr>
<tr>
<td>• PPP (point-to-point)</td>
</tr>
<tr>
<td>• IP</td>
</tr>
<tr>
<td>followed by the interface number.</td>
</tr>
<tr>
<td>You can change the port name to a name of your choice.</td>
</tr>
<tr>
<td><strong>Description</strong> This parameter specifies the name representing this port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong> Enable APPN routing on this port</td>
</tr>
<tr>
<td><strong>Valid Values</strong> Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong> Yes</td>
</tr>
<tr>
<td><strong>Description</strong> This parameter specifies whether APPN routing is to be enabled on this port.</td>
</tr>
</tbody>
</table>
### Table 18. Configuration Parameter List - Port Configuration (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Support multiple PU</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether the port will support multiple subarea.</td>
</tr>
</tbody>
</table>

| **Parameter**          |
| Service any node       |
| **Valid Values**       |
| Yes, No               |
| **Default Value**      |
| Yes                   |
| **Description**        |
| This parameter specifies how the router network node responds to a request from another node to establish a connection over this port. When this parameter is enabled, the network node accepts any request it receives from another node to establish a connection. When this parameter is disabled, the network node accepts connection requests only from nodes that you explicitly define (via link station definitions). This option provides an added level of security for the router network node.  

**Note:** When you disable this parameter, a connection request from an adjacent node will be accepted only if the node’s fully-qualified CP name parameter has been configured for a link station defined on this port.  

When this parameter is enabled (the default), you may still want this network node to be able to initiate connections with specific nodes over this port. |

| **Parameter**          |
| Treat non-configured callers as LEN nodes |
| **Valid Values**       |
| Yes, No               |
| **Default Value**      |
| No                    |
| **Description**        |
| This parameter specifies whether APPN should treat dynamic Network Node callers that do not request CP-CP sessions as LEN nodes. It is applicable only if **service any node** is **yes**.  

If this parameter is **yes**:  
- the router treats the adjacent node as a LEN node regardless of the node type in the received XID3  
- the router sends XID3s stating that the router is a LEN node (an EN with no CP-CP session and no HPR support) |
Table 18. Configuration Parameter List - Port Configuration (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>High-performance routing (HPR) supported</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes for token-ring, Ethernet, Frame Relay, and PPP ports.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates whether link stations on this port will support HPR. This value may be overridden on the link station definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Precedence</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter sets the IPv4 precedence value, which allows BRS precedence filtering of IPv4 encapsulated packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited Resource (PPP and FR over dial circuits only)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>If the dial circuit is dial on demand, the default is Yes. Otherwise, the default is No.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether link stations on this port are a limited resource. This value may be overridden on the link station definition.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support bridged formatted frames (Frame relay only)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether the Frame Relay port will support bridged formatted frames. If you are configuring Frame Relay to support bridged format, you will also need to configure a boundary node identifier.</td>
</tr>
</tbody>
</table>
### Table 18. Configuration Parameter List - Port Configuration (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subnet visit count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>1 - 255</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>Default taken from the equivalent node level parameter</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies this port's default for the maximum number of subnetworks that a multi-subnet session may traverse. <strong>Note:</strong> This question is asked only if the border node function is enabled on this node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Adjacent node subnet affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>0 (native)</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies the default for all links through this port as to whether the adjacent node is in this node's native APPN subnetwork or in a non-native APPN subnetwork. A value of 2 instructs the node to negotiate at link activation time to determine whether the adjacent link station is native or non-native. <strong>Note:</strong> This question is asked only if the border node function is enabled on this node.</td>
</tr>
</tbody>
</table>
### Table 19. Configuration Parameter List - Port Configuration for ATM

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Local ATM Address</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Any 14-hexadecimal character string</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the 7-byte string that comprises the user part of the local ATM address. The user part is the 6-byte ESI and the 1-byte selector field. This user-part must be unique with respect to the network part of the ATM address, which is retrieved from the ATM adapter. The selector must be unique for each protocol type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable incoming calls</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter determines whether calls will be rejected at the ATM level.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM Network Type</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Campus or Widearea</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Campus</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the network type used for default values for connection networks and other link stations defined on this port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shareable connection network traffic</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether connection network traffic can be routed on the ATM VC set up for a link station on this port.</td>
</tr>
<tr>
<td>Parameter Information</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Shareable other protocol traffic</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether other higher level protocol traffic can be routed on the ATM VC set up for a link station on this port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadband Bearer Class</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Class_A, Class_C, Class_X</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Class_X</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the bearer class requested from the ATM network. The classes are defined:</td>
</tr>
<tr>
<td><strong>Class A</strong></td>
</tr>
<tr>
<td>Constant bit rate (CBR) with end-to-end timing requirements</td>
</tr>
<tr>
<td><strong>Class C</strong></td>
</tr>
<tr>
<td>Variable bit rate (VBR) with no end-to-end timing requirements</td>
</tr>
<tr>
<td><strong>Class X</strong></td>
</tr>
<tr>
<td>Service allowing user-defined traffic type and timing requirements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Effort Indicator</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates if a throughput guarantee is required on this SVC. If the value of this parameter is yes, then VCCs associated with this interface will be allocated based upon the available bandwidth.</td>
</tr>
</tbody>
</table>

**Note:** The following parameters are forward traffic parameters.
### Table 19. Configuration Parameter List - Port Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Forward Traffic Peak Cell Rate</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>1 - 85% of line speed</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Port’s Default Effective Capacity/48</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter indicates an upper bound on the cell transmission rate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Traffic Sustained Cell Rate</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>1 - 85% of line speed</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Port’s Default Effective Capacity/48</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter indicates an upper bound on the average cell transmission rate. You cannot specify this parameter if you are using a Best Effort connection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Traffic Tagging</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network. You cannot specify this parameter if you are using a Best Effort connection.</td>
</tr>
</tbody>
</table>
### Table 19. Configuration Parameter List - Port Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Forward QoS</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where</td>
</tr>
<tr>
<td><strong>CLASS_0</strong></td>
</tr>
<tr>
<td>The unspecified class. The network does not specify any QoS.</td>
</tr>
<tr>
<td><strong>CLASS_1</strong></td>
</tr>
<tr>
<td>Performance is comparable to current digital private line performance.</td>
</tr>
<tr>
<td><strong>CLASS_2</strong></td>
</tr>
<tr>
<td>Intended for packetized video and audio in teleconferencing and multimedia applications.</td>
</tr>
<tr>
<td><strong>CLASS_3</strong></td>
</tr>
<tr>
<td>Intended for interoperation of connection-oriented protocols, such as Frame Relay.</td>
</tr>
<tr>
<td><strong>CLASS_4</strong></td>
</tr>
<tr>
<td>Intended for interoperation of connectionless protocols, such as IP.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>CLASS_0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates which class of service is provided to an ATM virtual connection. This parameter is always CLASS_0 for a Best Effort connection.</td>
</tr>
</tbody>
</table>

**Note:** The following parameters are backward traffic parameters.

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Backward Traffic Peak Cell Rate</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 - 85% of line speed</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Port’s Default Effective Capacity/48</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates an upper bound on the cell transmission rate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Backward Traffic Sustained Cell Rate</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 - 85% of line speed</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Port’s Default Effective Capacity/48</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates an upper bound on the average cell transmission rate. You cannot specify this parameter for a Best Effort connection.</td>
</tr>
</tbody>
</table>
### Table 19. Configuration Parameter List - Port Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Backward Traffic Tagging</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes, unless Best Effort connection</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network. You cannot specify this parameter for a Best Effort connection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Backward QoS</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where</td>
</tr>
<tr>
<td><strong>CLASS_0</strong></td>
</tr>
<tr>
<td>The unspecified class. The network does not specify any QoS.</td>
</tr>
<tr>
<td><strong>CLASS_1</strong></td>
</tr>
<tr>
<td>Performance is comparable to current digital private line performance.</td>
</tr>
<tr>
<td><strong>CLASS_2</strong></td>
</tr>
<tr>
<td>Intended for packetized video and audio in teleconferencing and multimedia applications.</td>
</tr>
<tr>
<td><strong>CLASS_3</strong></td>
</tr>
<tr>
<td>Intended for interoperation of connection-oriented protocols, such as Frame Relay.</td>
</tr>
<tr>
<td><strong>CLASS_4</strong></td>
</tr>
<tr>
<td>Intended for interoperation of connectionless protocols, such as IP.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>CLASS_0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates which class of service is provided to an ATM virtual connection. You cannot specify this parameter for a Best Effort connection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Callout Anonymously</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, no</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>no</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates whether APPN will pass the source address when making the call.</td>
</tr>
</tbody>
</table>
Table 19. Configuration Parameter List - Port Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>LDLC retry count</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 — 255</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter is used in conjunction with the LDLC timer period to provide reliable delivery of XIDs. The retry count is initialized when a command or request is first transmitted over the link. If the LDLC timer period expires before a response is received, the command or request is retransmitted, the retry count is decremented, and the LDLC timer period is restarted. If the timer expires with the retry count at 0, the link is assumed to be inoperative.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>LDLC Timer Period</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 — 255 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>For ATM: 1 second</td>
</tr>
<tr>
<td>For IP: 15 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the timer period used with the LDLC retry count.</td>
</tr>
<tr>
<td>Parameter Information</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Maximum BTU size</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>768 to 1496 bytes for Ethernet</td>
</tr>
<tr>
<td>768 to 17 745 bytes for token-ring</td>
</tr>
<tr>
<td>768 to 4096 bytes for ATM</td>
</tr>
<tr>
<td>768 to 4096 bytes for IP</td>
</tr>
<tr>
<td>768 to 8136 bytes for Frame Relay</td>
</tr>
<tr>
<td>768 to 8132 bytes for Frame Relay over ISDN and V.25 bis</td>
</tr>
<tr>
<td>768 to 4086 bytes for PPP</td>
</tr>
<tr>
<td>768 to 4082 bytes for PPP over ISDN and V.25 bis</td>
</tr>
<tr>
<td>X.25 will take value from network level</td>
</tr>
<tr>
<td>768 to 2048 bytes for all other ports</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>1289 bytes for Ethernet</td>
</tr>
<tr>
<td>2048 bytes for token-ring</td>
</tr>
<tr>
<td>2048 for ATM</td>
</tr>
<tr>
<td>1469 bytes for IP</td>
</tr>
<tr>
<td>2048 bytes for Frame Relay or PPP</td>
</tr>
<tr>
<td>2044 bytes for Frame Relay or PPP over ISDN and V.25 bis</td>
</tr>
<tr>
<td>2048 bytes for SDLC</td>
</tr>
<tr>
<td>X.25 will take value from network level</td>
</tr>
</tbody>
</table>

**Description**

This parameter specifies the number of bytes in the largest basic transmission unit (BTU) that can be processed (transmitted or received) by a link station defined on this port.

**Note:** If a negotiable BIND with an RU size greater than 2048 is received, the device will normally choose a maximum RU size of 2048. If a non-negotiable BIND with an RU size greater than 2048 is received, the device will support the larger RU size up to a maximum size of 4096.
### Table 20. Configuration Parameter List - Port Definition (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Maximum number of link stations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>1 to 127 for SDLC ports</td>
</tr>
<tr>
<td></td>
<td>1 to 65 535 for all other ports</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>If SDLC is configured as multipoint and primary, then this parameter defaults to 127.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies the maximum number of link stations that will be allowed to use this port. This parameter allows the resources for the APPN node and this port to be constrained.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Percent of link stations reserved for incoming calls (Ethernet, token-ring, FR, X.25 only)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>0 to 100</td>
</tr>
<tr>
<td></td>
<td>The sum of the percent of link stations reserved for incoming calls and the percent of link stations reserved for outgoing calls cannot exceed 100%.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies the percentage of the maximum number of link stations that will be reserved for incoming calls. Link stations that are not reserved for incoming or outgoing calls are available for either purpose on a demand basis.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Percent of link stations reserved for outgoing calls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>0 to 100</td>
</tr>
<tr>
<td></td>
<td>The sum of the percent of link stations reserved for incoming calls and the percent of link stations reserved for outgoing calls cannot exceed 100%. If SDLC primary and multipoint, then valid value is 100.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>0 If SDLC primary and multipoint, then default value is 100.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies the percentage of the maximum number of link stations that will be reserved for outgoing calls. Fractions resulting from the computation are truncated. Link stations that are not reserved for incoming or outgoing calls are available for either purpose on a demand basis.</td>
</tr>
</tbody>
</table>
### Table 20. Configuration Parameter List - Port Definition (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>UDP port number for XID exchange</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1024 to 65 535</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>11 000</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the UDP port number to be used for XID exchange and is used during IP port definition. This port number must be the same as the one defined on other devices in the network.</td>
</tr>
</tbody>
</table>

| **Parameter**          |
| UDP port number for network priority traffic |
| **Valid Values**       |
| 1024 to 65 535         |
| **Default Value**      |
| 11 001                 |
| **Description**        |
| This parameter specifies the UDP port number to be used for network priority traffic. |

| **Parameter**          |
| UDP port number for high priority traffic |
| **Valid Values**       |
| 1024 to 65 535         |
| **Default Value**      |
| 11 002                 |
| **Description**        |
| This parameter specifies the UDP port number to be used for high priority traffic. |

| **Parameter**          |
| UDP port number for medium priority traffic |
| **Valid Values**       |
| 1024 to 65 535         |
| **Default Value**      |
| 11 003                 |
| **Description**        |
| This parameter specifies the UDP port number to be used for medium priority traffic. |
Table 20. Configuration Parameter List - Port Definition (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>UDP port number for low priority traffic</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1024 to 65 535</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>11 004</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the UDP port number to be used for low priority traffic.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>IP network type</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Campus or Widearea</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Widearea</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the IP network type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Local APPN SAP address</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Multiples of four in the hexadecimal range X'04' to X'EC'</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>X'04'</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the local SAP address to be used for communicating with APPN link stations defined on this port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Local HPR SAP address (Ethernet and token-ring only)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Multiples of four in the hexadecimal range X'04' to X'EC'</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>X'C8'</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates the local service access point to be used for communicating with HPR link stations defined on this port.</td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

Table 20. Configuration Parameter List - Port Definition (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Branch uplink</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

This parameter indicates whether the default for link stations using this port will be uplink or downlink. If yes is specified, link stations using this port will default Branch uplink to yes.

**Notes:**
1. This question is asked only if the node-level parameter Enabled Branch Extender is yes.
2. If Branch uplink is yes, the Branch Extender will present its end node appearance to this link station. Otherwise, the Branch Extender will present its network node appearance.
3. Typically, Branch uplink is yes for WAN-attached network nodes and is no for LAN-attached end nodes.
<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>For ATM SVCs:</td>
</tr>
<tr>
<td>Campus ATM best effort</td>
</tr>
<tr>
<td>Campus ATM reserved</td>
</tr>
<tr>
<td>WAN ATM best effort</td>
</tr>
<tr>
<td>WAN ATM reserved</td>
</tr>
<tr>
<td>For ATM PVCs:</td>
</tr>
<tr>
<td>Campus ATM best effort</td>
</tr>
<tr>
<td>Campus ATM reserved</td>
</tr>
<tr>
<td>WAN ATM best effort</td>
</tr>
<tr>
<td>WAN ATM reserved</td>
</tr>
<tr>
<td>For IP: 0 for Campus and WAN</td>
</tr>
<tr>
<td>For all other: 0</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

The cost per connect time TG characteristic expresses the relative cost of maintaining a connection over the associated TG. The units are user-defined and are typically based on the applicable tariffs of the transmission facility being used. The assigned values should reflect the actual expense of maintaining a connection over the TG relative to all other TGs in the network. A value of zero means that connections over the TG may be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.
APPN Configuration Commands

Table 21. Configuration Parameter List - Port Default TG Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>

For ATM SVCs and ATM PVCs:

- **Campus ATM best effort**: 0
- **Campus ATM reserved**: 0
- **WAN ATM best effort**: 128
- **WAN ATM reserved**: 0

For IP: 0 for Campus and WAN

For all other: 0

**Description**

This parameter specifies the cost per byte TG characteristic for all link stations defined on this port.

The cost per byte TG characteristic expresses the relative cost of transmitting a byte over the associated TG. The units are user-defined and the assigned value should reflect the actual expenses incurred for transmitting over the TG relative to all other TGs in the network. A value of zero means that bytes may be transmitted over the TG at no additional cost. Higher values represent higher costs.
Table 21. Configuration Parameter List - Port Default TG Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Nonsecure</td>
</tr>
<tr>
<td>Public switched network</td>
</tr>
<tr>
<td>Underground cable</td>
</tr>
<tr>
<td>Secure conduit</td>
</tr>
<tr>
<td>Guarded conduit</td>
</tr>
<tr>
<td>Encrypted</td>
</tr>
<tr>
<td>Guarded radiation</td>
</tr>
</tbody>
</table>

**Default Value**

For ATM SVCs and ATM PVCs:
- **Campus ATM best effort**
  - Nonsecure
- **Campus ATM reserved**
  - Nonsecure
- **WAN ATM best effort**
  - Public switched network
- **WAN ATM reserved**
  - Public switched network

For IP:
- **Campus**
  - Nonsecure
- **WAN**
  - Public switched network

For all other: Nonsecure

**Description**

This parameter specifies the security TG characteristic for all link stations defined on this port. The security TG characteristic indicates the level of security protection associated with the TG. If security attributes other than the architecturally-defined ones are needed, one of the user-defined TG characteristics may be used to specify additional values.
### Parameter Information

#### Parameter
- Propagation delay

#### Valid Values
- **Minimum LAN**
  - less than 480 microseconds
- **Telephone**
  - between .48 and 49.152 milliseconds
- **Packet switched**
  - between 49.152 and 245.76 milliseconds
- **Satellite**
  - greater than 245.76 milliseconds maximum

#### Default Value
- For ATM SVCs and ATM PVCs:
  - **Campus ATM best effort**
    - Telephone
  - **Campus ATM reserved**
    - Minimum LAN
  - **WAN ATM best effort**
    - Packet switched
  - **WAN ATM reserved**
    - Telephone
- For IP:
  - **Campus**
    - Telephone
  - **WAN**
    - Packet switched

#### Description
This parameter specifies the propagation delay TG characteristic for all link stations defined on this port. The propagation delay TG characteristic specifies the approximate range for the length of time that it takes for a signal to propagate from one end of the TG to the other.
Table 21. Configuration Parameter List - Port Default TG Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>For ATM SVCs (25 Mbps) and ATM PVCs (25Mbps):</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>For IP:</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

| **Description**        | This parameter specifies the effective capacity TG characteristic for all associated connections (TGs) on this port. |
|                       | This parameter specifies the maximum bit transmission rate for both physical links and logical links. Note that the effective capacity for a logical link may be less than the physical link speed. The rate is represented in COS files as a floating-point number encoded in a single byte with units of 300 bps. The effective capacity is encoded as a single-byte representation. The values X'00' and X'FF' are special cases used to denote minimum and maximum capacities. The range of the encoding is very large; however, only 256 values in the range may be specified. |
|                       | This parameter provides the default value for the Effective capacity parameter on the Modify TG Characteristics Command Line option. The Modify TG Characteristics Command Line option enables you to override the .* default values assigned to TG characteristics on the individual link stations you define. |
### Table 21. Configuration Parameter List - Port Default TG Characteristics  (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>
| **Description**       | This parameter specifies the first user-defined TG characteristic for all link stations defined on this port.  

The first user-defined TG characteristic specifies the first of three additional characteristics that users can define to describe the TGs in a network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs. |

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>
| **Description**       | This parameter specifies the second user-defined TG characteristic for all link stations defined on this port.  

The second user-defined TG characteristic specifies the second of three additional characteristics that users can define to describe the TGs in a network. |

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>
| **Description**       | This parameter specifies the third user-defined TG characteristic for all link stations defined on this port.  

The third user-defined TG characteristic specifies the third of three additional characteristics that users can define to describe the TGs in a network. |
## Table 22. Configuration Parameter List - Port default LLC Characteristics

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Maximum number of outstanding I-format LPDUs (TW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>1 to 127</td>
</tr>
<tr>
<td>Default Value</td>
<td>26</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter specifies the LLC maximum number of outstanding I-format LPDUs (TW) for all link stations on this port. The maximum number of outstanding I-format LPDUs defines the transmit Command Line option (TW) which is the maximum number of sequentially numbered I-format LPDUs that the link station may have unacknowledged at any given time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Receive window size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>1 to 127</td>
</tr>
<tr>
<td>Default Value</td>
<td>26</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter specifies the LLC receive Command Line option size (RW) for all link stations on this port. The RW parameter specifies the maximum number of unacknowledged sequentially numbered I-format LPDUs that the link station can receive from the remote link station. RW is advertised in SNA XID frames and IEEE 802.2 XID frames. The XID receiver should set its effective TW to a value less than or equal to the value of the received RW to avoid overruns.</td>
</tr>
</tbody>
</table>
### Table 22. Configuration Parameter List - Port default LLC Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Inactivity timer (Ti)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>30 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the LLC inactivity timer (Ti) for all link stations on this port.</td>
</tr>
<tr>
<td>An LLC link station uses Ti to detect an inoperative condition in either the remote link station or in the transmission media. If an LPDU is not received in the time interval specified by Ti, an S-format command LPDU with the poll bit set is transmitted to solicit remote link station status. Recovery is then based on the reply timer (T1).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Reply timer (T1)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>2 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the LLC reply timer (T1) for all link stations on this port.</td>
</tr>
<tr>
<td>An LLC link station uses T1 to detect a failure to receive a required acknowledgment or response from the remote link station. When T1 expires, the link station sends an S-format command link layer protocol data unit (LPDU) with the poll bit set to solicit remote link station status or any U-format command LPDUs that have not been responded to. The duration of T1 should take into account any delays introduced by underlying layers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Maximum number of retransmissions (N2)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the maximum number of retransmissions (N2) for all link stations on this port.</td>
</tr>
<tr>
<td>The N2 parameter specifies the maximum number of times an LPDU will be retransmitted following expiration of the reply timer (T1).</td>
</tr>
</tbody>
</table>
### Table 22. Configuration Parameter List - Port default LLC Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Receive acknowledgment timer (T2)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254, measured in tenths of a second</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the LLC receiver acknowledgment timer (T2) for all link stations on this port. The T2 parameter may be used with the N3 counter to reduce acknowledgment traffic. A link station uses T2 to delay the sending of an acknowledgment for a received I-format LPDU. T2 is started when an I-format LPDU is received, and reset when an acknowledgment is sent in an I-format or S-format LPDU. If T2 expires, the link station must send an acknowledgment as soon as possible. The value of T2 must be less than that of T1, to ensure that the remote link station will receive the delayed acknowledgment before its T1 expires.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Acknowledgments needed to increment working window</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 127</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>When the working window (Ww) is not equal to the Maximum Transmit Window Size (Tw), this parameter is the number of transmitted I-format LPDUs that must be acknowledged before the working window can be incremented (by 1). When congestion is detected, by the loss of I-format LPDUs, Ww is set to 1.</td>
</tr>
</tbody>
</table>

### Table 23. Configuration Parameter List - HPR Override Defaults

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Inactivity timer override for HPR (HPR Ti)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>2 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the LLC inactivity timer (HPR Ti) that is to be used for all link stations on this port supporting HPR when the HPR supported parameter is enabled on this port. This default overrides the value of the default LLC inactivity timer (Ti) parameter specified on the default LLC characteristics parameter.</td>
</tr>
</tbody>
</table>
### Table 23. Configuration Parameter List - HPR Override Defaults (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Reply timer override for HPR (HPR T1)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>2 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the LLC reply timer (HPR T1) that is to be used for all link stations on this port supporting HPR when the HPR supported parameter is enabled on this port. This default overrides the value of the default LLC reply timer (T1) parameter specified on the default LLC characteristics parameter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of retransmissions for HPR (HPR N2)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the LLC maximum number of retransmissions (HPR N2) that is to be used for all link stations on this port supporting HPR when the HPR supported parameter is enabled on this port. This default overrides the value of the default LLC maximum number of retransmissions (N2) parameter specified on the default LLC Characteristics parameter.</td>
</tr>
</tbody>
</table>

**Syntax:**

```
add link-station
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

### Table 24. Configuration Parameter List - Link Station - Detail

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Does link support APPN function</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether this link station will support APPN function. If the answer is no, questions concerning CP-CP sessions, security, encryption, CP name, adjacent node type, branch extender, and extended border node will not be asked and all of these functions will be disabled. Also, HPR will be disabled and no HPR questions will be asked.</td>
</tr>
</tbody>
</table>
Table 24. Configuration Parameter List - Link Station - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Link station name (required)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 1 to 8 characters :</td>
</tr>
<tr>
<td>• First character: A to Z</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of a link station that represents the TG (link) between the router network node and the adjacent node. The link station name must be unique within this network node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Port name</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A unique unqualified name that is automatically generated.</td>
</tr>
<tr>
<td>The name will consist of:</td>
</tr>
<tr>
<td>• TR (token-ring)</td>
</tr>
<tr>
<td>• EN (Ethernet)</td>
</tr>
<tr>
<td>• DLS (DLSw)</td>
</tr>
<tr>
<td>• FR (Frame Relay)</td>
</tr>
<tr>
<td>• X25 (X.25)</td>
</tr>
<tr>
<td>• SDLC (SDLC)</td>
</tr>
<tr>
<td>• PPP (point-to-point)</td>
</tr>
<tr>
<td>• IP</td>
</tr>
<tr>
<td>followed by the interface number.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>The name of the port that this link station is defined on.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name representing the port this link station is defined on. The port must already have been configured for APPN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Link type (X.25 and ATM only)</td>
</tr>
<tr>
<td>If limited resource = yes is configured for this link station, then the link type parameter defaults to a value of 1 (SVC) and is not configurable.</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>If PVC, then specify a logical channel number in the range of 1 - 4095</td>
</tr>
<tr>
<td>If SVC, then specify a DTE address that is variable length up to 15 digits</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>0, unless it is a limited resource.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether the X.25 link is a PVC or SVC.</td>
</tr>
</tbody>
</table>
### Table 24. Configuration Parameter List - Link Station - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>MAC address of adjacent node (required) (Ethernet, token-ring, DLSw, FR bridged format only)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
</tbody>
</table>
| Token-ring and DLSw ports:  
  - 12 hexadecimal digits in the range X'000000000001' to X'7FFFFFFF' |
| Ethernet/802.3 ports:  
  - 12 hexadecimal digits in the form X'xyxxxxxxxxx' where:  
    - x is any hexadecimal digit  
    - y is a hexadecimal digit in the set {0, 2, 4, 6, 8, A, C, E} |
| **Default Value** |
| None |
| **Description** |
| This parameter specifies the medium access control (MAC) layer address of the adjacent node. Different formats are used for token-ring and Ethernet/802.3.  
  
  **Token-ring and DLSw ports:**  
  The MAC address is specified in noncanonical form. In the noncanonical address format, the bit within each octet that is to be transmitted first is represented as the most significant bit.  
  
  **Ethernet/802.3 ports:**  
  The MAC address is specified in canonical form. In the canonical address format, the bit within each octet that is to be transmitted first is represented as the least significant bit. |

| **Parameter** |
| IP address of adjacent node (Enterprise Extender only) |
| **Valid Values** |
| Any valid IP address |
| **Default Value** |
| none |
| **Description** |
| Each link on the HPR/IP port must have a unique destination IP address. |
### Parameter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Adjacent node type</th>
</tr>
</thead>
</table>

**Valid Values**
- APPN network node, APPN end node, LEN end node

**Default Value**
- APPN network node

**Description**
This parameter identifies whether the adjacent node is an APPN node, a low-entry networking (LEN) end node.

When **APPN end node** is selected and **Limited resource** is No, APPN changes the adjacent node type internally to learn and will work with any node type.

When **APPN end node** is selected and **Limited resource** is Yes, the adjacent node type is unchanged.

When you select **LEN end node**, the fully-qualified control point name parameter is a required parameter. If this network node is communicating with the IBM Virtual Telecommunications Access Method (VTAM) product through the LEN node, and the LEN node is not a T2.1 node or does not have an explicitly defined control point (CP) name, then the router network node’s XID number for the Subarea connection parameter also must be specified to establish a connection.

**Note:** **LEN end node** is not a valid node type for HPR/IP interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>XID node identification</th>
</tr>
</thead>
</table>

**Valid Values**
- A string of 8 hex digits (0-F)

**Default Value**
- X’00000000’

**Description**
This parameter specifies the ID block and ID number fields that identify the adjacent node. It is applicable only when the **Adjacent node type** field is set to **LEN end node**. If you choose yes for replace inbound XID3 CP name and XID with configured values, the value of this field replaces the corresponding parameters in the received XID.
### APPN Configuration Commands

#### Table 24. Configuration Parameter List - Link Station - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> An existing fully-qualified CP name, using the special characters @, $, and from the character set A, continues to be supported; however, these characters should not be used for new CP names.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Note:</strong> This parameter is required when any of the following occur:</td>
</tr>
<tr>
<td>• The Service any node parameter is set to Disable.</td>
</tr>
<tr>
<td>• The Adjacent node type parameter is set to LEN end node.</td>
</tr>
<tr>
<td>• The CP-CP session level security parameter is set to Enable.</td>
</tr>
<tr>
<td>• The link is a limited resource.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>If you have a large number of LEN nodes that are not configured adequately to participate in a full APPN network, you can configure their identity at the router and have the router override the values in their XIDs before forwarding those XIDs on.</td>
</tr>
</tbody>
</table>
### Parameter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activate link automatically</strong></td>
<td>When this parameter is enabled, the router network node automatically activates the link to the adjacent node and initiates a connection.</td>
</tr>
<tr>
<td><strong>Retry link activation unconditionally</strong></td>
<td>This parameter specifies whether or not the router should always try to reactivate the link regardless of the cause of link failure. It is applicable only for dial-out capable links where activate link automatically is yes. Normally if a link fails to start or comes down due to some event other than an operator command, the router selectively chooses whether to reactivate it. If the failure cause is likely to require reconfiguration of one of the two nodes, the router does not automatically restart the link. This avoids a periodic repeat (with logging, alarming, etc.) of the unsuccessful connection attempt. If you want to override this behavior and have links always attempt to reconnect, select yes for this parameter.</td>
</tr>
<tr>
<td><strong>Allow CP-CP sessions on this link</strong></td>
<td>This parameter specifies whether sessions between control points are to be activated over this link station. This parameter allows control of CP-CP session establishment between adjacent network nodes so that the overhead associated with topology database updates (TDUs) may be constrained. <strong>Note:</strong> Every APPN network node must have at least one CP-CP session established to another APPN network node in order to maintain the minimum connectivity necessary to update the topology database. In addition, more than minimum connectivity could be desired to eliminate single points of failure and to improve network dynamics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate link automatically</td>
<td>Yes, No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Retry link activation unconditionally</td>
<td>Yes, No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Allow CP-CP sessions on this link</td>
<td>Yes, No</td>
<td>Yes, if adjacent node type is APPN network node or APPN end node. No for all other adjacent node types</td>
<td></td>
</tr>
</tbody>
</table>

---

**APPN Configuration Commands**

*Chapter 3. Configuring and Monitoring APPN*
### APPN Configuration Commands

Table 24. Configuration Parameter List - Link Station - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption key</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use enhanced session security (If security is enabled)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-performance routing (HPR) supported</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
Table 24. Configuration Parameter List - Link Station - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Station address of adjacent node (SDLC only)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited Resource (PPP, X.25 FR over dial circuits, ATM)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch Uplink</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### Table 24. Configuration Parameter List - Link Station - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred Network Node Server</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>
| **Description** | This parameter indicates whether this uplink is to a network node server that is to be used as the network node server for the node supporting Branch Extender function and acting as an end node. If yes is specified, this uplink will be used as the network node server for this node. This question will be asked only if:  
  - Enabled Branch Extender is yes,  
  - This station is a network node,  
  - Branch Uplink is yes, and  
  - CP-CP sessions are supported on this link. |

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>TG Number</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
**Table 24. Configuration Parameter List - Link Station - Detail (continued)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
</table>

**Parameter**
- Solicit SSCP session

**Valid Values**
- Yes or No

**Default Value**
- No

If the link station name is the same as the CP name, then the default is yes.

**Description**
- This parameter indicates whether this link is to solicit SSCP sessions.

**Parameter**
- Local Node ID

**Valid Values**
- 5 hexadecimal digits

**Default Value**
- X'00000'

**Description**
- This parameter specifies the local node identifier that represents the local dependent PU to VTAM. This question is asked only if Solicit SSCP session is yes. The local node id must be unique.

**Parameter**
- Enable Host Initiated Dynamic LU Definition

**Valid Values**
- Yes or No

**Default Value**
- No

**Description**
- This parameter indicates whether or not dependent LUs will be created dynamically (as opposed to having to be configured.) If yes is specified, LUs will be defined for this PU as ACTLU requests (with CV0E) are received. With this feature, LUs for the TN3270E Server do not have to be configured.

**Note:** This question is asked only if Solicit SSCP session is yes.
### Table 24. Configuration Parameter List - Link Station - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Pool Name for Host-initiated Dynamic LUs</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>• First character: A to Z, $, #, @, or &lt;</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9, $, #, @, &gt;, or &lt;</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of a pool to be created to contain LUs that the host activates on this subarea link. This parameter is applicable only if Solicit SSCP session is yes, and Enable Host Initiated Dynamic LU Definition is yes.</td>
</tr>
<tr>
<td>You do not need to use the add implicit-pool command to define this pool; specifying the name and other parameters here is sufficient to cause the pool to be created. If you do enter a pool name, you will be prompted to enter values for the following parameters:</td>
</tr>
<tr>
<td>• Pool class (See Table 42 on page 219)</td>
</tr>
<tr>
<td>• LU type (See Table 42 on page 219)</td>
</tr>
<tr>
<td>You can provide the same pool name for multiple subarea links, if you wish.</td>
</tr>
<tr>
<td>By specifying pool information, you cause host-initiated LUs that are not already configured at the router to be placed into the specified pool. TN3270 clients can then be assigned to them by requesting the pool name, or by mapping client IP addresses or destination ports to that pool.</td>
</tr>
<tr>
<td>If you do not specify pool information, these host-initiated LUs are treated as explicit LUs and can only be assigned to clients that request them by their individual LU names.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Local SAP address</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Any valid SAP address between X’04’ and X’EC’.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Value taken from port</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies local SAP address.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td>1. This question is displayed only if there are multiple PUs defined on the port.</td>
</tr>
<tr>
<td>2. If the local SAP address is not the main local SAP address on the port,</td>
</tr>
<tr>
<td>3. the port name and SAP name will display in monitoring and SNMP display output.</td>
</tr>
<tr>
<td>Parameter Information</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Send Terminate-Self when TN3270 Client Disconnects</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
<th>Yes or No</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
<th>No</th>
</tr>
</thead>
</table>

| Description | This parameter indicates whether or not a terminate_self request will be sent to the SSCP when the TN3270 client disconnects. If yes is specified, terminate_self will be sent and the host will be responsible for terminating the LU-LU session (i.e., the SLU will NOT send an UNBIND request.) |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subnet visit count</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
<th>1 - 255</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
<th>Default taken from the equivalent port level parameter</th>
</tr>
</thead>
</table>

| Description | This parameter specifies the default for the maximum number of subnetworks that a multi-subnet session may traverse. Note: This question is asked only if the border node function is enabled on this node. |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Adjacent node subnet affiliation</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
<th>0 (native)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 1 (non-native)</td>
<td></td>
</tr>
<tr>
<td>• 2 (negotiable)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
<th>Default is taken from the equivalent port level parameter</th>
</tr>
</thead>
</table>

| Description | This parameter specifies whether the adjacent node is in this node’s native APPN subnetwork or in a non-native APPN subnetwork. A value of 2 instructs the node to negotiate at link activation time to determine whether the adjacent link station is native or non-native. Note: This question is asked only if the border node function is enabled on this node. |
### Table 25. Configuration Parameter List - Station Configuration for ATM

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Virtual Channel Type</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>SVC, PVC</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>SVC</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter identifies the ATM channel type as switched virtual circuit (SVC) or permanent virtual circuit (PVC).</td>
</tr>
</tbody>
</table>

**Note:** The following parameters are common for SVCs and PVCs.

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination ATM Address</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A 40-character hexadecimal string</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the 20-byte string that comprises the entire destination ATM address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM network type</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Campus, Widearea</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Campus</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the ATM network type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shareable connection network traffic</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether connection network traffic can be routed on the ATM VC set up this TG.</td>
</tr>
</tbody>
</table>
Table 25. Configuration Parameter List - Station Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Shareable other protocol traffic</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter specifies whether other higher level protocol traffic can be routed on the ATM VC set up for this TG.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>LDLC retry count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>1 — 255</td>
</tr>
<tr>
<td>Default Value</td>
<td>3</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>This parameter is used in conjunction with the LDLC timer period to provide reliable delivery of XIDs. The retry count is initialized when a command or request is first transmitted over the link. If the LDLC timer period expires before a response is received, the command or request is retransmitted, the retry count is decremented, and the LDLC timer period is restarted. If the timer expires with the retry count at 0, the link is assumed to be inoperative.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>LDLC Timer Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>1 — 255 seconds</td>
</tr>
<tr>
<td>Default Value</td>
<td></td>
</tr>
<tr>
<td>For ATM: 1 second</td>
<td></td>
</tr>
<tr>
<td>For IP: 15 seconds</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>This parameter specifies the timer period used with the LDLC retry count.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>VPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>0 — 255</td>
</tr>
<tr>
<td>Default Value</td>
<td>0</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>This parameter identifies the VPI of the PVC at the interface.</td>
<td></td>
</tr>
</tbody>
</table>
**APPN Configuration Commands**

*Table 25. Configuration Parameter List - Station Configuration for ATM (continued)*

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>VCI</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 65535</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter identifies the VCI of the PVC at the interface.</td>
</tr>
</tbody>
</table>

| **Parameter**         |
| Broadband Bearer Class |
| **Valid Values**      |
| Class_A, Class_C, Class_X |
| **Default Value**     |
| Class_X               |
| **Description**       |
| This parameter specifies the bearer class requested from the ATM network. The classes are defined: |
| **Class A**           |
| Constant bit rate (CBR) with end-to-end timing requirements |
| **Class C**           |
| Variable bit rate (VBR) with no end-to-end timing requirements |
| **Class X**           |
| Service allowing user-defined traffic type and timing requirements |

| **Parameter**         |
| Best Effort Indicator |
| **Valid Values**      |
| Yes, No               |
| **Default Value**     |
| No                    |
| **Description**       |
| This parameter indicates if a throughput guarantee is required on this SVC. If the value of this parameter is yes, then VCCs associated with this interface will be allocated based upon the available bandwidth. |

**Note:** The following parameters are forward traffic parameters.
### Table 25. Configuration Parameter List - Station Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Forward Peak Cell Rate</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>85% of line speed</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Port’s Default Effective Capacity/48</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates an upper bound on the cell transmission rate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Forward Sustained Cell Rate</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 - 85% of line speed</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Port’s Default Effective Capacity/48</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates an upper bound on the average cell transmission rate. You cannot specify this parameter for Best Effort connections.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Forward Tagging</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network. You cannot specify this parameter for Best Effort connections.</td>
</tr>
</tbody>
</table>
### Table 25. Configuration Parameter List - Station Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong> QoS</td>
</tr>
<tr>
<td><strong>Valid Values</strong> CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where</td>
</tr>
<tr>
<td>CLASS_0 The unspecified class. The network does not specify any QoS.</td>
</tr>
<tr>
<td>CLASS_1 Performance is comparable to current digital private line performance.</td>
</tr>
<tr>
<td>CLASS_2 Intended for packetized video and audio in teleconferencing and multimedia applications.</td>
</tr>
<tr>
<td>CLASS_3 Intended for interoperation of connection-oriented protocols, such as Frame Relay</td>
</tr>
<tr>
<td>CLASS_4 Intended for interoperation of connectionless protocols, such as IP.</td>
</tr>
<tr>
<td><strong>Default Value</strong> CLASS_0</td>
</tr>
<tr>
<td><strong>Description</strong> This parameter indicates which class of service is provided to an ATM virtual connection. You cannot specify this parameter for Best Effort connections.</td>
</tr>
</tbody>
</table>

**Note:** The following parameters are backward traffic parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Backward Peak Cell Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>1 - 85% of line speed</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>Taken from the port definition</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter indicates an upper bound on the cell transmission rate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Backward Sustained Cell Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>1 - 85% of line speed</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>Taken from the port definition</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter indicates an upper bound on the average cell transmission rate. You cannot specify this parameter for Best Effort connections.</td>
</tr>
</tbody>
</table>
### Table 25. Configuration Parameter List - Station Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Backward Tagging</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network. You cannot specify this parameter for Best Effort connections.</td>
</tr>
</tbody>
</table>

| **Parameter**         |
| QoS                   |
| **Valid Values**      |
| CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where |
| **CLASS_0**           |
| The unspecified class. The network does not specify any QoS. |
| **CLASS_1**           |
| Performance is comparable to current digital private line performance. |
| **CLASS_2**           |
| Intended for packetized video and audio in teleconferencing and multimedia applications. |
| **CLASS_3**           |
| Intended for interoperation of connection-oriented protocols, such as Frame Relay |
| **CLASS_4**           |
| Intended for interoperation of connectionless protocols, such as IP. |
| **Default Value**     |
| CLASS_0               |
| **Description**       |
| This parameter indicates which class of service is provided to an ATM virtual connection. You cannot specify this parameter for Best Effort connections. |

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Callout Anonymously</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes, no</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>no</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates whether APPN will pass the source address when making the call.</td>
</tr>
</tbody>
</table>
### Parameter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost per connect time</td>
<td>0 to 255</td>
<td>Default value is taken from the associated port parameter.</td>
<td>This parameter expresses the relative cost of maintaining a connection over the associated TG. The units are user-defined and are typically based on the applicable tariffs of the transmission facility being used. The assigned values should reflect the actual expense of maintaining a connection over the TG relative to all other TGs in the network. A value of zero means that connections over the TG may be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.</td>
</tr>
<tr>
<td>Cost per byte</td>
<td>0 to 255</td>
<td>Default value is taken from the associated port parameter.</td>
<td>This parameter expresses the relative cost of transmitting a byte over the associated TG. The units are user-defined and the assigned value should reflect the actual expenses incurred for transmitting over the TG relative to all other TGs in the network. A value of zero means that bytes may be transmitted over the TG at no additional cost. Higher values represent higher costs.</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td>Default value is taken from the associated port parameter.</td>
<td>This parameter indicates the level of security protection associated with the TG. If security attributes other than the architecturally-defined ones are needed, one of the user-defined TG characteristics may be used to specify additional values.</td>
</tr>
</tbody>
</table>

### Description

- **Nonsecure**: all else (for example, satellite-connected, or located in a nonsecure country).
- **Public switched network**: secure in the sense that route is not predetermined.
- **Underground cable**: located in secure country (as determined by the network administrator).
- **Secure conduit**: Not guarded, (for example, pressurized pipe).
- **Guarded conduit**: protected against physical tapping.
- **Encrypted**: link-level encryption is provided.
- **Guarded radiation**: guarded conduit containing the transmission medium; protected against physical and radiation tapping.
### Table 26. Configuration Parameter List - Modify TG Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### Table 26. Configuration Parameter List - Modify TG Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Second user-defined TG characteristic</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 255</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the second of three additional characteristics that users can define to describe the TGs in a network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Third user-defined TG characteristic</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 255</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the third of three additional characteristics that users can define to describe the TGs in a network.</td>
</tr>
</tbody>
</table>

### Table 27. Configuration Parameter List - Modify Dependent LU Server

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>fully-qualified CP name of primary DLUS</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of up to 17 characters in the form of netID.CPname, where:</td>
</tr>
<tr>
<td>- netID is a network ID from 1 to 8 characters</td>
</tr>
<tr>
<td>- CPname is a control point name from 1 to 8 characters</td>
</tr>
<tr>
<td>Each name must conform to the following rules:</td>
</tr>
<tr>
<td>- First character: A to Z</td>
</tr>
<tr>
<td>- Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Note:</strong> An existing fully-qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>The value specified in the default fully-qualified CP name of primary dependent LU server parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the fully-qualified CP name of the dependent LU server (DLUS) that is to be used for incoming requests from the downstream PU associated with this link station.</td>
</tr>
</tbody>
</table>
### Table 27. Configuration Parameter List - Modify Dependent LU Server (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> An existing fully-qualified CP name, using the special characters @, $, and # from the character set, continues to be supported; however, these characters should not be used for new CP names.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

### Table 28. Configuration Parameter List - Modify LLC Characteristics

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### Table 28. Configuration Parameter List - Modify LLC Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Maximum number of outstanding I-format LPDUs (TW)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 127</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the transmit Command Line option which is the maximum number of sequentially numbered I-format LPDUs that the link station may have unacknowledged at any given time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive window size</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 127</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the maximum number of unacknowledged sequentially numbered I-format LPDUs that the LLC link station can receive from the remote link station. RW is advertised in SNA XID frames and IEEE 802.2 XID frames. The XID receiver should set its effective TW to a value less than or equal to the value of the received RW to avoid overruns.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivity timer (Ti)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>A link station uses Ti to detect an inoperative condition in either the remote link station or in the transmission media. If an LPDU is not received in the time interval specified by Ti, an S-format command LPDU with the poll bit set is transmitted to solicit remote link station status. Recovery is then based on the reply timer (T1).</td>
</tr>
</tbody>
</table>
Table 28. Configuration Parameter List - Modify LLC Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Reply timer (T1)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>A link station uses T1 to detect a failure to receive a required acknowledgment or response from the remote link station. When T1 expires, the link station sends an S-format command link layer protocol data unit (LPDU) with the poll bit set to solicit remote link station status or any U-format command LPDUs that have not been responded to. The duration of T1 should take into account any delays introduced by underlying layers.</td>
</tr>
</tbody>
</table>

| **Parameter**         |
| Maximum number of retransmissions (N2) |
| **Valid Values**      |
| 1 to 254              |
| **Default Value**     |
| Default value is taken from the associated port parameter. |
| **Description**       |
| This parameter specifies the maximum number of times an LPDU will be retransmitted following the expiration of the reply timer (T1). |

| **Parameter**         |
| Receive acknowledgment timer (T2) |
| **Valid Values**      |
| 1 to 254, measured in tenths of a second |
| **Default Value**     |
| Default value is taken from the associated port parameter. |
| **Description**       |
| This parameter may be used in conjunction with the N3 counter to reduce acknowledgment traffic. A link station uses T2 to delay the sending of an acknowledgment for a received I-format LPDU. T2 is started when an I-format LPDU is received, and reset when an acknowledgment is sent in an I-format or S-format LPDU. If T2 expires, the link station must send an acknowledgment as soon as possible. The value of T2 must be less than that of T1, to ensure that the remote link station will receive the delayed acknowledgment before its T1 expires. |
### Table 28. Configuration Parameter List - Modify LLC Characteristics (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Acknowledgment needed to increment working window</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 127 acknowledgments</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>When the working window (Ww) is not equal to the Maximum Transmit Window Size (Tw), this parameter is the number of transmitted I-format LPDUs that must be acknowledged before the working window can be incremented (by 1). When congestion is detected, by the lost of I-format LPDUs, Ww is set to 1.</td>
</tr>
</tbody>
</table>

### Table 29. Configuration Parameter List - Modify HPR Defaults

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Inactivity timer override for HPR (HPR Ti)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the HPR override LLC inactivity timer (HPR Ti) that is to be used when HPR is supported by this link station. This parameter overrides the value taken from the default inactivity timer override for the HPR parameter. This parameter supersedes the value of the LLC inactivity timer (Ti) parameter specified on the Modify Logical Link Control (LLC) Characteristics parameter when HPR is supported.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Reply timer override for HPR (HPR T1)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 254 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value is taken from the associated port parameter.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the HPR override LLC reply timer (HPR T1) that is to be used when HPR is supported by this link station. This parameter overrides the value taken from the default reply timer override for HPR parameter specified on HPR Defaults. This parameter supersedes the value of the LLC reply timer (T1) parameter specified on the Modify Logical Link Control (LLC) Characteristics parameter when HPR is supported.</td>
</tr>
</tbody>
</table>
### Parameter Information

**Parameter**  
Maximum number retransmission (HPR N2)

**Valid Values**  
1 to 216 000

**Default Value**  
Default value is taken from the associated port parameter.

**Description**  
This parameter specifies the HPR override LLC maximum number of retransmissions (HPR N2) that is to be used when HPR is supported by this link station. This parameter overrides the value taken from the default maximum number of retransmissions for HPR parameter specified on the HPR LLC Override defaults.

This parameter supersedes the value of the LLC maximum number of retransmissions (N2) parameter specified on the Modify Logical Link Control (LLC) Characteristics parameter when HPR is supported.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Limited Resource Timer</td>
<td>Default value is taken from the associated port parameter.</td>
<td>This parameter specifies the timer value associated with the limited resource.</td>
</tr>
</tbody>
</table>

**Syntax:**

```
add lu-name
```

You will be prompted to enter a station name to associate this LU with.

You will be prompted to enter a value for the following parameter. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].
### Table 30. Configuration Parameter List - LEN End Node LU Name

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of up to 17 characters in the form of <code>netID.LUname</code>, where:</td>
</tr>
<tr>
<td>• <code>netID</code> is a network ID from 1 to 8 characters</td>
</tr>
<tr>
<td>• <code>LUname</code> is a control point name from 1 to 8 characters</td>
</tr>
<tr>
<td>Each name must conform to the following rules:</td>
</tr>
<tr>
<td>• First character: A to Z</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Note:</strong> An existing fully-qualified LU name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new LU names.</td>
</tr>
<tr>
<td>To reduce the number of fully-qualified LU names you need to specify, you can define a generic LU name using the wildcard character (*) to represent a portion of the LU name (<code>LUname</code>). You can also define a wildcard entry by using the wildcard character as the whole LU name.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>You need to specify a fully-qualified LU name, which consists of a network ID and the LU name. The network ID is the name of the network that contains the adjacent LEN end node. The LU name is the name of a logical unit accessible through the adjacent LEN end node.</td>
</tr>
</tbody>
</table>

**Syntax:**

```
add connection-network
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].
### Table 31. Configuration Parameter List - Connection Network - Detail

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

All nodes that are members of a given connection network must use the same VRN Name.

The fully-qualified VRN Name (CP name of VRN) has the form: NetworkID.ConnectionNetworkName where NetworkID is this router network node's network identifier.

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

*Table 31. Configuration Parameter List - Connection Network - Detail (continued)*

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Port name (required)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
</tbody>
</table>
| Name of port on which APPN routing has been enabled.  
*Note:* If the **port type** is IP, no **port name** will be specified since there is only one IP port.  
**Default Value** |
| None                  |
| **Description**       |
| This parameter specifies the name of a port providing connectivity to the shared access transport facility (SATF) for the connection network being defined.  
All ports defined for a given connection network must be the same type and have the same characteristics.  
*Note:* For a **port type** of IP, additional ports added to an IP connection network can be any port that IP has been defined to use.  
At least one additional port besides the IP port must be added for the connection network to be used.  
Since the IP port is a pseudo port that always comes up when the node is initialized, real ports that IP is defined on (TR, ATM, FR, ...) must be added to the CN. When at least one of these real ports is up, the connection network link is assumed active. When all of these real ports is down, the connection network link is assumed to be inactive. |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Limited Resource Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>1 to 216,000 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>180</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies the timer value associated with a limited resource.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>DLCI number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>16 to 1007</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies the DLCI number used by the router to connect to the Frame Relay network. When the router initiates a connection to a link station on the LAN through the connection network, it will use this DLCI number to connect to the Frame Relay network.</td>
</tr>
</tbody>
</table>
Table 31. Configuration Parameter List - Connection Network - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>BAN destination address (BDA)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>X’0000 0000 0000’ to X’7FFF FFFF FFFF’</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>X’0000 0000 0000’</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the BAN destination address configured in the node that is performing the BAN function. If you are using bridging to connect the LAN network to the Frame Relay network, specify X’0000 0000 0000’ as the value of this parameter. In this case, the MAC address reported to the APPN topology for the connection network TG is the BNI MAC address coded on the APPN port associated with this connection network definition.</td>
</tr>
</tbody>
</table>

Table 32. Configuration Parameter List - Connection Network Configuration for ATM

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Port name (required)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Name of port on which APPN routing has been enabled.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of a port providing connectivity to the shared access transport facility (SATF) for the connection network being defined.</td>
</tr>
</tbody>
</table>

All ports defined for a given connection network must be the same type and have the same characteristics.

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>fully-qualified connection network name</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 3 to 17 characters in the form of netID.CName, where:</td>
</tr>
<tr>
<td>- netID is a network ID from 1 to 8 characters</td>
</tr>
<tr>
<td>- CName is a connection network name from 1 to 8 characters</td>
</tr>
<tr>
<td>Each name must conform to the following rules:</td>
</tr>
<tr>
<td>- First character: A to Z</td>
</tr>
<tr>
<td>- Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the fully-qualified CN name to which this TG is defined.</td>
</tr>
</tbody>
</table>
## APPN Configuration Commands

Table 32. Configuration Parameter List - Connection Network Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Connection network TG number</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 239</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the TG number uniquely identifying this connection from the local port to the CN. The CN name and TG number pair must be unique.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Limited Resource</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates if this TG should be brought down when not in use by session traffic.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Limited Resource Timer</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 2 160 000 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>180 seconds</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates the time limit after which this CN TG should be brought down when not in use by session traffic.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>LDLC retry count</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 255</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter is used in conjunction with the LDLC timer period to provide reliable delivery of XIDs. The retry count is initialized when a command or request is first transmitted over the link. If the LDLC timer period expires before a response is received, the command or request is retransmitted, the retry count is decremented, and the LDLC timer period is restarted. If the timer expires with the retry count at 0, the link is assumed to be inoperative.</td>
</tr>
</tbody>
</table>
### Table 32. Configuration Parameter List - Connection Network Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>LDLC Timer Period</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 255 seconds</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>For ATM: 1 second</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the timer period used with the <strong>LDLC retry count</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Broadband Bearer Class</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Class_A, Class_C, or Class_X</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Class_X</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the bearer class requested from the ATM network. The classes are defined:</td>
</tr>
<tr>
<td><strong>Class A</strong></td>
</tr>
<tr>
<td>Constant bit rate (CBR) with end-to-end timing requirements</td>
</tr>
<tr>
<td><strong>Class C</strong></td>
</tr>
<tr>
<td>Variable bit rate (VBR) with no end-to-end timing requirements</td>
</tr>
<tr>
<td><strong>Class X</strong></td>
</tr>
<tr>
<td>Service allowing user-defined traffic type and timing requirements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Shareable Regular Network traffic</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes, if this is a Best Effort CN. No, otherwise.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether traffic on this connection network TG can be routed on an ATM VC set up for a regular TG or another CN TG.</td>
</tr>
</tbody>
</table>
### Table 32. Configuration Parameter List - Connection Network Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Shareable other protocol traffic</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether the ATM VC established for this CN TG may be shared with other higher level protocols in the router.</td>
</tr>
</tbody>
</table>

**Note:** The following parameters are forward traffic parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Peak Cell Rate</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 85% of line speed</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Taken from the port definition</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates an upper bound on the cell transmission rate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Sustained Cell Rate</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 85% of line speed</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Taken from the port definition</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates an upper bound on the average cell transmission rate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Tagging</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network.</td>
</tr>
</tbody>
</table>
### Table 32. Configuration Parameter List - Connection Network Configuration for ATM (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>QoS</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where</td>
</tr>
<tr>
<td><strong>CLASS_0</strong></td>
</tr>
<tr>
<td>The unspecified class. The network does not specify any QoS.</td>
</tr>
<tr>
<td><strong>CLASS_1</strong></td>
</tr>
<tr>
<td>Performance is comparable to current digital private line performance.</td>
</tr>
<tr>
<td><strong>CLASS_2</strong></td>
</tr>
<tr>
<td>Intended for packetized video and audio in teleconferencing and multimedia applications.</td>
</tr>
<tr>
<td><strong>CLASS_3</strong></td>
</tr>
<tr>
<td>Intended for interoperation of connection-oriented protocols, such as Frame Relay.</td>
</tr>
<tr>
<td><strong>CLASS_4</strong></td>
</tr>
<tr>
<td>Intended for interoperation of connectionless protocols, such as IP.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>CLASS_3</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates which class of service is provided to an ATM virtual connection.</td>
</tr>
</tbody>
</table>

### Table 33. Configuration Parameter List - TG Characteristics (Connection Network)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Cost per connect time</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 to 255</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter expresses the relative cost of maintaining a connection over the associated TG. The units are user-defined and are typically based on the applicable tariffs of the transmission facility being used. The assigned values should reflect the actual expense of maintaining a connection over the TG relative to all other TGs in the network. A value of zero means that connections over the TG may be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.</td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

**Table 33. Configuration Parameter List - TG Characteristics (Connection Network) (continued)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
</tbody>
</table>
| **Valid Values**       | - Minimum LAN – less than 480 microseconds  
- Telephone – between .48 and 49.152 milliseconds  
- Packet switched – between 49.152 and 245.76 milliseconds  
- Satellite – greater than 245.76 milliseconds Maximum |
| **Default Value**      | LAN |
| **Description**        | This parameter specifies the approximate range for the length of time that it takes for a signal to propagate from one end of the TG to the other. |
### Parameter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective capacity</td>
<td>2 hexadecimal digits in the range X'00' to X'FF'</td>
<td>X'75'</td>
<td>This parameter specifies the effective maximum bit transmission rate for this connection network TG. Effective capacity specifies the maximum effective rate for both physical links and logical links. The effective capacity is encoded as a single-byte representation. The values X'00' and X'FF' are special cases used to denote minimum and maximum capacities. The range of the encoding is very large; however, only 256 values in the range may be specified.</td>
</tr>
<tr>
<td>First user-defined characteristic</td>
<td>0 to 255</td>
<td>128</td>
<td>This parameter specifies the first of three additional characteristics that users may define to describe the TGs in the network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs.</td>
</tr>
<tr>
<td>Second user-defined characteristic</td>
<td>0 to 255</td>
<td>128</td>
<td>This parameter specifies the second of three additional characteristics that users may define to describe the TGs in the network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs.</td>
</tr>
</tbody>
</table>
### Table 33. Configuration Parameter List - TG Characteristics (Connection Network) (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Third user-defined characteristic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 255</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This parameter specifies the third of three additional characteristics that users may define to describe the TGs in the network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs.</td>
</tr>
</tbody>
</table>

**Syntax:**

```
add mode
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

### Table 34. Configuration Parameter List - APPN COS - Mode Name to COS Name Mapping - Detail

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Mode name (required)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>• First character: A to Z</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9</td>
</tr>
</tbody>
</table>

**Note:** An existing mode name for an existing network, of which this router network node is to become a member, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new mode names.

<table>
<thead>
<tr>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This parameter specifies the Mode name for the Mode name to COS name mapping being defined. See <a href="#">CoS Options</a> on page 32 for additional information about Mode name to COS mapping.</td>
</tr>
</tbody>
</table>
Table 34. Configuration Parameter List - APPN COS - Mode Name to COS Name Mapping - Detail (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>COS name (required)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>The name of a previously defined COS definition, selected from the list of COS names defined for this router network node.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the COS Name to be associated with the Mode name being defined for this mode name to COS name mapping.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-level pacing Command Line option size</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 63</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the session-level pacing Command Line option size. This parameter has different definitions depending upon the type of pacing used:</td>
</tr>
<tr>
<td>• For fixed session-level pacing:</td>
</tr>
<tr>
<td>‒ The session-level pacing Command Line option size parameter specifies the receive pacing Command Line option for this node.</td>
</tr>
<tr>
<td>‒ The value of this parameter is the suggested receive pacing Command Line option for the adjacent node.</td>
</tr>
<tr>
<td>• For adaptive session-level pacing:</td>
</tr>
<tr>
<td>‒ The session-level pacing Command Line option size parameter specifies a tuning parameter to be used as the minimum size for Isolated Pacing Messages sent by the adjacent nodes.</td>
</tr>
</tbody>
</table>

**Syntax:**

```
add     additional-port-to-connection-network
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

**Note:** You can have a maximum of 5 ports per connection network definition.
### APPN Configuration Commands

**Table 35. Configuration Parameter List - APPN Additional port to Connection Network**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Connection network name (fully-qualified) (required for each connection network defined)</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
</tbody>
</table>
| A string of 1 to 8 characters:  
  - First character: A to Z  
  - Second to eighth characters: A to Z, 0 to 9 |
| **Note:** An existing connection network of which this node desires to become a member, named using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new connection network names. |
| **Default Value**     |
| None |
| **Description**       |
| This parameter specifies the name of the connection network being defined on this router network node. Since this name becomes the CP name of the virtual routing node (VRN), the name must be unique among all CP and LU names in the APPN network (same as in the local Control Point Name).  

All nodes that are members of a given connection network must use the same VRN Name.  

The fully-qualified VRN Name (CP name of VRN) has the form:  

`NetworkID.ConnectionNetworkName` where `NetworkID` is this router network node’s network identifier. |

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port name</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A unique unqualified name that is automatically generated by the Command Line.</td>
</tr>
</tbody>
</table>
| The name will consist of:  
  - TR (token-ring)  
  - EN (Ethernet) |
| **Default Value** |
| Unqualified name generated by the Command Line. |
| **Description** |
| This parameter specifies the name representing this port. |

When the connection network that the port is being added to is IP, only ports that IP is defined to have an interface on will be permitted to be added to the IP CN. At least one real port that has IP defined must be added to the IP CN for the CN to become active and to be used. |

**Syntax:**

```
add focal_point
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].
Table 36. Configuration Parameter List - APPN Implicit Focal Point

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

Syntax:

```
add local-pu
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 37. Configuration Parameter List - APPN Local PU

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

| Parameter             | Primary DLUS name |
| Valid Values          | A string of 1 to 8 characters: |
|                       | • First character: A to Z |
|                       | • Second to eighth characters: A to Z, 0 to 9 |
| Default Value         | None |
| Description           | This parameter specifies the name to be used to override the primary DLUS configured for this node. |
### APPN Configuration Commands

**Table 37. Configuration Parameter List - APPN Local PU (continued)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong>&lt;br&gt;Secondary DLUS name</td>
</tr>
<tr>
<td><strong>Valid Values</strong>&lt;br&gt;A string of 1 to 8 characters:&lt;br&gt;• First character: A to Z&lt;br&gt;• Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Default Value</strong>&lt;br&gt;None</td>
</tr>
<tr>
<td><strong>Description</strong>&lt;br&gt;This parameter specifies the name to be used to override the secondary DLUS configured for this node.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong>&lt;br&gt;Autoactivate</td>
</tr>
<tr>
<td><strong>Valid Values</strong>&lt;br&gt;Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong>&lt;br&gt;Yes</td>
</tr>
<tr>
<td><strong>Description</strong>&lt;br&gt;This parameter specifies whether to activate this link at start-up.&lt;br&gt;<strong>Note:</strong> If the local link will be used for a DDDLU PU, you should specify yes to this question.</td>
</tr>
</tbody>
</table>

If the local link is not set to autoactivate, then the first attempt to use the local pu (that is, the first attempt to establish a TN3270 session) will Fail because the link is not yet up. While this attempt will fail, it causes the link to come up, and that link will be available for the next attempt. Since the link comes up when the SSCP-PU session is established, and that is when the link is identified as a DDDLU link. No DDDLU sessions can be established until the link is identified as a DDDLU link.

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong>&lt;br&gt;Enable Host Initiated Dynamic LU Definition</td>
</tr>
<tr>
<td><strong>Valid Values</strong>&lt;br&gt;Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong>&lt;br&gt;No</td>
</tr>
<tr>
<td><strong>Description</strong>&lt;br&gt;This parameter indicates whether or not dependent LUs will be created dynamically (as opposed to having to be configured.) If yes is specified, LUs will be defined for this PU as ACTLU requests (with CV0E) are received. LUs for the TN3270E Server do not have to be configured.</td>
</tr>
</tbody>
</table>
### Table 37. Configuration Parameter List - APPN Local PU (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Pool Name for Host-initiated Dynamic LUs</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>• First character: A to Z, $, #, @, or &lt;</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9, $, #, &gt;, or &lt;</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of a pool to be created to contain LUs that the host activates on this local PU. This parameter is applicable only if <strong>Enable Host Initiated Dynamic LU Definition</strong> is <strong>yes</strong>.</td>
</tr>
<tr>
<td>You do not need to use the <strong>add implicit-pool</strong> command to define this pool; specifying the name and other parameters here is sufficient to cause the pool to be created.</td>
</tr>
<tr>
<td>If you do enter a pool name, you will be prompted to enter values for the following parameters:</td>
</tr>
<tr>
<td>• Pool class (See <strong>Table 42 on page 219</strong>.</td>
</tr>
<tr>
<td>• LU type (see <strong>Table 42 on page 219</strong>.</td>
</tr>
<tr>
<td>You can provide the same pool name for multiple local PUs, if you wish.</td>
</tr>
<tr>
<td>By specifying pool information, you cause host-initiated LUs that are not already configured at the router to be placed into the specified pool. TN3270 clients can then be assigned to them by requesting the pool name, or by mapping client IP addresses or destination ports to that pool.</td>
</tr>
<tr>
<td>If you do not specify pool information, these host-initiated LUs are treated as explicit LUs and can only be assigned to clients that request them by their individual LU names.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Terminate-Self when TN3270 Client Disconnects</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter indicates whether or not a terminate_self request will be sent to the SSCP when the TN3270 client disconnects. If <strong>yes</strong> is specified, terminate_self will be sent and the host will be responsible for terminating the LU-LU session (i.e., the SLU will NOT send an UNBIND request.)</td>
</tr>
</tbody>
</table>

**Syntax:**

```
add routing_list
```

**Note:** These questions are asked only if you have configured the node as a border node.
Routing lists are not supported for 2210 12x models.

There are a number of editing shortcut keys available to speed the modification of existing data in a previously configured routing list. These shortcut keys may be used when you are prompted for the Destination LUs and the Routing CPs.

- Pressing **Enter** alone will retain the currently displayed name.
- Pressing the **Space bar** followed by **Enter** will delete the currently displayed name.
- Entering character data followed by pressing **Enter** will replace the currently displayed name with the new character data.
- Entering 9 followed by pressing **Enter** will jump to the end of the list where new names can be appended.
- At the end of a list, pressing **Enter** alone completes the list.

Table 38. Configuration Parameter List - Routing List Configuration

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Routing list name</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>Character string up to 20 characters in length with no imbedded blanks. Mixed case and special characters are allowed.</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Blank</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter identifies a specific routing list for modification, listing, or deletion by the configuration code. It is not used by the operational code. Up to 255 routing lists may be configured depending upon availability of configuration memory. Case is respected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet visit count</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>1 to 255</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Default taken from corresponding node level parameter</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter specifies how many networks a locate search procedure may traverse.</td>
</tr>
</tbody>
</table>
Table 38. Configuration Parameter List - Routing List Configuration (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Dynamic routing list updates</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 (none)</td>
</tr>
<tr>
<td>1 (full)</td>
</tr>
<tr>
<td>2 (limited)</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Default value taken from corresponding node level parameter</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter controls whether entries can be automatically added to the node’s temporary subnet routing list. It can be set to the same values as the analogous node level parameter. If this function is enabled the automatically added entries are only added to the temporary copy of the routing list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Enable routing list optimization</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Indicates whether the node is allowed to reorder the subnetwork routing list so that entries most likely to succeed come first. This reordering occurs in the internal temporary copy of the routing list.</td>
</tr>
</tbody>
</table>
### APPN Configuration Commands

Table 38. Configuration Parameter List - Routing List Configuration (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Destination LU found via this list</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A fully-qualified LU name with optional trailing wildcard. Legal characters for the LU name are: A-Z, @, $, #, 0-9.</td>
</tr>
<tr>
<td>The first character of the NETID part and of the LU name part must be non-numeric.</td>
</tr>
<tr>
<td>Any of the FQ LU names may be terminated with a wild card &quot;*&quot; character to designate the range of LUs. For example,</td>
</tr>
<tr>
<td>- *</td>
</tr>
<tr>
<td>- NETI*</td>
</tr>
<tr>
<td>- NETI.LUA*</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies a list of destination LUs that can be found via this routing list.</td>
</tr>
<tr>
<td>This question will be repeated until terminated with a null entry.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td>1. Only a single entry among all of the routing lists may have a standalone &quot;*&quot;. This will match all LUs, and the routing list containing it is known as the default routing list.</td>
</tr>
<tr>
<td>2. All the editing shortcuts described at the beginning of this table are available to speed modification of a previously configured routing CP(s) list.</td>
</tr>
<tr>
<td>3. Any given LU name may not be duplicated in another routing list.</td>
</tr>
<tr>
<td>4. Maximum number of LU names that may be specified:</td>
</tr>
<tr>
<td>- 2210 12x - not supported</td>
</tr>
<tr>
<td>- 2210 14x or 24x - 98</td>
</tr>
</tbody>
</table>
**Table 38. Configuration Parameter List - Routing List Configuration (continued)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Syntax:**

```
add cos_mapping_table
```

**Note:** These questions are asked only if you have configured the node as a border node.

COS mapping tables are not supported for 2210 12x models.

The editing shortcut keys specified at the beginning of the routing list table are also valid here. Use them to speed modification of the non-native CP names and COS name pairs.
# APPN Configuration Commands

Table 39. Configuration Parameter List - COS Mapping Table Configuration

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>COS mapping table name</th>
</tr>
</thead>
</table>

**Valid Values**

Character string up to 20 characters in length, with no imbedded blanks. Mixed case and special characters are allowed.

**Default Value**

Blank

**Description**

This parameter identifies a specific COS mapping table. It allows you to identify the table for modification, listing, or deletion by the configuration software. It is not used by the operational software. Up to 255 COS mapping tables may be configured depending upon availability of configuration memory. Case is respected.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Non-native NETID or CP name</th>
</tr>
</thead>
</table>

**Valid Values**

A fully-qualified CP name with optional trailing wildcard. Legal characters for the CP name are: A-Z, @, $, #, 0-9

The first character of the NETID part and of the CP name part must be non-numeric. Any of the fully-qualified CP names may be terminated with a wildcard "*" character to designate a range of CPs. For example:

- *
- NET1*
- NET1.LUA*

**Default Value**

Blank

**Description**

This parameter specifies a list of one or more non-native networks that this mapping table applies to. This question is repeated until terminated with a null entry.

**Notes:**

1. Only a single entry among all the routing lists may have a standalone "*" . This will match all non-native networks, and is known as the default routing list.
2. Any given CP name may not be duplicated in another COS mapping table.
3. Maximum number of CP names that may be specified:
   - 2210 12x - not supported
   - 2210 14x or 24x - 98
Table 39. Configuration Parameter List - COS Mapping Table Configuration (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Delete

Use the **delete** command to delete:

**Syntax:**
APPN Configuration Commands

- delete
  - port port-name
  - link link-station-name
  - lu-name lu-name
  - connection-network connection-network-name
  - additional-port-to-connection-network cn-port-name
  - mode name
  - focal_point focal-point-name
  - local-pu
  - routing_list routing list name
  - cos_mapping_table mapping table name

List

Use the list command to list:

Syntax:

- list
  - all
  - node
  - traces
  - management
  - hpr
  - dlur
  - port (port name)
  - link station (link station name)
  - lu name lu name
  - mode name mode name
  - connection network connection network name
  - focal_point
  - routing_list routing list name
  - cos_mapping_table mapping table name

Activate_new_config

Use the activate_new_config command to read the configuration into non-volatile memory.

Syntax:

- activate_new_config
Table 40. TN3270E Configuration Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>See page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxvii.</td>
<td></td>
</tr>
<tr>
<td>Set</td>
<td>tn3270e</td>
<td>218</td>
</tr>
<tr>
<td>Add</td>
<td>Adds or updates the following: implicit-pool, lu, mapping, port</td>
<td>219, 220, 226, 227</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the following: implicit-pool, lu, mapping, port</td>
<td>228</td>
</tr>
<tr>
<td>List all</td>
<td>Lists the configuration memory</td>
<td>230</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxvii.</td>
<td></td>
</tr>
</tbody>
</table>

Syntax:

```
set
```

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 41. Configuration Parameter List - Set TN3270E

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Enable TN3270E Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default Value</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter specifies whether TN3270E Server support will be enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>TN3270E Server IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid values</td>
<td>Any IP address is accepted as valid input. However, the address must also be configured in IP either as an interface address or as the router’s internal IP address.</td>
</tr>
<tr>
<td>Default Value</td>
<td>None</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter is the IP address associated with the TN3270E Server.</td>
</tr>
</tbody>
</table>
## APPN Configuration Commands

Table 41. Configuration Parameter List - Set TN3270E (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Port number</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 65535</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>23</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the port number associated with the TN3270E Server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Enable Client IP address to LU name mapping?</td>
</tr>
<tr>
<td><strong>Valid values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether client IP address to LU name mapping occurs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Default pool name</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Any alphanumeric string of 1 to 8 characters</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>PUBLIC</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of the default pool. This pool is used when TN3270 clients connect and do not specify an LU/pool name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>NetDisp Advisor Port Number</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 65535</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>10 008</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter sets the port number for the Network Dispatcher Advisor.</td>
</tr>
</tbody>
</table>
### Table 41. Configuration Parameter List - Set TN3270E (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Keepalive type</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Valid Values</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Default Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This parameter specifies the Keepalive type.</td>
</tr>
</tbody>
</table>

A Keepalive type of *Timing mark* requires responses from the client within the amount of time specified using the *Timer* parameter.

A Keepalive type of *NOP* specifies that the client will not send back a response to the Keepalive message. Notification that the client is no longer there will come from TCP.

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Valid Values</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 65 535 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Default Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This parameter specifies how often the Keepalive message is sent to the client.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Valid Values</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 65535 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Default Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This parameter sets the timer value to be used with the Keepalive function.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic logoff</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Valid Values</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes or No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Default Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This parameter specifies whether automatic logoff will be enabled.</td>
</tr>
</tbody>
</table>
### Table 41. Configuration Parameter List - Set TN3270E (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Time</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 65 535 minutes</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>30</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter sets the time that the TN3270E link can be idle before being automatically logged off.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Precedence</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter sets the IPv4 precedence value, which allows priority queueing of IPv4 encapsulated packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LU Capping?</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter allows you to determine how many TN3270 sessions each IP address is allowed to initiate. If the answer to this question is yes, you will be asked the following question.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of LUs per IP address</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>0 - 65 535</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter sets the maximum number of TN3270 sessions each client IP address is allowed to initiate.</td>
</tr>
</tbody>
</table>

**Syntax:**

`add implicit-pool`

This command defines a pool of LUs as opposed to the `add lu` command which adds a single LU. You will be prompted to enter
values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 42. Configuration Parameter List - Add TN3270E Implicit

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

| Parameter             | Pool class                                     |
| Valid Values          | 1 or 2, where:                                 |
|                       | • Implicit workstation                         |
|                       | • Implicit printer                             |
| Default Value         | 1                                              |
| Description           | This parameter specifies type of LU pool.      |

| Parameter             | Station name                                    |
| Valid Values          | A string of 1 to 8 characters:                  |
|                       | • First character: A to Z                       |
|                       | • Second to eighth characters: A to Z, 0 to 9   |
| Default Value         | None                                           |
| Description           | This parameter specifies the name representing the link between the DLUR and the PU or the subarea link over which SNA data will flow. |
### APPN Configuration Commands

Table 42. Configuration Parameter List - Add TN3270E Implicit (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>

**Description**

This parameter specifies the mask to be used to ensure that the LU names will not duplicate other names in the network.

LU names are generated by appending the NAU address to the end of the LU name mask. When not specifying an address range, NAU addresses from 2 - 253 will be checked to see if the address is unused. If the address is available, it will be used. Otherwise, the next NAU address will be tried.

For example, if the LU name mask is FRED, the possible LU names are [FRED2, FRED3, ..., FRED253].

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>

**Description**

This parameter specifies the type of dependent LU for the LU being added.

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
</tbody>
</table>

**Description**

This parameter specifies whether you want to define an LU address range.
Table 42. Configuration Parameter List - Add TN3270E Implicit (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>LU address range</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>Any range of values within 1 - 255</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>none</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter specifies LU address range.</td>
</tr>
</tbody>
</table>

The LU address range can be specified by using the following format:

\[
\text{lower_address_bound-upper_address_bound}
\]

If no hyphen follows the first value, that value is assumed to be a single LU address. Multiple ranges can be entered, separated by commas. For example, the following string specifies 2 address ranges and 2 specific LU addresses:

\[
2-40,56,58,100-250
\]

| Parameter |
| Number of implicit workstation definitions |
| Valid Values |
| 1 to 255 |
| Default Value |
| 1 |
| Description |
| This parameter specifies the number of dependent LUs to be added to the implicit pool. |

```
add lu
```

This command adds a specific LU. You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].
### Parameter Information

**Parameter**
- LU name

**Valid Values**
- A string of 1 to 8 characters:
  - First character: A to Z, @, $, and #
  - Second to eighth characters: A to Z, 0 to 9

**Default Value**
- None

**Description**
- This parameter specifies the LU name of the dependent LU being defined.

**Parameter**
- NAU address

**Valid Values**
- 1 to 255

**Default Value**
- None

**Description**
- This parameter specifies the NAU address of the LU being defined.

**Parameter**
- Station name

**Valid Values**
- A string of 1 to 8 characters:
  - First character: A to Z
  - Second to eighth characters: A to Z, 0 to 9

**Default Value**
- None

**Description**
- This parameter specifies the name representing either the link between the DLUR and the PU defined using the `add local-pu` command or the subarea link over which SNA data will flow.

**Parameter**
- Class

**Valid Values**
- 1. Explicit Workstation
- 2. Implicit Workstation
- 3. Explicit Printer
- 4. Implicit Printer

**Default Value**
- 1

**Description**
- This parameter specifies the LU class.
## APPN Configuration Commands

### Table 43. Configuration Parameter List - Add TN3270E LU (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>LU type</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 — 3270 Mod 2 display</td>
</tr>
<tr>
<td>2 — 3270 Mod 3 display</td>
</tr>
<tr>
<td>3 — 3270 Mod 4 display</td>
</tr>
<tr>
<td>4 — 3270 Mod 5 display</td>
</tr>
<tr>
<td>5 — 3270 printer</td>
</tr>
<tr>
<td>6 — SCS printer</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the type of dependent LU for the LU being added.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Implicit pool name</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>First character: A to Z, &lt;</td>
</tr>
<tr>
<td>Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>&lt;DEFLT&gt;</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of the implicit pool to be used in the LU definition. This question is asked only if the class is an implicit workstation or implicit printer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Define an associated printer</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether you want to define an associated printer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Associated printer name</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>First character: A to Z, @, $, and #</td>
</tr>
<tr>
<td>Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of the associated printer.</td>
</tr>
</tbody>
</table>
### Parameter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Associated printer NAU address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Values</td>
<td>1 to 255</td>
</tr>
<tr>
<td>Default Value</td>
<td>None</td>
</tr>
<tr>
<td>Description</td>
<td>This parameter specifies the NAU address for the associated printer LU definition.</td>
</tr>
</tbody>
</table>

**Syntax:**

```
add map
```

This command adds a client IP address to LU name mapping. You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

The following mapping rules apply:

- If a map definition contains a full subnet mask (255.255.255.255), indicating that the entry is for a specific client and a specific LU/pool is not requested by the client, any LU/pool in the map definition that matches the connection type may be tried.
- If a map definition does not contain a full subnet mask and a specific LU/pool is not requested, only pool entries in the map definition will be tried. You cannot create a definition that maps a subnet to a specific LU. You must map the subnet to a pool.
- If a connection request is received from a client and there are no map entries that match, the request will be rejected.
- A mixture of pool and LU types can be added to a particular map. The resource selected will be based on the type of connection request. The order in which the resources are defined in the map will be the order in which it is chosen for a particular connection request.
- If a map definition contains a non-zero destination port number, only clients that connect to that port will be checked against that mapping.

**Note:** When a client connects while mapping is enabled, the server will begin ANDing the client’s IP address with the subnet mask of each sequential map. The longest match between the incoming client IP address and the map definition determines which map definition is tried first. If all eligible resources in the map definition are in use and final LU mapping connection attempt is no, the map definitions are again searched for the next most specific match.
### Table 44. Configuration Parameter List - Add TN3270E Map

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP address or Network address</td>
</tr>
</tbody>
</table>

| **Valid Values** | Any valid IP address |
| **Default Value** | 0.0.0.0 |
| **Description** | This parameter specifies the IP address of the client or network map definition to be added. |

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Mask</td>
</tr>
</tbody>
</table>

| **Valid Values** | Any valid IP address mask |
| **Default Value** | 0.0.0.0 |
| **Description** | This parameter specifies the IP address mask the router applies to incoming client IP addresses and configured client IP or network addresses to determine whether they match. |
### APPN Configuration Commands

**Table 44. Configuration Parameter List - Add TN3270E Map (continued)**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Port number</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 65535</td>
</tr>
<tr>
<td>If you want to specify a particular port, you should select either the global TN3270 server port value defined with the set command, or one of the port values defined with the add port command.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the destination TCP port number a TN3270 client must connect to in order for this mapping entry to be checked. If the value is zero, the mapping entry applies to client connections to any defined TCP port number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Final LU mapping connection attempt</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether the router should continue to try less specific mapping entries if a client match with this entry failed to yield a valid available LU.</td>
</tr>
</tbody>
</table>

**Syntax:**

```
add port
```

This command specifies additional port for the TN3270E Server to listen on. You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

**Table 45. Configuration Parameter List - Add TN3270E Port**

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Port number</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 65535</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>none</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the port number to be added.</td>
</tr>
</tbody>
</table>
### Table 45. Configuration Parameter List - Add TN3270E Port (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Pool name</th>
</tr>
</thead>
</table>
| **Valid Values** | A string of 1 to 8 characters:  
  • First character: A to Z  
  • Second to eighth characters: A to Z, 0 to 9 |
| **Default Value** | None |
| **Description** | This parameter specifies the name of the pool associated with this port. Clients that connect to this port and do not specify an LU name or pool name will be assigned an LU from this pool. |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Disable Client Filtering for this port?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Values</strong></td>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This parameter specifies whether incoming connections on this port should use the box-wide Client IP Address to LU Name Mapping function if it is enabled.</td>
</tr>
</tbody>
</table>

**Syntax:**
```
delete lu
```

This command removes a TN3270E LU. You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].
APPN Configuration Commands

Table 46. Configuration Parameter List - Delete TN3270E LU

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>LU name</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>• First character: A to Z, @, $, and #</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter specifies the LU name of the dependent LU to be removed.</td>
</tr>
</tbody>
</table>

Syntax:
```
delete implicit-pool
```

This command removes a TN3270E implicit pool. You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 47. Configuration Parameter List - Delete TN3270E Implicit

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Pool name</td>
</tr>
<tr>
<td>Valid Values</td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>• First character: A to Z</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td>Default Value</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>This parameter specifies the name of the LU pool to be deleted.</td>
</tr>
</tbody>
</table>

| Parameter             |
| Delete entire pool    |
| Valid Values          |
| Yes or No             |
| Default Value         |
| No                    |
| Description           |
| This parameter specifies whether the entire pool or a specific entry is to be deleted. |
Table 47. Configuration Parameter List - Delete TN3270E Implicit (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Station name</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>A string of 1 to 8 characters:</td>
</tr>
<tr>
<td>• First character: A to Z</td>
</tr>
<tr>
<td>• Second to eighth characters: A to Z, 0 to 9</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the name of the station to be deleted.</td>
</tr>
</tbody>
</table>

**Syntax:**

deleatemap

This command removes a client IP address to LU name mapping. You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 48. Configuration Parameter List - Delete TN3270E Map

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Client IP address or Network address</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Any valid IP address</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>0.0.0.0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the IP address of the client or network map definition to be deleted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Client IP address or Network address Mask</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Any valid IP address mask</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>0.0.0.0</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the IP address mask of the client or network map definition to be deleted.</td>
</tr>
</tbody>
</table>
### Table 48. Configuration Parameter List - Delete TN3270E Map (continued)

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Delete all entries for this client?</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>Yes or No</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies whether the entire pool or a specific name is to be deleted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Pool name</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
</tbody>
</table>
| A string of 1 to 8 characters:  
  • First character: A to Z  
  • Second to eighth characters: A to Z, 0 to 9 |
| **Default Value**     |
| None                  |
| **Description**       |
| This parameter specifies the LU name or pool name to be deleted. |

Syntax:
```
delete port
```

This command deletes port definitions. You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

### Table 49. Configuration Parameter List - Delete TN3270E Port

<table>
<thead>
<tr>
<th>Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Port number</td>
</tr>
<tr>
<td><strong>Valid Values</strong></td>
</tr>
<tr>
<td>1 to 65536</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
</tr>
<tr>
<td>none</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>This parameter specifies the port number to be added.</td>
</tr>
</tbody>
</table>

Syntax:
```
list all
```

This command lists a TN3270E configuration.
Monitoring APPN

This section describes how to monitor APPN. It includes the following sections:

- [Accessing the APPN Monitoring Commands]
- [APPN Monitoring Commands]

Accessing the APPN Monitoring Commands

Use the following procedure to access the APPN monitoring commands. This process gives you access to an APPN’s monitoring process.

At the OPCON prompt, enter `talk 5`.

After you enter the `talk 5` command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press `Return` again.

Enter `protocol APPN` For example:

```
* talk 5
+
+ protocol APPN
APPN>
```

If typing `p appn` results in the message “Protocol APPN is available but not configured”, you probably have one of the following errors:

- You have not enabled APPN globally in the active configuration (although you may have configured APPN parameters). Check the current configuration and if this is the case, enable APPN and restart or reload the router.
- The amount of memory required for APPN to initialize properly was not available in the router. Use `talk 2` to see if an error message to this effect has been logged. If so, reconfigure APPN to use less memory and restart or reload the router.

Once you have reached the APPN monitoring prompt, enter `tn3270` to reach the TN3270E > monitoring prompt.

APPN Monitoring Commands

This section describes the APPN monitoring commands for monitoring APPN interfaces. Enter the commands at the APPN> prompt, and TN3270 server commands at the TN3270E> prompt.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>See details on page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists keyword options for specific commands.</td>
<td>--</td>
</tr>
<tr>
<td>activate link</td>
<td>Activates a configured link.</td>
<td>&quot;Activate&quot; on page 234</td>
</tr>
<tr>
<td>aping</td>
<td>Tests SNA/APPN connectivity to a target LU.</td>
<td>&quot;Aping&quot; on page 234</td>
</tr>
<tr>
<td>deactivate link</td>
<td>Deactivates a configured or dynamic link.</td>
<td>&quot;Deactivate link&quot; on page 235</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>list cp-cp_sessions</td>
<td>Displays a list of all adjacent CPs that may have CP-CP sessions with this router.</td>
<td>238</td>
</tr>
<tr>
<td>list dlur dlus</td>
<td>Displays a list of active DLUS's and the status of each session in the DLUS-DRU pipe.</td>
<td>238</td>
</tr>
<tr>
<td>list dlur lu</td>
<td>Displays a list of downstream or internal PUs with LU statistics for each PU.</td>
<td>238</td>
</tr>
<tr>
<td>list dlur pu</td>
<td>Displays a list of downstream or internal PUs with their connection status.</td>
<td>247</td>
</tr>
<tr>
<td>list dlur status</td>
<td>Displays a summary of currently active global DLUR configuration information.</td>
<td>241</td>
</tr>
<tr>
<td>list ds incomplete_locates</td>
<td>Displays a list of APPN searches that are currently in progress.</td>
<td>241</td>
</tr>
<tr>
<td>list ds resource</td>
<td>Displays a complete or partial list of LU names in this router's APPN directory.</td>
<td>242</td>
</tr>
<tr>
<td>list ds status</td>
<td>Displays summary statistics for APPN Directory Services.</td>
<td>242</td>
</tr>
<tr>
<td>list focal</td>
<td>Displays a list of network management focal points with their status.</td>
<td>243</td>
</tr>
<tr>
<td>list isr_sessions</td>
<td>Displays the number of active ISR LU-LU sessions that pass through this router, by link.</td>
<td>244</td>
</tr>
<tr>
<td>list link</td>
<td>Displays a list of configured and dynamic links from this router.</td>
<td>247</td>
</tr>
<tr>
<td>list link link-name</td>
<td>Displays detailed configuration and status about one particular link.</td>
<td>247</td>
</tr>
<tr>
<td>list local_link</td>
<td>Displays a list of logical links from DLUR to local PU2.0s in this router (which are used to contain TN3270 LUs).</td>
<td>247</td>
</tr>
<tr>
<td>list log</td>
<td>Now replaced by &quot;log view&quot; and &quot;log status&quot;.</td>
<td>253</td>
</tr>
<tr>
<td>list port</td>
<td>Displays a list of configured physical and logical APPN router ports with their status.</td>
<td>248</td>
</tr>
<tr>
<td>list port port-name</td>
<td>Displays detailed configuration and status about one particular port.</td>
<td>248</td>
</tr>
<tr>
<td>list rtp</td>
<td>Displays a list of nodes in the RTP Partner Table, and summary information about all active RTP connections.</td>
<td>251</td>
</tr>
<tr>
<td>list rtp tcid</td>
<td>Displays detailed information about one or all RTP connection(s).</td>
<td>253</td>
</tr>
<tr>
<td>list session</td>
<td>Displays a list of ISR sessions that flow through the router.</td>
<td>253</td>
</tr>
</tbody>
</table>
### Table 50. APPN Monitoring Command Summary (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>See details on page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>list status</td>
<td>Displays a summary of general APPN configuration and status information.</td>
<td>page 254</td>
</tr>
<tr>
<td>list topo node</td>
<td>Displays information in this router’s topology database about a particular node in this topology subnet.</td>
<td>page 253</td>
</tr>
<tr>
<td>list topo status</td>
<td>Displays a summary of topology database statistics.</td>
<td>page 256</td>
</tr>
<tr>
<td>list topo tg</td>
<td>Displays a complete or partial list of active TGs in this topology subnet.</td>
<td>page 257</td>
</tr>
<tr>
<td>log status</td>
<td>Displays summary information about the APPN event log.</td>
<td>page 258</td>
</tr>
<tr>
<td>log view</td>
<td>Enters a submenu for navigating and viewing APPN event log entries.</td>
<td>page 261</td>
</tr>
<tr>
<td>memory</td>
<td>Displays summary and detailed information about APPN memory usage within the router.</td>
<td>page 261</td>
</tr>
<tr>
<td>restart</td>
<td>Stops and reactivates APPN and TN3270 disruptively.</td>
<td>&quot;Restart&quot; on page 264</td>
</tr>
<tr>
<td>rtp status</td>
<td>Displays currently in-use global RTP configuration information.</td>
<td>&quot;Rtp status&quot; on page 263</td>
</tr>
<tr>
<td>rtp switchpath</td>
<td>Causes an RTP connection to path switch to the best currently available path.</td>
<td>&quot;Rtp switchpath&quot; on page 263</td>
</tr>
<tr>
<td>rtp test</td>
<td>Does an HPR route test and displays the results.</td>
<td>&quot;Rtp test&quot; on page 263</td>
</tr>
<tr>
<td>stop</td>
<td>Stops APPN and TN3270 disruptively.</td>
<td>&quot;Stop&quot; on page 265</td>
</tr>
<tr>
<td>test rtp</td>
<td>Does an HPR route test and display the results (old form of &quot;rtp test&quot;).</td>
<td>&quot;Rtp test&quot; on page 263</td>
</tr>
<tr>
<td>tn3270e</td>
<td>Accesses the TN3270 monitoring command menu.</td>
<td>&quot;TN3270E Monitoring Commands&quot; on page 265</td>
</tr>
<tr>
<td>exit</td>
<td>Returns you to the main Talk 5 monitoring menu.</td>
<td>--</td>
</tr>
</tbody>
</table>

### Table 51. TN3270E Server Monitoring Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>See details on page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists keyword options for specific commands.</td>
<td>--</td>
</tr>
<tr>
<td>deactivate lu</td>
<td>Deactivates by force an LU in use by a TN3270 client, and disconnects the corresponding TCP connection to that client.</td>
<td>&quot;Deactivate LU&quot; on page 265</td>
</tr>
<tr>
<td>list connections</td>
<td>Displays a complete or partial list of active client connections.</td>
<td>267</td>
</tr>
<tr>
<td>list lu lu-name</td>
<td>Displays detailed configuration and status information about a single internal LU.</td>
<td>268</td>
</tr>
<tr>
<td>list mapping</td>
<td>Displays a list of configured client IP address to LU/pool name mappings.</td>
<td>269</td>
</tr>
</tbody>
</table>
Table 51. TN3270E Server Monitoring Command Summary (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>list pools</td>
<td>Displays a list of configured implicit LU pools.</td>
<td>269</td>
</tr>
<tr>
<td>list pools pool-name</td>
<td>Displays detailed information about a single LU pool.</td>
<td>270</td>
</tr>
<tr>
<td>list ports</td>
<td>Displays a list of configured TN3270 server target TCP ports.</td>
<td>271</td>
</tr>
<tr>
<td>list pu</td>
<td>Displays a list of all internal PUs (both DLUR and subarea) with summary status and configuration information.</td>
<td>272</td>
</tr>
<tr>
<td>list pu pu-name</td>
<td>Displays a list of all internal LUs under the specified PU, with summary status and configuration information for each LU.</td>
<td>273</td>
</tr>
<tr>
<td>list rejections</td>
<td>Displays a list of the most recent client connections rejected.</td>
<td>273</td>
</tr>
<tr>
<td>list status</td>
<td>Displays global TN3270 server configuration and statistical summary.</td>
<td>275</td>
</tr>
<tr>
<td>exit</td>
<td>Returns you to the APPN monitoring menu.</td>
<td>--</td>
</tr>
</tbody>
</table>

APPN Monitoring Command Details

This section describes the detailed syntax of the APPN monitoring commands. You enter these commands at the APPN> command prompt.

Activate

Use the activate link command to activate a configured link. Use the list link command to look up the name of the link you wish to activate and to view the status of the link after activating it.

**Syntax:**

activate link link_name

Aping

Use the aping command to send a message to another address and watch for a response.

**Note:** When APING responds faster than 1 millisecond, the data rate displayed appears as “-----”.

**Syntax:**

aping flag-value-pairs lu_name

where,

**flag-value-pairs**

Specifies one or more of the following flags followed by a value. Specify these flag values only if you want to override the default values.

<table>
<thead>
<tr>
<th>Flag</th>
<th>Meaning</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m</td>
<td>Mode name for LU6.2 session</td>
<td>#INTER</td>
</tr>
</tbody>
</table>

Table 52. Flags
Table 52. Flags (continued)

<table>
<thead>
<tr>
<th>-t</th>
<th>Destination TP (transaction program) name</th>
<th>APING</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>Count of sends and receives to issue 1</td>
<td></td>
</tr>
<tr>
<td>-x</td>
<td>Count of LU6.2 conversations to run (serially)</td>
<td>1</td>
</tr>
<tr>
<td>-y</td>
<td>Count of TPs to run (serially)</td>
<td>1</td>
</tr>
<tr>
<td>-s</td>
<td>Size of packet</td>
<td>100 bytes</td>
</tr>
<tr>
<td>-q</td>
<td>Quiet</td>
<td>Status messages</td>
</tr>
<tr>
<td>-b</td>
<td>Output display goes to talk 2 (in background)</td>
<td>Display to Talk 5</td>
</tr>
</tbody>
</table>

**lu_name**

Specifies the fully-qualified LU name of the target of the APING.

**Valid Values:** Any valid fully-qualified LU name

**Example:**

```
APPN >apn stfnet.mvs8
Allocate duration: 536 msec
Iteration Duration Data Sent Data Rate
number (msec) (bytes) (Kb/s) LU name
------------------------------------------------------
0 458 100 1 STFNET.MVS8
------------------------------------------------------
```

**Table 53. APING Output Description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocate duration</td>
<td>Time required to set up the LU6.2 session and conversation for the aping.</td>
<td>--</td>
</tr>
<tr>
<td>Iteration duration</td>
<td>Round-trip time required to send and receive acknowledgement for the data packet.</td>
<td>--</td>
</tr>
<tr>
<td>Iteration data rate</td>
<td>Calculated data rate (min 1Kb/s) based on duration and bytes sent.</td>
<td>--</td>
</tr>
</tbody>
</table>

**Deactivate link**

Use the **deactivate link** command to deactivate a configured link. Use the **list link** command to see link names and to view the status of the link after using this command. Configured links should have an inactive status and dynamic links should disappear.

**Syntax:**

```
deactivate link link_name
```

**Dump**

Use the **Dump** command to create an APPN dump. You can use **Boot config>** on **talk 6** to determine where the dump will be saved. The dump name will be the same as the dump of the whole router with '_A.1' concatenated to the end. You can initiate multiple dumps. The concatenation will be incremented for each dump. When the dump name has reached '_A.5', it will be reset to '_A.1'.

**Syntax:**

```
dump
```
APPN Monitoring Commands

Since this dump is non-disruptive to APPN functions, you can improve its integrity by minimizing traffic and APPN control commands while the dump is in progress.

List
Use the List command to display information about the APPN configuration. The command lists:

Syntax:

list
  - appc_sessions
  - cp-cp_sessions
  - dlur dlus
  - dlur lu
  - dlur pu
  - dlur status
  - ds incomplete_locates
  - ds resource
  - ds status
  - dumps
  - focal
  - isr_sessions
  - link
  - link link-name
  - local_link
  - log
  - port
  - port port-name
  - rtp
  - rtp tcid
  - session
  - status
  - topo node
  - topo status
  - topo tg

Command Function

_list appc_sessions
Use the list appc command to display a list of all LU6.2 sessions that have an endpoint in this router. Examples of such sessions include: CP-CP sessions, sessions from DLUR to a DLUS, sessions to a network management focal point, and sessions started due to an “aping” command. This command lists all active sessions. If a pipe consists of two one-way sessions, both sessions in the pair are displayed.
### Example:

```plaintext
APPN >li appc
```

<table>
<thead>
<tr>
<th>LU Name</th>
<th>Mode</th>
<th>Type</th>
<th>FSM</th>
<th>FID</th>
<th>PCID</th>
</tr>
</thead>
<tbody>
<tr>
<td>STFNET.CP3174BC</td>
<td>CPSVCMG</td>
<td>Pri</td>
<td>ACT</td>
<td>FID2</td>
<td>C4 9B 1F 3B 03 54 83 3D</td>
</tr>
<tr>
<td>STFNET.CP3174BC</td>
<td>CPSVCMG</td>
<td>Sec</td>
<td>ACT</td>
<td>FID2</td>
<td>CB 13 AF 23 AC E5 06</td>
</tr>
<tr>
<td>STFNET.VL14</td>
<td>CPSVCMG</td>
<td>Pri</td>
<td>ACT</td>
<td>FID5</td>
<td>C4 9B 1F 3B 03 54 83 40</td>
</tr>
<tr>
<td>STFNET.VL14</td>
<td>CPSVCMG</td>
<td>Sec</td>
<td>ACT</td>
<td>FID5</td>
<td>CB 67 9F CA F8 27 B5 9F</td>
</tr>
<tr>
<td>STFNET.VLNN045</td>
<td>CPSVCMG</td>
<td>Pri</td>
<td>ACT</td>
<td>FID5</td>
<td>C8 8B 1F 3B 04 42 34 FA</td>
</tr>
<tr>
<td>STFNET.VLNN045</td>
<td>CPSVCMG</td>
<td>Sec</td>
<td>ACT</td>
<td>FID5</td>
<td>C4 9B 1F 3B 03 54 83 41</td>
</tr>
<tr>
<td>STFNET.MVS8</td>
<td>CPSVRMGR</td>
<td>Pri</td>
<td>ACT</td>
<td>FID2</td>
<td>C4 9B 1F 3B 03 54 83 42</td>
</tr>
<tr>
<td>STFNET.MVS8</td>
<td>CPSVRMGR</td>
<td>Sec</td>
<td>ACT</td>
<td>FID2</td>
<td>D3 B7 7C D5 57 35 0B C8</td>
</tr>
</tbody>
</table>

Table 54. List appc_sessions Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU name</td>
<td>Fully qualified partner LU name</td>
<td><code>--</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Mode name for the session</td>
<td>• #CONNECT = standard medium priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• #INTER = standard high priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPSVCMG = CP-CP session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPSVRMGR = DLUR-DLUS session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SNASVCMG = Focal point session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• other mode names are architected and can also be user-defined</td>
</tr>
<tr>
<td>Type</td>
<td>Router session activation role</td>
<td>• Pri = Primary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sec = Secondary</td>
</tr>
<tr>
<td>FSM</td>
<td>Current session status (Finite State Machine value)</td>
<td>• ACT = active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PBIR = pending BIND request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PCIN = pending CINIT (Session services is finding and activating the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>outbound TG)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RES = reset (initial)</td>
</tr>
<tr>
<td>FID</td>
<td>Format ID type</td>
<td>• FID2 = ISR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FID5 = HPR</td>
</tr>
<tr>
<td>PCID</td>
<td>Procedure correlator ID: session identifier</td>
<td><code>--</code></td>
</tr>
</tbody>
</table>

**list cp-cp_sessions**

Use the `list cp` command to display a list of all the adjacent nodes that may have CP-CP sessions with this router. The output list includes all CPs that have an active link that supports CP-CP sessions, as well as CPs that are no longer connected but had an active CP-CP capable link in the past (since APPN was last restarted). Unlike the `list appc` command, one line of output represents a conwinner/conloser session pair.

If the router is configured as a Branch Extender node, the list will indicate only one active CP-CP session pair to an adjacent NN. This is the BEX node’s NN server.

**Example:**

```plaintext
APPN >li cp
```

<table>
<thead>
<tr>
<th>CP Name</th>
<th>Type</th>
<th>Status</th>
<th>ConWinner ID</th>
<th>ConLoser ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Chapter 3. Configuring and Monitoring APPN  237
Table 55. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP name</td>
<td>Fully qualified name of adjacent CP</td>
<td>--</td>
</tr>
</tbody>
</table>
| Type            | Node type of adjacent CP                         | NN = network node  
                    |                     | EN = end node       |
|                 |                                                  | Virt = virtual node |
| Status          | CP-CP session-pair status                        | Active     |
|                 |                                                  | Inactive   |
|                 |                                                  | Pending    |
| ConWinner/Loser ID | Router internal session id for the         | --         |
|                 | contention winner/loser session in the      |            |
|                 | CP-CP session pair, 0 if session is         |            |
|                 | not connected                                   |            |
| ConWinner/Loser sense | SNA sense code for why the     | --         |
|                 | conwinner/loser session last disconnected     |            |

Use the `list dlur dlus` command to display a list of active DLUSs and the status of each session in the DLUR-DLUS pipe. The DLUSs listed may come from one of these sources:

- Configured in the router as the global primary or backup DLUS
- Configured in the router as the primary or backup DLUS for a particular downstream link
- Dynamic DLUS (not configured) that connects to the router and drives call-out to dependent PUs

Example:

```plaintext
APPN > list dlur dlus
```

<table>
<thead>
<tr>
<th>DLUS name</th>
<th>CONWINNER</th>
<th>CONLOSER</th>
</tr>
</thead>
<tbody>
<tr>
<td>STFNET.MVS8</td>
<td>UP</td>
<td>UP</td>
</tr>
</tbody>
</table>

Table 56. List dlur-dlus Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLUS name</td>
<td>Fully qualified CP name of DLUS</td>
<td>--</td>
</tr>
</tbody>
</table>
| ConWinner/Loser state | Status of the contention winner/loser session in the DLUR-DLUS session pair | UP  
                      |                                                  | DOWN   |
|                 |                                                  | PENDING_UP|
|                 |                                                  | PENDING_DOWN|
|                 |                                                  | BLOCKED = waiting for SSCP takeover |

Use the `list dlur lu` command to display a list of active downstream (or internal, for TN3270) PUs with LU statistics for each PU. Dependent PUs in this list either have an active link to the router, or the router is currently attempting to establish a link.
APPN Monitoring Commands

Example:

APPN > list dlur lu

<table>
<thead>
<tr>
<th>CP NAME</th>
<th>LINK NAME</th>
<th>TOTAL LUs</th>
<th>DOWN</th>
<th>PENDING</th>
<th>ACTIVE LU_LU SESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>STFNET.VLNN105 PUSU01</td>
<td>253</td>
<td>0</td>
<td>0</td>
<td>253</td>
<td>0</td>
</tr>
<tr>
<td>STFNET.VLNN105 PUSU021</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>STFNET.VLNN105 PUSU02</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>STFNET.VLNN105 PUSU01</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 57. List dlur lu Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP name</td>
<td>Name of CP on which the LU resides. For TN3270 internal LUs, the router's CP name.</td>
<td>--</td>
</tr>
<tr>
<td>Link name</td>
<td>Configured or dynamically constructed link station name for the link to the dependent PU. This link can be external or internal to the router.</td>
<td>--</td>
</tr>
<tr>
<td>Total LUs</td>
<td>Sum of the number of LUs in all the SSCP-LU states. These LUs need not be defined at the router, but are defined at the host.</td>
<td>--</td>
</tr>
<tr>
<td>SSCP-LU state: down</td>
<td>Number of LUs that have no owning SSCP but still have LU-LU sessions (lost SSCP link but ANS=CONT).</td>
<td>--</td>
</tr>
<tr>
<td>SSCP-LU state: pending</td>
<td>Number of LUs that are waiting for ACTLU response.</td>
<td>--</td>
</tr>
<tr>
<td>SSCP-LU state: active</td>
<td>Number of LUs that have received ACTLU response. This number is not decremented when an LU is bound and enters LU-LU state.</td>
<td>--</td>
</tr>
<tr>
<td>LU-LU session</td>
<td>Number of LUs that currently have LU-LU sessions active</td>
<td>--</td>
</tr>
</tbody>
</table>

Use the list dlur pu command to display a list of downstream (or internal, for TN3270) PUs with their connection status. Dependent PUs in this list either have an active link to the router, or the router is currently attempting to establish a link.

Example:

APPN > list dlur pu

<table>
<thead>
<tr>
<th>CP NAME</th>
<th>STATUS</th>
<th>LOC NAME</th>
<th>SESS</th>
<th>ANS</th>
<th>SSCP</th>
<th>ACT DLUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>; PUNAME NAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STFNET.VLNN105 active</td>
<td>INT</td>
<td>PUSU01</td>
<td>act</td>
<td>CON</td>
<td>PUSU01</td>
<td>STFNET.MVS8</td>
</tr>
<tr>
<td>STFNET.VLNN105 active</td>
<td>INT</td>
<td>PUSU02</td>
<td>act</td>
<td>CON</td>
<td>PUSU02</td>
<td>STFNET.MVS8</td>
</tr>
<tr>
<td>STFNET.VLNN105 active</td>
<td>INT</td>
<td>PUSU01</td>
<td>act</td>
<td>CON</td>
<td>PUSU01</td>
<td>STFNET.MVS8</td>
</tr>
</tbody>
</table>

Table 58. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP name</td>
<td>CP name of the dependent PU. For external PUs, this is the CP name they send in their XID, or, if they do not send one, it is a name the router makes up using the format DLRU..@nnn. For internal PUs, this is the CP name of the router.</td>
<td>--</td>
</tr>
</tbody>
</table>
### Table 58. Output Description (continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>SSCP-PU session status, from the perspective of the DLUR router. You can decode status values as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• pe = pending</td>
</tr>
<tr>
<td></td>
<td>• Re = request</td>
</tr>
<tr>
<td></td>
<td>• Rs = response</td>
</tr>
<tr>
<td></td>
<td>• Actp, Actpu = ACTPU Dactpu = DACTPU</td>
</tr>
<tr>
<td></td>
<td>• LnkAct = link activation</td>
</tr>
<tr>
<td></td>
<td>• Inop = inoperative</td>
</tr>
<tr>
<td>Loc</td>
<td>Location of the PU relative to the DLUR router</td>
</tr>
<tr>
<td></td>
<td>INT = internal</td>
</tr>
<tr>
<td></td>
<td>DON = downstream</td>
</tr>
<tr>
<td>Link name</td>
<td>Configured or dynamically constructed link station name for the link to the dependent PU. This link can be external or internal to the router.</td>
</tr>
<tr>
<td>Sess stat</td>
<td>Status of the DLUR-DLUS pipe that carries control flows for this dependent PU.</td>
</tr>
<tr>
<td></td>
<td>act = active</td>
</tr>
<tr>
<td></td>
<td>res = reset (down)</td>
</tr>
<tr>
<td></td>
<td>pAct = pending active</td>
</tr>
<tr>
<td></td>
<td>plnac = pending inactive</td>
</tr>
<tr>
<td>ANS</td>
<td>Host sysdef value for Automatic Network Shutdown: whether LU-LU sessions should continue or stop when SSCP connectivity is lost.</td>
</tr>
<tr>
<td></td>
<td>CON = continue</td>
</tr>
<tr>
<td></td>
<td>STP = stop</td>
</tr>
<tr>
<td>SSCP PU name</td>
<td>VTAM name for this dependent PU, received in ACTPU.</td>
</tr>
<tr>
<td>Act DLUS name</td>
<td>CP name of the DLUS that currently owns this PU (the &quot;active DLUS&quot;).</td>
</tr>
</tbody>
</table>

#### list dlur status

Use the `list dlur status` command to display a summary of currently active global DLUR configuration information. Note that some of these values have optional link-level overrides.

**Example:**

```
APPN > list dlur st
Primary DLUS Name = STFNET.MVS8
Backup DLUS Name =
retry Time Limit = 15
short Retry Timer = 15
short Retry Count = 20
long retry Timer = 30
Drop Link when there are no session = NO
```

These are all configured data items. See page 112.

#### list ds incompletes

Use the `list ds inc` command to display a list of APPN search
requests ("locates") that are currently in progress. This router is waiting for replies from other nodes in the network.

The command prompts for several possible data filters. For a description of each, see the output description table below.

**Example:**

```appn
APPN > li ds inc
PCID (0 if unknown) [00000000 00000000]? c49bf3d 03310d51
Locate origin CP (NetID.CPname or *) [*]?
Locate origin LU (NetID.LUname or *) [*]?
Locate destination LU (NetID.LUname or *) [*]?
```

<table>
<thead>
<tr>
<th>PCID &amp; Incomplete</th>
<th>Origin CP</th>
<th>Origin LU</th>
<th>Destination LU</th>
</tr>
</thead>
<tbody>
<tr>
<td>STFNET.VLNN105</td>
<td>STFNET.VLNN105</td>
<td>STFNET.VL12</td>
<td></td>
</tr>
<tr>
<td>STFNET.VL15</td>
<td>STFNET.VLNN105</td>
<td>STFNET.VL12</td>
<td></td>
</tr>
</tbody>
</table>

Table 59. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCID</td>
<td>Procedure correlator ID: a network-level correlator for this particular search procedure.</td>
<td>--</td>
</tr>
<tr>
<td>Incomplete child CP names</td>
<td>CP names of nodes to which this router has sent locate requests, and from which it is still awaiting replies.</td>
<td>--</td>
</tr>
<tr>
<td>Origin CP</td>
<td>Name of the CP that started the search originally.</td>
<td>--</td>
</tr>
<tr>
<td>Origin LU</td>
<td>Name of the LU that started the search originally.</td>
<td>--</td>
</tr>
<tr>
<td>Destination LU</td>
<td>Name of the LU being searched for.</td>
<td>--</td>
</tr>
</tbody>
</table>

**list ds resource flag-value pair**

Use this command to display a list of resource (LU) names in this router’s APPN directory.

To limit the data displayed, you can specify one of the following filter flags and a corresponding value:

Table 60. Output Description

<table>
<thead>
<tr>
<th>Filter flag</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>CP name of LU owner, can be qualified with net id or not</td>
<td></td>
</tr>
<tr>
<td>-n</td>
<td>Net id of LU owner</td>
<td></td>
</tr>
<tr>
<td>-l</td>
<td>Fully-qualified LU name</td>
<td></td>
</tr>
<tr>
<td>-s</td>
<td>Fully-qualified server name</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```appn
APPN > li ds res
```

<table>
<thead>
<tr>
<th>LU NAME</th>
<th>SERVER NAME</th>
<th>OWNER NAME</th>
<th>LOCATION TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>STFNET.VLNN105</td>
<td>STFNET.TEMP</td>
<td>WILDCARD HOME</td>
<td></td>
</tr>
<tr>
<td>STFNET.MVS8</td>
<td>STFNET.MVS8</td>
<td>STFNET.MVS8</td>
<td>X-DOMAIN CACHE</td>
</tr>
<tr>
<td>STFNET.CMM08</td>
<td>STFNET.MVS8</td>
<td>STFNET.MVS8</td>
<td>X-DOMAIN CACHE</td>
</tr>
<tr>
<td>STFNET.SD1102</td>
<td>STFNET.VLNN105</td>
<td>STFNET.VLNN105</td>
<td>LOCAL HOME</td>
</tr>
<tr>
<td>STFNET.SD1103</td>
<td>STFNET.VLNN105</td>
<td>STFNET.VLNN105</td>
<td>LOCAL HOME</td>
</tr>
<tr>
<td>STFNET.SD1104</td>
<td>STFNET.VLNN105</td>
<td>STFNET.VLNN105</td>
<td>LOCAL HOME</td>
</tr>
</tbody>
</table>

Chapter 3. Configuring and Monitoring APPN 241
APPN Monitoring Commands

Table 61. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU name</td>
<td>Name of the LU, or &quot;*&quot; to represent a full wildcard.</td>
<td>--</td>
</tr>
<tr>
<td>Server name</td>
<td>CP name of the NN server for that LU.</td>
<td>--</td>
</tr>
<tr>
<td>Owner name</td>
<td>CP name of the LU’s owner. For instance, an EN might own an LU that resides in the EN.</td>
<td>--</td>
</tr>
<tr>
<td>Location</td>
<td>Where the LU is located.</td>
<td>REGISTER = registered by a served EN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X-DOMAIN = in or served by another NN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOCAL = in the router, including LUs served by DLUR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DOMAIN = served by the router as a NN, but not registered</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WILDCARD = owner has a full wild-card (non-explicit) definition</td>
</tr>
<tr>
<td>Type</td>
<td>Category of entry in the directory, reflecting how the entry is to be handled.</td>
<td>HOME = sysdef’d in the router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CACHE = dynamically learned by the router, will age out</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REGISTER = registered by a served EN, can be deregistered by the same EN</td>
</tr>
</tbody>
</table>

**list ds status**

Use this command to display summary statistics about this router’s APPN directory.

**Example:**

```
APPN > l ds s
Maximum Directory Entries = 4000
Current Cache Entries = 3
Current Home Entries = 284
Registered Entries = 0
Directed Locates Received = 0
Broadcast Locates Received = 1
Directed Locates Sent = 2
Broadcast Locates Sent = 2
Directed Locates Not Found = 0
Broadcast Locates Not Found = 0
Outstanding Locates = 0
```

**list dumps**

Use this command to list all APPN dump files on the router hard disk. This command is not available for routers that do not have a hard disk.

**Example:**

```
APPN > l du
1 168084 Thu Jul 01 15:11:18 1999
```
### Table 62. Output Description (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Dump number to use with the transmit dump command</td>
<td>--</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the dump file, in bytes. This number grows while the dump is in progress.</td>
<td>--</td>
</tr>
<tr>
<td>Date/time</td>
<td>Date and time of the last file change. The time changes while the dump is in progress.</td>
<td>--</td>
</tr>
</tbody>
</table>

#### list focal

Use this command to display a list of configured and active dynamic network management focal points with their status.

**Example:**

```
APPN > list foc
```

```
CATEGORY     STATUS  TYPE      FOCAL POINT
ALERT        NOTACT  IMP_PRI  STFNET.CNM08
```

### Table 63. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Category of function performed by the focal point.</td>
<td>ALERT, MS_CAPS, ACCTNG, OTH = other</td>
</tr>
<tr>
<td>Status</td>
<td>Status of LU6.2 sessions to this focal point.</td>
<td>NOTACT = not active, ACT = active, PENDING, NEVERACT = was never active</td>
</tr>
<tr>
<td>Type</td>
<td>Nature of the focal point, using host-centric terms: Explicit = FP is not configured at the router, connects to the router Implicit = FP is configured at the router, router connects to FP Values at the right are listed in high-to-low priority order, where a higher priority FP can dynamically take over as FP.</td>
<td>EXP_PRI = explicit primary, IMP_PRI = implicit primary, BKUP_FP = backup foc. pt., DEF_PRI = default primary, DEF_BKP = default backup, DOMAIN, HOST</td>
</tr>
<tr>
<td>Focal point</td>
<td>CP name of the node providing the focal point function.</td>
<td>--</td>
</tr>
</tbody>
</table>

#### list isr_session

Use this command to display the number of active ISR LU-LU sessions that pass through this router, by link. The counts include:

- Sessions that enter and exit the box using ISR (these sessions count once on each of the inbound and outbound TGs)
- Sessions that enter the box using ISR but exit on an RTP connection (these sessions count once only on the non-HPR TG)
APPN Monitoring Commands

- TN3270 LU sessions routed by DLUR that exit the box using ISR (these sessions are counted only on the real external ISR TG, not on the internal links between DLUR and the local PUs)

Use the list session command to display more information about the counted ISR sessions.

**Example:**

```
APPN >lst isr
```

<table>
<thead>
<tr>
<th>Adjacent CP Name</th>
<th>TG Number</th>
<th>ISR Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>STFNET.CP3174BC</td>
<td>21</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 64. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjacent CP name</td>
<td>CP name of the node adjacent to the router on this TG, either configured or received in an XID.</td>
<td>--</td>
</tr>
<tr>
<td>TG number</td>
<td>Negotiated TG number for this link.</td>
<td>--</td>
</tr>
<tr>
<td>ISR sessions</td>
<td>Number of active ISR sessions on this link.</td>
<td>--</td>
</tr>
</tbody>
</table>

**list link_information**

Use this command to display a list of all configured and all active dynamic links.

**Example:**

```
APPN >ll
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Port Name</th>
<th>Intf</th>
<th>Adj CP Name</th>
<th>Type</th>
<th>HPR</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TO3174</td>
<td>TR005</td>
<td>5</td>
<td>STFNET.CP3174BC</td>
<td>NN</td>
<td>INACTIVE</td>
<td>ACT_LS</td>
</tr>
<tr>
<td>TOLEN</td>
<td>TR00</td>
<td>0</td>
<td>STFNET.TEMP</td>
<td>LEN</td>
<td>ENABLED</td>
<td>RESET_LS</td>
</tr>
<tr>
<td>TOLEN1</td>
<td>TR00</td>
<td>0</td>
<td>STFNET.ABCD</td>
<td>LEN</td>
<td>ENABLED</td>
<td>RESET_LS</td>
</tr>
<tr>
<td>000</td>
<td>TR005</td>
<td>5</td>
<td>STFNET.NN12</td>
<td>NN</td>
<td>ACTIVE</td>
<td>ACT_LS</td>
</tr>
</tbody>
</table>

Table 65. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>For configured links, the link station name you configured. For dynamic links, the router constructs a name of the format &quot;@@@nnnn&quot;, where nnnn starts at zero and continues to increase until it wraps.</td>
<td>--</td>
</tr>
<tr>
<td>Port name</td>
<td>The configured APPN name for the port through which this link is connected.</td>
<td>--</td>
</tr>
<tr>
<td>Intf</td>
<td>The router’s logical interface number for the port through which this link is connected.</td>
<td>--</td>
</tr>
<tr>
<td>Adj CP name</td>
<td>CP name of the node adjacent to the router on this link, either configured or received in an XID.</td>
<td>--</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Configured or actual (if link is active) node type of the adjacent node.</th>
<th>LEN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LEARN (configured only)</td>
</tr>
</tbody>
</table>
### Table 65. Output Description (continued)

<table>
<thead>
<tr>
<th>HPR</th>
<th>Configured or actual (if link is active) status of HPR on the link</th>
<th>ACTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>INACTIVE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ENABLED (configured only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DISABLED (configured only)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Current connection status of the logical link</th>
<th><strong>Steady states</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Some intermediate state definitions:</td>
<td>RESET_LS = reset (down)</td>
</tr>
<tr>
<td></td>
<td>SENT_REQ_OPNSTN = underlying port is active, DLC has been asked to</td>
<td>ACT_LS = active (up)<strong>Going-up states</strong></td>
</tr>
<tr>
<td></td>
<td>contact the remote link station</td>
<td>SENT_CONN_REQ</td>
</tr>
<tr>
<td></td>
<td>PEND_XID_EXCH = remote station contacted, exchanging XIDs</td>
<td>PEND_RCV_CONN_IND</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PEND_SEND_CONN_RSP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SENT_CONN_RSP<strong>Going-down states</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SENT_DEACT_ORD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SENT_DISC_ORD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SENT_DESTROY_TG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PEND_DEACT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PEND_CLOSE_STN</td>
</tr>
</tbody>
</table>

**list link_information link-name**

Use this command to get detailed configuration and status information about a single logical link to an adjacent node.

**Example:**

Appn > li link vm30pu1

Link Station Information
-------------------------------
ls_name = VM30PU1
type = DEFINED
act_at_startup = TRUE
auto_act_supported = FALSE
pan uplink = FALSE
replace inbound CP name/node id = FALSE
retry link act unconditionally = FALSE
adjacent node subnet affiliation = NEGOTIABLE
subnet visit count = 3
remote mac_addr = 402222222222
remote sap_value = 04
hpr_sap_value = C8
real_adj_cp_name = USIBMNR.NRMVM30
node_id = 00000000
cp_cp_sessions_supported = FALSE
hpr_supp = FALSE
### Table 66. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>How the link is known to the router.</td>
<td>DEFINED = configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DYNAMIC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TEMPORARY = not yet able to match against configured links</td>
</tr>
<tr>
<td><strong>Act_at_startup</strong></td>
<td>Whether link is configured to activate when APPN starts up.</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE</td>
</tr>
<tr>
<td><strong>Auto_act_supported</strong></td>
<td>Link is able to be activated only when needed</td>
<td>--</td>
</tr>
<tr>
<td><strong>Pan_uplink</strong></td>
<td>Whether link is configured as a Branch Extender (peripheral access node) uplink (EN appearance upstream to NN).</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE</td>
</tr>
<tr>
<td><strong>Replace inbound CP name / node ID</strong></td>
<td>Whether link is configured that these XID fields from an adjacent LEN node should be overridden by values configured in the router.</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE</td>
</tr>
<tr>
<td><strong>Retry link act unconditionally</strong></td>
<td>Whether link activation failure and link failure should always be retried regardless of the cause.</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE</td>
</tr>
<tr>
<td><strong>Adjacent node subnet affiliation</strong></td>
<td>Whether link is configured to be an EBN link to a different topology subnet.</td>
<td>NATIVE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NON-NATIVE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NEGOTIABLE</td>
</tr>
<tr>
<td><strong>Real adj CP name</strong></td>
<td>CP name received in XID from the adjacent node</td>
<td>--</td>
</tr>
<tr>
<td><strong>CP-CP sessions supported</strong></td>
<td>Configured value from router port or link definition</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE</td>
</tr>
<tr>
<td><strong>Hpr_supp</strong></td>
<td>Configured support for HPR</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE</td>
</tr>
<tr>
<td><strong>Hpr link</strong></td>
<td>Actual negotiated support for HPR on this link</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FALSE</td>
</tr>
<tr>
<td><strong>Link station state</strong></td>
<td>Current connection status of the logical link</td>
<td>Same values as in “list link”</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td>Direction in which link activation occurred</td>
<td>INBOUND</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OUTBOUND</td>
</tr>
<tr>
<td>Tg_isr_type</td>
<td>Link/TG type</td>
<td>ENDPOINT_TG = adjacent node acts as an EN</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>INTERMEDIATE_ROUTING_TG = router acts as NN or EBN and adjacent node is a NN</td>
<td></td>
</tr>
<tr>
<td>Received CV22 sense code</td>
<td>SNA error code for XID exchange failure, received from the adjacent node on this link.</td>
<td>--</td>
</tr>
</tbody>
</table>

**list local_link_information**

Use this command to display a list of logical links inside the router from DLUR to internal PU2.0s. These PUs are used to contain LUs for the TN3270 server function.

**Example:**

```
APPN > li loc
```

<table>
<thead>
<tr>
<th>Name</th>
<th>SSCP PU Name</th>
<th>Node ID</th>
<th>Auto Act</th>
<th>Sense</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSUD1</td>
<td>STFNET.PUSUD12</td>
<td>77DE711</td>
<td>TRUE</td>
<td>0</td>
<td>LOCAL_ACT_LS</td>
</tr>
<tr>
<td>PUSUO2</td>
<td>STFNET.PUSUO2</td>
<td>77D7F12</td>
<td>TRUE</td>
<td>0</td>
<td>LOCAL_ACT_LS</td>
</tr>
<tr>
<td>PUSUO1</td>
<td>STFNET.PUSUO1</td>
<td>77D7F11</td>
<td>TRUE</td>
<td>0</td>
<td>LOCAL_ACT_LS</td>
</tr>
<tr>
<td>PUSU01</td>
<td>STFNET.PUSU01</td>
<td>77D7F11</td>
<td>TRUE</td>
<td>0</td>
<td>LOCAL_ACT_LS</td>
</tr>
</tbody>
</table>

**list port_information**

Use this command to display a list of configured physical and logical APPN router ports and their status.

**Example:**
### Table 68. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf</td>
<td>Router’s logical interface number for this port.</td>
<td>--</td>
</tr>
<tr>
<td>Name</td>
<td>Configured APPN port name.</td>
<td>--</td>
</tr>
<tr>
<td>DLC type</td>
<td>Configured or physical interface type.</td>
<td>ATM, ETHERAND = ethernet, FDDI, FR = frame relay, HPR_IP = enterprise extender, IBMTRNET = token-ring, PPP, MPC+ = multi-path channel +, SDLC, X25 = X.25 QLLC</td>
</tr>
<tr>
<td>HPR</td>
<td>Default HPR status you configured for dynamic links on this port.</td>
<td>TRUE, FALSE</td>
</tr>
<tr>
<td>State</td>
<td>State of the physical or logical interface as APPN perceives it.</td>
<td>Steady states: RESET_PORT = reset (down), ACT_PORT = active (up) <strong>Going-up</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SENT_ENABLE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SENT_ACT_SAP <strong>Going-down</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PEND_START_PORT_DEACT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PEND_LS_DEACT_ORD_PORT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PEND_LS_DEACT_IMM_PORT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SENT_DEACT_SAP</td>
</tr>
</tbody>
</table>

#### list port_information port-name

Use this command to display detailed configuration and status information about one particular port.

**Example:**

```plaintext
APPN > li port t00004
Port Information
===================================
port_name = T00004
dlc_name = IBMTRNET
port_num = 4
max_rcv_btu_size = 2048
ls_role = NEGOTIABLE
sap_value = 04
```
Table 69. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLC name</td>
<td>Port type</td>
<td>Same values as DLC type field in “list port”</td>
</tr>
<tr>
<td>Port num</td>
<td>Router logical interface number for this port</td>
<td>--</td>
</tr>
<tr>
<td>LS role</td>
<td>Initial local link station role on this interface.</td>
<td>PRIMARY, SECONDARY, NEGOTIABLE</td>
</tr>
<tr>
<td>Pan uplink</td>
<td>Whether dynamic links on this port are configured as Branch Extender (peripheral access node) uplinks (EN appearance upstream to NN).</td>
<td>TRUE, FALSE</td>
</tr>
<tr>
<td>Adjacent node subnet affiliation</td>
<td>Whether dynamic links on this port are configured to be EBN links to a different topology subnet.</td>
<td>NATIVE, NON-NATIVE, NEGOTIABLE</td>
</tr>
<tr>
<td>HPR support</td>
<td>Configured support for HPR on dynamic links on this port</td>
<td>TRUE, FALSE</td>
</tr>
<tr>
<td>Port state</td>
<td>State of the physical or logical interface as APPN perceives it</td>
<td>Same values as in list port</td>
</tr>
</tbody>
</table>

**_list rtp_**

Use this command to display a list of the entries in the RTP Partner Table, and summary information about all active RTP connections with an endpoint in the router (the RTP Connection Table).

The RTP Partner Table does not appear if there are no entries in it. An entry is created for each remote node for which all of the following are true:

- The router performed an RTP Route Setup to the node
- The node uses only one NCE for all its RTP connections
- The node has at least one active RTP connection with the router

Note that an RTP Route Setup is not performed during CP-CP or RSETUP RTP activation, so there will be no entry for an adjacent node if the only active RTP connections to it are for carrying CP-CP session or Route Setups. Also note that all levels of the IBM 3746-900/950, and recent levels of VTAM, use multiple NCEs.

**Example:**

```
APPN > li rtp
RTP PARTNER TABLE:
Remote Partner Name Remote Boundary Name TG Number
============================================================================
STFNET.NN12       STFNET.NN12   -1
STFNET.VLNN045     STFNET.CP3174BC 21
RTP CONNECTION TABLE:
```

Chapter 3. Configuring and Monitoring APPN   249
### APPN Monitoring Commands

<table>
<thead>
<tr>
<th>TCID</th>
<th>CP Name</th>
<th>ISR</th>
<th>APPC</th>
<th>Pathswitch</th>
<th>Alive</th>
<th>COS</th>
<th>TPF</th>
<th>TG Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>31BE30E0</td>
<td>STFNET.NN12</td>
<td>0</td>
<td>1</td>
<td>180</td>
<td>180</td>
<td>CPSVCMG</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>31BE4428</td>
<td>STFNET.NN12</td>
<td>0</td>
<td>1</td>
<td>180</td>
<td>180</td>
<td>CPSVCMG</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>31BF4B50</td>
<td>STFNET.NN12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>180</td>
<td>RSETUP</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>31BF6EE0</td>
<td>STFNET.NN12</td>
<td>0</td>
<td>1</td>
<td>180</td>
<td>180</td>
<td>SNASVCMG</td>
<td>21</td>
<td></td>
</tr>
</tbody>
</table>

#### Table 70. Partner Table

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote partner name</td>
<td>CP name of the node in which an RTP connection terminates.</td>
<td>--</td>
</tr>
<tr>
<td>Remote boundary name</td>
<td>CP name of the next ISR node adjacent to the remote partner node, or LU name of the remote application using the RTP connection.</td>
<td>--</td>
</tr>
<tr>
<td>TG number</td>
<td>TG number of the TG to the next ISR node adjacent to the remote partner node. A value of “-1” indicates that the session which caused RTP activation ended in the remote partner node; in this case the “Remote boundary name” is the name of session’s destination LU in the remote partner node.</td>
<td>--</td>
</tr>
</tbody>
</table>

#### Table 71. Connection Table

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCID</td>
<td>Transport Connection ID, a unique identifier for this RTP connection shared by its two end-points.</td>
<td>--</td>
</tr>
<tr>
<td>CP name</td>
<td>CP name of the node in which this RTP connection terminates.</td>
<td>--</td>
</tr>
</tbody>
</table>
| ISR | Number of ISR LU-LU sessions routed onto this RTP connection in the router. This number includes the following session types:  
  • Sessions from LUs in external nodes that come in ISR and leave on HPR, whether routed using DLUR or not  
  • Sessions from TN3270 LUs in this router that leave on HPR, but only if routed using DLUR (sessions on subarea links cannot use HPR) | --         |
| APPC | Number of LU6.2 sessions with an endpoint in this router that are routed onto this RTP connection. This number can include the following session types:  
  • CP-CP sessions to HPR CF-tower capable nodes  
  • DLUR-DLUS pipe sessions  
  • Focal point sessions  
  • Aping sessions | --         |
### Table 71. Connection Table (continued)

<table>
<thead>
<tr>
<th>Pathswitch</th>
<th>Maximum time in seconds to do a path switch, before failing the RTP connection</th>
<th>--</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alive</td>
<td>Time in seconds between heartbeat messages when there is no user traffic</td>
<td>--</td>
</tr>
</tbody>
</table>

### COS TPF

- **CPSVCMG** = CP-CP sessions
- **SNASVCMG** = DLUR-DLUS or FP sessions
- **#BATCH** = standard low-priority
- **#CONNECT** = standard medium-priority
- **#INTER** = standard high-priority
- Other architected and user-defined names exist

- **TG number** = Link/TG number for the first hop of the RTP connection out of the router

- **list rtp tcid** Use this command to display detailed status and statistical information about one or all RTP connections.

### Example:

```plaintext
APPN > li rtp 31CC5DA8
------------------------------------------------------------------------------------------------------------------
TCID CP Name ISR APPC Pathswitch Alive COS TPF TG Number
31CC5DA8 STFNET.VL15 0 2 200 180 CPSVCMG 21
RemoteTCID: 00000000 31C680C8, Role: ACTIVE, State: CONNECTED
FwdRSCV: 16260100 12461080 150BE2E3 C6D5C5E3 ........STFNET
4BE5D3F1 F521 *.VL15.
Xmit: SentBytes SentFrames FramesAck AllowRate ActualRate Tokens?
0x00003009 0x00000057 0 0 311Kbps 0Kbps AVAIL
Recv: RcvdBytes RcvdFrames OutOfSeqQ FramesDiscarded ARBmode
0x0000349B 0x00000055 0 0 GREEN
Misc: SmoothedRoundTrip SR_timeouts FramesResent Pathswitches
   654ms 2 0
FwdMinLinkCapacity: 15974Kb/s, ReverseMinLinkCapacity: 15974Kb/s

Each set of data below is taken over 5 min intervals - New(top), Old(bottom)
Allwdsntrate Actlsendrate SmRoundTrip FramesResent PacketsDisc GapsReptd
0Kb/s 0Kb/s 0ms 0 0 0
0Kb/s 0Kb/s 0ms 0 0 0
0Kb/s 0Kb/s 0ms 0 0 0
0Kb/s 0Kb/s 0ms 0 0 0
```

### Table 72. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Router’s role in establishing this RTP connection</td>
<td>ACTIVE, PASSIVE</td>
</tr>
</tbody>
</table>
**Table 72. Output Description (continued)**

<table>
<thead>
<tr>
<th>Description</th>
<th>State</th>
<th>CONNECTED</th>
<th>CONNECTING</th>
<th>DISCONNECTING</th>
<th>OPENED</th>
<th>CALLING</th>
<th>LISTENING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current state of the connection. If the RTP connection is currently undergoing a path switch, the string &quot;in path switch&quot; is appended to the state value (e.g., &quot;CONNECTED, in path switch&quot;).</td>
<td>State</td>
<td>AVAIL</td>
<td>NOT AVAIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whether the router has permission to send at this instant in time. It is normal for Tokens to be NOT AVAIL whenever FramesQd is nonzero, as long as subsequent displays show SentBytes and SentFrames increasing.</td>
<td>Tokens?</td>
<td>AVAIL</td>
<td>NOT AVAIL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status the router is reporting as a receiver to its partner, based on network congestion detected through ARB calculations.</td>
<td>ARB mode</td>
<td>GREEN</td>
<td>YELLOW</td>
<td>RED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of times the Short Request timer expired. This timer starts when the router sends a control message to its RTP partner. Timer expiration indicates that the reply did not come within the expected time.</td>
<td>SR timeouts</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity of the slowest TG along this RTP's route.</td>
<td>MinLinkCapacity</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum data send rate permitted by the receiver. This is an average value over the 5-minute interval.</td>
<td>Allowed send rate</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculated data send rate based on actual bytes transmitted between the last two rate requests. If there is no data to send, this rate drops. This is an average value over the 5-minute interval.</td>
<td>Actual send rate</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average time to send data to and get reply from the other end of the connection, over the 5-minute interval.</td>
<td>Smoothed round trip</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of frames this router resent in this 5-minute interval due to gaps reported by the receiving partner node (a single gap can result in multiple frames resent).</td>
<td>Frames resent</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of received packets that this router discarded in this 5-minute interval, due to a shortage of APPN buffers in this router or a protocol violation detected.</td>
<td>Packets disc</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 72. Output Description (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaps reptd</td>
<td>Number of data gaps this router reported as a receiver during this 5-minute interval, to the sending partner node.</td>
<td>--</td>
</tr>
</tbody>
</table>

**list session_information**

Use this command to display a list of ISR sessions that flow through the router. These sessions are the same ones counted by link with the command `list isr` and include:

- Sessions that enter and exit the box using ISR
- Sessions that enter the box using ISR but exit on an RTP connection
- TN3270 LU sessions routed by DLUR that exit the box using ISR

This command does not list LU6.2 control sessions with an end-point in the router; use `list appc` to see these sessions. In order to see the full output of this command, you must have configured APPN Node Management parameters to save RSCV information for intermediate sessions.

**Example:**

```
APPN > list sess
```

```
<table>
<thead>
<tr>
<th>Origin CP Name</th>
<th>Primary LU</th>
<th>Secondary LU</th>
<th>Mode Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>STFNET.VL15</td>
<td>STFNET.VL15</td>
<td>STFNET.MVS8</td>
<td>#INTER</td>
</tr>
<tr>
<td>STFNET.VL15</td>
<td>STFNET.MVS8</td>
<td>STFNET.VL15</td>
<td>CPSVRMGR</td>
</tr>
<tr>
<td>STFNET.VL15</td>
<td>STFNET.MVS8</td>
<td>STFNET.VL15</td>
<td>CPSVRMGR</td>
</tr>
</tbody>
</table>
```

Table 73. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin CP name</td>
<td>CP name of the node that owns the primary LU for this session.</td>
<td>--</td>
</tr>
<tr>
<td>Primary LU</td>
<td>LU name of the primary LU.</td>
<td>--</td>
</tr>
<tr>
<td>Secondary LU</td>
<td>LU name of the secondary LU.</td>
<td>--</td>
</tr>
<tr>
<td>Mode name</td>
<td>Mode name used to set up this session. Note that mode names for LU6.2 control sessions (e.g., DLUR-DLUS pipe) do not mean that these sessions terminate in the router. Rather, they are passing through the router via ISR. Use <code>list appc</code> to see the sessions that terminate in the router.</td>
<td>#CONNECT = standard medium priority #INTER = standard high priority CPSVCMG = CP-CP session CPSVRMGR = DLUR-DLUS session SNASVCMG = Focal point session other mode names are architected and can also be user-defined</td>
</tr>
</tbody>
</table>

**list status**

Use this command to display a summary of general APPN configuration and status information. The output provides an “at a glance” view of current status.

**Example:**

```
APPN > list stat
```

```
Fully Qualified CP NAME : STFNET.NETU24
Node up Time : 6 hrs 30 min 21 Sec
Extended Border Node : Not Supp Branch Extender : Not Supp
DLUR : ACTIVE TN3270E : ACTIVE
Main Mem Stat : OK Buffer Mem Stat : OK
```
### Table 74. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQ CP name</td>
<td>Configured network ID and CP name of this router.</td>
<td>--</td>
</tr>
<tr>
<td>Node up time</td>
<td>Amount of time since APPN last restarted.</td>
<td>--</td>
</tr>
</tbody>
</table>
| Extended border node | Whether the router is configured to be an EBN.                             | Supp = configured  
Not Supp = not configured |
| Branch Extender    | Whether the router is configured to be a branch extender node.              | Supp = configured  
Not Supp = not configured |
| DLUR               | Whether DLUR function is configured and active.                            | ACTIVE = configured and running  
NOT ACT = not configured or not running |
| TN3270E            | Whether TN3270 server function is configured and active.                   | ACTIVE = configured and running  
NOT ACT = not configured or not running |
| Main mem stat      | The current state of the main part of APPN memory.                          | OK         
CONSTRED = constrained  
CRITICAL |
| Buffer mem stat    | The current state of the buffer part of APPN memory.                        | OK         
SLOWDOWN  
CONSTRED = constrained  
CRITICAL |

**list topo node**

Use this command to display topology information about a particular node in this router’s topology subnet.

**Example:**

```plaintext
APPN > li topo node
NODE_NAME {}? stfnet.rbkim
CP_NAME NODE ROUTE CON TIME RSN BN HPR ICN CDS NAT TYPE RES GES LEFT SUP
; IVE
*******************************************************************************
stfnet.rbkim NN 128 N 15 23 Y CF N N Y
ACTIVE TGs ORIGINATING FROM THIS NODE
DESTINATION CP CP CP HPR TG_TYPE TG_NUM
*******************************************************************************
NETIDA.RB61 ACT Y APPN 21
STFNET.WK33 ACT Y APPN 21
STFNET.RBB00B NOTSUP Y APPN 21
STFNET.RBRBRUNO ACT Y APPN 21
```

### Table 75. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP name</td>
<td>Control point name of the node, which you input</td>
<td>--</td>
</tr>
</tbody>
</table>
Table 75. Output Description (continued)

<table>
<thead>
<tr>
<th>Node type</th>
<th>Architected type of the node</th>
<th>NN</th>
<th>EN</th>
<th>VN = virtual node (e.g., connection network)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route res</td>
<td>Route addition resistance (higher is more resistant to adding new routes through the node). This value is usually configured at the node and is not dynamic.</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Conges</td>
<td>Congested or not, as dynamically reported by the node.</td>
<td>Y = yes</td>
<td>N = no</td>
<td>--</td>
</tr>
<tr>
<td>Time left</td>
<td>Days remaining for this topology database entry to age out. If you need to force the entry out sooner, VTAM provides topology delete functions that can cause the router to remove entries.</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>RSN</td>
<td>Resource sequence number for this node, used to determine whether an received update contains new information not previously seen.</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>BN</td>
<td>Whether the node performs a Border Node function</td>
<td>Y = yes</td>
<td>N = no</td>
<td>--</td>
</tr>
<tr>
<td>HPR sup</td>
<td>Level of HPR support the node can perform</td>
<td>BASE = ANR forwarding only</td>
<td>TRAN = transport - can have RTP endpoints for data sessions only</td>
<td>CF = control flow - can have RTP endpoints for data and control sessions</td>
</tr>
<tr>
<td>ICN</td>
<td>Interchange node - whether the node is a VTAM performing both SNA subarea and APPN function</td>
<td>Y = yes</td>
<td>N = no</td>
<td>--</td>
</tr>
<tr>
<td>CDS</td>
<td>Central directory server</td>
<td>Y = yes</td>
<td>N = no</td>
<td>--</td>
</tr>
<tr>
<td>Native</td>
<td>Whether the node is in the router’s topology subnet. Note that a node could have the same net id yet be in a different topology subnet.</td>
<td>Y = yes</td>
<td>N = no</td>
<td>--</td>
</tr>
</tbody>
</table>

For a description of the fields in the list “Active TGs originating from this node”, see list topo tg.

**list topo status**

Use this command to display a summary of topology database statistics.

```
APPN > list topo st
Max num of Nodes allowed in Topo( 0 = limit is memory ) : 5400
Current number of Nodes in Topology : 25
Number of Node records purged from this node : 0
```
**APPN Monitoring Commands**

Number of TG records purged from this node : 0
The last flow reduction seq num sent out by this node : 259
Topology safe store frequency (0 = not saved) : 0

Table 76. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max nodes allowed</td>
<td>Calculated value for the maximum number of nodes allowed in the database, based on the amount of APPN memory, the product type, and various min and max limits.</td>
<td>--</td>
</tr>
<tr>
<td>Number of node records purged</td>
<td>Number of node records deleted because they aged out or because of VTAM-initiated network topology operations.</td>
<td>--</td>
</tr>
<tr>
<td>Number of TG records purged</td>
<td>Number of node records deleted because they aged out or because of VTAM-initiated network topology operations</td>
<td>--</td>
</tr>
<tr>
<td>Last FRSN sent out</td>
<td>Latest flow reduction sequence number sent out by this node to any other node.</td>
<td>--</td>
</tr>
<tr>
<td>Topology safe store frequency</td>
<td>Configured time in minutes between backups of topology data base to the router’s hard disk.</td>
<td>0 = topology safe store is not enabled</td>
</tr>
</tbody>
</table>

**list topo tg flag-value pairs**

Use this command to display information in the router’s topology database about active TGs (links, or transmission groups) in this topology subnet.

To limit the data displayed, you can specify one or more of the following filter flags and corresponding values.

Table 77. Output Description

<table>
<thead>
<tr>
<th>Filter flag</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>CP name of TG owner, can be qualified with net id or not</td>
</tr>
<tr>
<td>-n</td>
<td>Net id of TG owner</td>
</tr>
<tr>
<td>-p</td>
<td>Fully qualified name of TG partner</td>
</tr>
</tbody>
</table>

**Example:**

```appn
APPN > li topo tg -c c20015
ACTIVE TG'S
TG OWNER   TG DESTINATION   CP_CP   HPR   TG_TYPE   TG   RSN
NUM
STFNET.C20015 STFNET.VLNN045 ACT Y APPN 23 444
STFNET.C20015 STFNET.PDLUR2 ACT N APPN 1 436
```

Table 78. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>TG owner</td>
<td>CP name of the node that reported this TG. Both endpoints of a TG report the TG, each as the owner with the other as the destination.</td>
<td>--</td>
</tr>
<tr>
<td>TG destination</td>
<td>CP name of the other end of the TG relative to the owner.</td>
<td>--</td>
</tr>
</tbody>
</table>
Table 78. Output Description (continued)

<table>
<thead>
<tr>
<th>CP-CP</th>
<th>CP-CP session support on this TG</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>active</td>
</tr>
<tr>
<td>NOTSUP</td>
<td>not supported</td>
</tr>
<tr>
<td>SUPINACT</td>
<td>supported but inactive</td>
</tr>
<tr>
<td>(e.g., parallel TGs where only one carries CP-CP sessions)</td>
<td></td>
</tr>
<tr>
<td>UNK</td>
<td>unknown</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HPR</th>
<th>HPR support on this TG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>yes</td>
</tr>
<tr>
<td>N</td>
<td>no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TG type</th>
<th>Architected type of this TG</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPN</td>
<td></td>
</tr>
<tr>
<td>INTER</td>
<td>interchange, a Subarea to APPN link</td>
</tr>
<tr>
<td>VIRT</td>
<td>virtual, e.g., a link to a connection network virtual node</td>
</tr>
</tbody>
</table>

Log

Use this command to display APPN’s internal event log.

Syntax:

```
log
status
view
```

APPN keeps its own internal event log, in addition to the router’s ELS event logging. Use this command to display current summary statistics about the APPN event log.

Example:

```
APPN > log st
Entries: 32, Discarded: 0, Filtered: 25959, Memory: 9348 of 273400
Filters enabled:
    none
Display direction: Descending
Top Entry:
    32|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
Bottom Entry:
    1|Jul 23 08:55:45 2F104-14 (E) NOF unable to monitor EGPE environment
Current Time:
    Fri Jul 23 15:47:35 1999
```

Table 79. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry numbers</td>
<td>The total number of entries, the number discarded due to the log being full, and the number filtered out as duplicates.</td>
<td>--</td>
</tr>
<tr>
<td>Memory size</td>
<td>Error log current size and maximum size in bytes. The maximum size is fixed at about 1% of APPN memory.</td>
<td>--</td>
</tr>
</tbody>
</table>
**APPN Monitoring Commands**

*Table 79. Output Description (continued)*

<table>
<thead>
<tr>
<th>Filters enabled</th>
<th>A list of log output viewing filters that you currently have set.</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Severity: severity level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Message: message ID</td>
</tr>
<tr>
<td>Display direction</td>
<td>The time order of output viewing that you currently have set.</td>
<td>Descending (newest at top)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ascending</td>
</tr>
<tr>
<td>Top/bottom entries</td>
<td>Summary line for each of these entries (order is dependent on display direction). This lets you see the time scope of the entries currently in the log.</td>
<td>--</td>
</tr>
<tr>
<td>Current time</td>
<td>Current day and time with same basis as log entries.</td>
<td>--</td>
</tr>
</tbody>
</table>

**log view**

Use the `log view` command to enter a submenu of commands for navigating and viewing the APPN event log.

When you enter log viewing mode, you can use the commands `bottom`, `top`, `goto`, `next`, and `prev` to move around and display log entries in summary mode (a page of 1 or 2-line entries at a time). You use the commands `det next`, `det prev`, and `det entry` to move around and display the details of individual log entries.

The log viewing submenu also contains commands to control settings for log viewing. You can use the `filter` command to select the minimum severity level you wish to see, or to only look for a single message type. Each use of the `filter` command overrides all previous settings; it does not combine with previous commands. You can use the `set` command to establish log viewing preferences.

Submenu syntax and functions are as follows:

*Table 80. Log view Submenu Syntax*

<table>
<thead>
<tr>
<th>Command</th>
<th>Keywords and Parameters</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bottom</code></td>
<td></td>
<td>Move to bottom, show summary page</td>
</tr>
<tr>
<td><code>current</code></td>
<td></td>
<td>Redisplay current summary page</td>
</tr>
<tr>
<td><code>detail</code></td>
<td><code>next_entry</code></td>
<td>Display the next entry in detail</td>
</tr>
<tr>
<td></td>
<td><code>prev_entry</code></td>
<td>Display the previous entry in detail</td>
</tr>
<tr>
<td></td>
<td><code>entry_id seq_num</code></td>
<td>Display the specified entry in detail</td>
</tr>
<tr>
<td><code>filter</code></td>
<td><code>all</code></td>
<td>Clear output filters (show all)</td>
</tr>
<tr>
<td></td>
<td><code>only severity action_required</code></td>
<td>Show entries with this severity or greater.</td>
</tr>
<tr>
<td></td>
<td><code>critical</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>error</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>warning</code></td>
<td></td>
</tr>
</tbody>
</table>
APPN Monitoring Commands

Table 80. Log view Submenu Syntax (continued)

<table>
<thead>
<tr>
<th>Submenu Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>informational</td>
<td>Show only entries with this msg</td>
</tr>
<tr>
<td>message message-id</td>
<td>Move to entry, show summary page</td>
</tr>
<tr>
<td>sequence_num</td>
<td>Display next summary page</td>
</tr>
<tr>
<td>prev_page</td>
<td>Display previous summary page</td>
</tr>
<tr>
<td>lines_in_page</td>
<td>Show this many lines in page</td>
</tr>
<tr>
<td>direction ascending</td>
<td>Show newest entry last</td>
</tr>
<tr>
<td>descending</td>
<td>Show newest entry last</td>
</tr>
<tr>
<td>top</td>
<td>Move to top, display summary page</td>
</tr>
<tr>
<td>exit</td>
<td>Return to main APPN menu</td>
</tr>
</tbody>
</table>

Example:

APPN > log v
LOG VIEW
LOG VIEW >?
BOTTOM
CURRENT
DETAIL
FILTER
GOTO_ENTRY
NEXT_PAGE
PREV_PAGE
SET =
TOP
EXIT

LOG VIEW > top
32 Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
31 Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
30 Jul 23 15:08:15 2F10A-1A (I) Request Route
29 Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
28 Jul 23 15:08:15 2F10A-1A (I) Request Route
27 Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
26 Jul 23 15:08:15 2F10A-1A (I) Request Route
25 Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
24 Jul 23 11:41:06 2F120-18 (C) Correlation table entry was not found.
23 Jul 23 11:37:46 2F120-18 (C) Correlation table entry was not found.
22 Jul 23 11:07:27 2F120-18 (C) Correlation table entry was not found.
21 Jul 23 11:07:27 2F126-0D (E) TNS0013I %1: Keepalive processing detected error ; the connection between IP addr %2 and LU %3 has been ended.

LOG VIEW > det e 21
-------------
Sequence Number: 210
APPN Lifetime: 7206.950 seconds
Fri Jul 23 11:07:27 1999
ProbeID 22606683
Message 2F126000-0000000D
Severity: Error
TNS0013I %1: Keepalive processing detected error ; the connection between IP addr %2 and LU %3 has been ended.
(Sn) e124102
(Sn) 15.170.99.210
(Sn) STAT1
### APPN Monitoring Commands

**Table 81. Output Description (Summary Page, left to right)**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Unique number assigned to this event when it is written to the log (not when displayed). This is the number you use with the &quot;goto&quot; and &quot;detail&quot; commands.</td>
<td>--</td>
</tr>
<tr>
<td>Date / time</td>
<td>When the event occurred, per this router's clock.</td>
<td>--</td>
</tr>
<tr>
<td>Message ID</td>
<td>Major-minor message identifier for the condition that occurred. See the “APPN Log Event Reference Guide” for a description of every possible message. Append three zeros to the major and prepend six zeros to the minor part of the ID to map to the values in the Reference Guide.</td>
<td>--</td>
</tr>
</tbody>
</table>
| Severity      | APPN classification of how serious the event is. Key values are listed in the order of decreasing severity. | A = action required  
C = critical  
E = error  
W = warning  
I = informational |
| Event name    | Brief description of the event. Use the “detail” command and the Reference Guide for more information. | --         |

**Table 82. Output Description (Event Details)**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Same number described above for the summary page.</td>
<td>--</td>
</tr>
<tr>
<td>APPN lifetime</td>
<td>Time in seconds from when APPN last started.</td>
<td>--</td>
</tr>
<tr>
<td>Date / time</td>
<td>Same as on summary page.</td>
<td>--</td>
</tr>
<tr>
<td>Probe ID</td>
<td>ID for the exact software location that logged this error.</td>
<td></td>
</tr>
<tr>
<td>Message ID</td>
<td>Same as on summary page, but expanded with leading and trailing zeros to match the “APPN Log Event Reference Guide”.</td>
<td>--</td>
</tr>
<tr>
<td>Severity</td>
<td>Same values as on summary page, but expanded in words.</td>
<td>See above</td>
</tr>
<tr>
<td>Event name</td>
<td>Brief description of the event, enhanced by the data items listed below it. Use the Reference Guide for more information.</td>
<td>--</td>
</tr>
</tbody>
</table>
Table 82. Output Description (Event Details) (continued)

| Data type labels | Identifiers for the different types of data logged with each message. See the Reference Guide for a description of the data items with each message. | (lx) (Se) (X) others ... |

Memory

Use the Memory command to display APPN memory usage information.

Syntax:

```
memory
```

Example:

```
APPN > mem
APPN memory status:
        Size (MB) Percent in-use State
Main 152  17     OK
Buffer 19  0     OK
Total 171  14

APPN total shared memory size= 179200000, special use= 800
APPN main part: size = 159487200 crit_thresh= 151512840 cons_thresh= 143538480
APPN main part: inuse= 26516176 (incl: Trace tbl=65536, Error log= 1447)
APPN main part: peak memory usage= 26518048
APPN main part: event counts: crit= 0 cons= 0 OK = 1
APPN main part: OK for last 278211 seconds
APPN bufr part: size = 19712000 crit= 18726400 cons= 17740800 slow= 13404160
APPN bufr part: inuse= 1232 reserved (< slow)= 24992
APPN bufr part: peak memory usage= 26360
APPN bufr part: event counts: crit= 0 cons= 0 slow= 0 OK = 1
APPN bufr part: OK for last 278211 seconds
```

Table 83. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total shared memory</td>
<td>Configured size of APPN and TN3270 server data memory, in bytes. You set this when you configure APPN. It does not include the APPN or router code space, or the data/buffer memory needed by other router components. The &quot;special use&quot; part of this is not counted in the main or buffer parts, and is for APPN system control structures.</td>
<td>--</td>
</tr>
</tbody>
</table>
### APPN Monitoring Commands

**Table 83. Output Description (continued)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main part</strong></td>
<td>Part of APPN shared memory that is used for control blocks, trace tables, internal messages, and other general fixed and dynamic data. This part includes two special data areas: - a trace table (Trace tbl) fixed at 2% of total shared memory or 64KB, whichever is larger. For Network Utility, it is fixed at 20MB. This table is allocated at APPN startup. - an event log (Error log) that grows up to 1% of total shared memory</td>
</tr>
<tr>
<td><strong>Buffer part</strong></td>
<td>Part of APPN shared memory that is used for packet/frame buffering. The &quot;reserved&quot; part of this is a dynamic number of committed buffer space that statistically backs a larger logical buffer space. &quot;(&lt; slow)&quot; indicates that this value must remain below the slow threshold for normal functioning.</td>
</tr>
<tr>
<td><strong>Main states</strong></td>
<td>State of the main part of APPN memory relative to calculated threshold values. When the main state becomes progressively more congested, APPN takes some of these actions to help ease congestion: put links into local busy, and reject incoming broadcast searches.</td>
</tr>
<tr>
<td><strong>Buffer states</strong></td>
<td>State of the buffer part of APPN memory relative to calculated threshold values. Note that the buffer state is considered critical any time the main part is critical, regardless of the level of buffer memory usage. When the buffer state becomes progressively more congested, APPN takes some of these actions to help ease congestion: reject new sessions, pace session data flow more slowly, report the node as congested in topology updates, slow down RTP senders, put links into local busy, and even disconnect current lowest-priority sessions.</td>
</tr>
<tr>
<td><strong>Inuse, peak usage</strong></td>
<td>Current number of bytes in use, and the high water mark that the in-use value ever reached.</td>
</tr>
<tr>
<td><strong>Event counts</strong></td>
<td>Number of times a given state occurred since APPN last restarted.</td>
</tr>
</tbody>
</table>
Table 83. Output Description (continued)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;state&gt; for last nn seconds</td>
<td>Length of time that the memory part has been in the current state. If the node has ever entered a depletion state, additional information is provided about how long that state lasted, how long ago it was, etc.</td>
</tr>
</tbody>
</table>

**Rtp status**
Use the `rtp status` to display currently in-use global RTP configuration information.

**Syntax:**

`rtp status`

**Example:**

```
APPN > rtp stat
```

<table>
<thead>
<tr>
<th></th>
<th>Network</th>
<th>High</th>
<th>Medium</th>
<th>&amp;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liveness timer</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>Path Switch Timer</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>Retries</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 84. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network, etc.</td>
<td>SNA transmission priority</td>
</tr>
<tr>
<td>Liveness timer</td>
<td>Time in seconds between heartbeat messages when there is no user traffic.</td>
</tr>
<tr>
<td>Path switch timer</td>
<td>Maximum time in seconds to do a path switch, before failing the RTP connection.</td>
</tr>
<tr>
<td>Retries</td>
<td>Number of short request retries to do before attempting a path switch.</td>
</tr>
</tbody>
</table>

**Rtp switchpath**
Use the `rtp switchpath` to force an HPR path switch for an RTP connection that has an endpoint in this router. The path switch operation selects the best currently available path, which may in fact be the current path. In any case, the path switch causes a temporary suspension of user traffic flow on the specified RTP connection.

To use this command, use `list rtp` first to determine the TCID of the RTP connection you wish to force a path switch on. Type “rtp switch” and provide that TCID when prompted. To see the results of the path switch, use `list rtp tcid`, and look at the status of the connection to determine when path switch is complete (status reverts to “active”). You can see the new path either in the RSCV or by using `rtp test`.

**Syntax:**

`rtp switchpath`

**Rtp test**
Use the `rtp test` command to perform an HPR route test and display information about each link hop along the path of the RTP connection. Use the `list rtp` command first to determine the TCID of the RTP connection you wish to test. This command performs the same action as the older command `test rtp`.

**Syntax:**

`rtp test`
APPN Monitoring Commands

**_rtp test_

**Example:**

APPN > _rtp test_
Enter TCID of the route to be tested [0]? 31B96928
Route Test issued
Waiting for 10 Seconds....
Information

=================
Result : SUCCESS
Detailed Information

=================

<table>
<thead>
<tr>
<th>TG OWNER</th>
<th>TG DEST NAME</th>
<th>TGNUM</th>
<th>RT TIME</th>
<th>DELTA TIME</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>STFNET.VLNN105</td>
<td>STFNET.VL16</td>
<td>21</td>
<td>8</td>
<td>8</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>STFNET.VL16</td>
<td>STFNET.VL15</td>
<td>21</td>
<td>68</td>
<td>60</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

Table 85. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result (overall)</td>
<td>Status or failure reason for the route test operation.</td>
<td>SUCCESS, IN PROGRESS, NO RESPONSE, INVALID NCE ID, INVALID TCID, NO ROUTE</td>
</tr>
<tr>
<td>TG owner</td>
<td>CP name of the nearest node on this route hop.</td>
<td>--</td>
</tr>
<tr>
<td>TG dest name</td>
<td>CP name of the far node on this route hop.</td>
<td>--</td>
</tr>
<tr>
<td>TG num</td>
<td>Number for this link as negotiated between the owner and destination.</td>
<td>--</td>
</tr>
<tr>
<td>RT time</td>
<td>Round-trip time in milliseconds from the router to the TG destination.</td>
<td>--</td>
</tr>
<tr>
<td>Delta time</td>
<td>Round-trip time in milliseconds from the TG owner to the destination, i.e., the portion of RT time that is just for this hop.</td>
<td>--</td>
</tr>
<tr>
<td>Result (detailed)</td>
<td>Status of reaching the destination of this hop.</td>
<td>SUCCESS, NO RESPONSE</td>
</tr>
</tbody>
</table>

**Restart**

Use the `restart` command to restart APPN and TN3270 disruptively, without restarting or reloading the rest of the router software. If APPN is not already stopped, this command stops APPN before restarting.

When APPN restarts, it uses the current in-memory configuration information, whether or not that information has been written to disk using the `talk 6 write` command (only for router models with a hard disk).

**Syntax:**

```
restart
```
Stop
Use the **stop** command to stop APPN and TN3270 disruptively without affecting the rest of the route.

Syntax:
```
stop
```

**TN3270E**
Use the **tn3270e** command to access the **TN3270E>** command prompt from which you can display information about the TN3270E configuration.

See [Table 86](#) for a description of these commands.

Syntax:
```
tn3270e
```

### TN3270E Monitoring Commands

**Table 86. TN3270E Monitoring Command Summary**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See Getting Help on page xxvii.</td>
</tr>
<tr>
<td>Deactivate lu_name</td>
<td>Deactivates an LU in use by a TN3270 client, and to disconnect the corresponding TCP connection to that client.</td>
</tr>
<tr>
<td>List</td>
<td>Lists the following from configuration memory:</td>
</tr>
<tr>
<td></td>
<td>• Connections</td>
</tr>
<tr>
<td></td>
<td>• Connections <strong>LU name</strong></td>
</tr>
<tr>
<td></td>
<td>• Connections <strong>IP address</strong></td>
</tr>
<tr>
<td></td>
<td>• Maps</td>
</tr>
<tr>
<td></td>
<td>• Pools</td>
</tr>
<tr>
<td></td>
<td>• Pools <strong>pool name</strong></td>
</tr>
<tr>
<td></td>
<td>• Ports</td>
</tr>
<tr>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See Entering a Lower Level Environment on page xxvii.</td>
</tr>
</tbody>
</table>

---

**Deactivate LU**

Use the **deactivate LU** command to deactivate an LU in use by a TN3270 client, and to disconnect the corresponding TCP connection to that client. Use the **list conn** command first to determine the local LU name based on IP address, VTAM LU name, or pool name.

This command provides success/failure completion status, and you can also use list commands to check status. After deactivation, the client should no longer appear under **list conn**, and **list lu** or **list pu** **puname** should reflect the change in LU status.

Syntax:
```
deactivate lu local lu_name
```
APPN Monitoring Commands

List

Use the list command to display information about TN32870 connections.

Syntax:

```
list
   connections
   lu internal_LU_name
   _mapping
   pools
   pools pool_name
   ports
   pu
   pu pu_name
   _rejections
   status
```

Command Function

```
list connections flag-value pair
```

Use this command to display a complete or subset list of active TN3270 client connections.

To limit the data displayed, you can specify one or more of the following filter flags and corresponding values:

**Table 87. Flag Description**

<table>
<thead>
<tr>
<th>Filter flag</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l (flag not required, you can just type the value)</td>
<td>Router LU name or pool name</td>
</tr>
<tr>
<td>-i (flag not required, you can just type the value)</td>
<td>Client IP address, or a leading substring of that address. For example, 9.67 will satisfy all IP addresses of format 9.67.<em>.</em></td>
</tr>
<tr>
<td>-p</td>
<td>VTAM primary LU name</td>
</tr>
<tr>
<td>-s</td>
<td>VTAM secondary LU name (normally does not match router LU name)</td>
</tr>
</tbody>
</table>

**Example:**

```
TN3270E > li conn

Local LU | Class | Assoc LU | Client Addr | Status | Prim LU | Sec LU | Idle Min
---------|-------|----------|-------------|--------|--------|--------|---------
PU1LU207 | IW | 9.37.182.187 | LU-LU | NRAW30 | LU2207 | 8 |
PU1LU60 | IW | 9.37.176.39 | LU-LU | NRAW30 | LU2260 | 52 |
PU1LU89 | IW | 9.37.178.49 | LU-LU | NRAW30 | LU2289 | 288 |
```

**Table 88. Output Description**

<table>
<thead>
<tr>
<th>Column title</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local LU</td>
<td>LU name configured or host-defined in the router.</td>
<td>--</td>
</tr>
</tbody>
</table>
### Table 88. Output Description (continued)

<table>
<thead>
<tr>
<th>Class</th>
<th>Type of LU</th>
<th>IW = implicit workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EW = explicit workstation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP = implicit printer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP = explicit printer</td>
</tr>
</tbody>
</table>

| Assoc LU    | For a workstation LU, the name of any associated printer LU | -- |

| Client addr | IP address of the client. Note that a single client IP address may have multiple LUs in use, by varying its TCP source port. | -- |

<table>
<thead>
<tr>
<th>Status</th>
<th>Connected state of the LU</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SSCP-LU state</td>
</tr>
<tr>
<td></td>
<td>LU-LU state</td>
</tr>
<tr>
<td></td>
<td>blank = TCP connection exists but LU is not connected yet</td>
</tr>
</tbody>
</table>

| Prim LU     | Primary LU name as known to VTAM                                             | -- |

| Sec LU      | Secondary LU name as known to VTAM                                           | -- |

| Idle min    | Number of minutes since this connection carried any user data               | -- |

**list lu internal LU name**

Use this command to display detailed configuration and status information about a single internal LU. Use the **list conn** or **list pu name** commands to help determine the router LU name for a particular LU.

**Example:**

```
TN3270E > li lu pu1lu207
LUNAME : PU1LU207 NAU : 207 LINK NAME : VM30PU1
POOL NAME : PUBLIC MODEL : 3270002
SSCP LU ST : NOT PCHSCON , LUNENABLE , NOT ACTURSP , NOT TRMNOTFY
             NOT NOTIFIED , ACTIVATD , NOT DEACTING , NOT ACTIVNG
             NOT NMVTSNT , NOT NMVTRCV , COUNTED , NOT DACPUPEN
             NOT TERMPEND , NOT NMVTOFF
LU LU ST : NOT SNTUNBIND , BOUND , NOT UNBINDING , NOT BINDING
FLAGS : NOT SEGSFOR , FAPBP , GETPCID , NOT BINDFR
         NOT SESSTOP , NOT DETCHRCV , LSACON , HSACON
FLAGS1 : NOT MXEXPD , NOT PENDSF , WRAPNORM , NOT INOPST
         NOT SII , NOT EXIT , OWNED , INITCOMP
VERB FLAGS: NOT EXIT , NOT SF , NOT TERM , NOT INIT , NOT PURG , NOT R01
            NOT R02 , NOT R03 , NOT R04 , BID , NOT WR1 , NOT WR2
ACTLU : 4915 DACTLU : 0 BIND : 0 UNBIND : 0 NOTIFY : 1 MINI TRACE : WRAPPED : NO NUMBER OF ENTRIES : 7
OTHERS : 14 : INIT ,NEW : INIT ,GETPCID : INIT ,PCIDREPY : INIT ,PCHSCOND
           INIT ,SENNOTFY : INIT ,NOTFYRSP
```

### Table 89. Output Description

<table>
<thead>
<tr>
<th>Column title</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU name</td>
<td>LU name configured or host-defined in the router, which you input.</td>
<td>--</td>
</tr>
<tr>
<td>NAU</td>
<td>SNA 1-byte NAU address of this LU on its PU (2-254). This value is now displayed in decimal.</td>
<td>--</td>
</tr>
</tbody>
</table>
APPN Monitoring Commands

Table 89. Output Description (continued)

| Link name | For subarea host links, the link station name of the external link associated with this PU. For DLUR host links, the PU/station name of the internal link to DLUR. | -- |
| Pool name | Name of the pool through which this LU can be selected by a client. | -- |
| Model | 3270 display or printer model this LU supports. | -- |
| SSCP_LU state | Value decodings of individual bits of SSCP-LU session status for this LU, for engineering use | -- |
| LU_LU state | Value decodings of individual bits of LU-LU session status for this LU, for engineering use | -- |
| Flags, Flags1, Verb flags | Other state flags for engineering use | -- |
| Other output | Other state information for engineering use | -- |

**list mapping**

Use this command to see the currently active configured mappings between client IP address and TN3270 LUs in the router. You can also test which mapping entries apply to a particular client IP address.

To limit the data displayed to the entries the server will use for a particular IP address, just specify that IP address when you invoke this command.

**Example:**

```
TN3270E > 11 map
TN3270E Client IP Address to LU Name Maps
Client IP Address Mask Name Resource Port Map Type Resource
---------------------------------------------------------------------------
8.1.1.99 255.255.255.255 <DEFLT> 23 Y POOL WORKSTATION
9.9.9.9 255.255.255.255 LU45 0 Y LU WORKSTATION
9.1.1.1 255.255.255.255 LU47 0 Y LU PRINTER
4.4.4.4 255.255.255.255 LU46 0 Y LU WORKSTATION
7.7.7.7 255.255.255.255 LU48 0 Y LU PRINTER
2.2.2.2 255.255.0.0 POOL2 0 N POOL PRINTER
1.1.1.1 1.1.1.1 POOL1 0 N POOL WORKSTATION
0.0.0.0 0.0.0.0 <DEFLT> 0 N POOL WORKSTATION
```

Table 90. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP address</td>
<td>IP address seed for matching client IP addresses</td>
<td>--</td>
</tr>
<tr>
<td>Address mask</td>
<td>Bit mask to be applied to the address seed and incoming client addresses to determine whether this mapping applies to this client. Only bit positions where the mask bit is 1 are compared.</td>
<td>255.255.255.255 = compare the entire incoming client IP address</td>
</tr>
<tr>
<td>Resource name</td>
<td>LU name or pool name configured in the router</td>
<td>&lt;DEFLT&gt; = the globally configured default pool</td>
</tr>
</tbody>
</table>
Table 90. Output Description (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Server destination TCP port for incoming connections to be matched against this entry. 0 = entry applies to all destination ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last map</td>
<td>If a match is found on this entry but cannot be satisfied by the pool/LU, whether the server should go on to try and match the connection against less specific entries. Y = yes N = no</td>
</tr>
<tr>
<td>Type</td>
<td>Whether the resource name is an LU or pool</td>
</tr>
<tr>
<td>Resource</td>
<td>Type of LU or type of LUs in pool</td>
</tr>
</tbody>
</table>

Example:

```
list pools
```

Use this command to list configured named pools of implicit LUs. Clients can request any LU in a pool by passing the pool name on their connection request.

```
TN3270E > li pool
TN3270E Implicit pools
Default pool name : PUBLIC
Name   Class
----------------------------
PUBLIC   WORKSTATION
POOL2   PRINTER
POOL1   WORKSTATION
POOL3   WORKSTATION
POOL4   WORKSTATION
```

Table 91. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default pool name</td>
<td>Name of the global default pool into which all implicit LUs not placed into another pool fall. This is the pool referenced by the string &lt;DEFLT&gt; in various commands and displays.</td>
<td>--</td>
</tr>
<tr>
<td>Name</td>
<td>Configured name of the pool</td>
<td>--</td>
</tr>
<tr>
<td>Class</td>
<td>Configured type of LUs in the pool</td>
<td>WORKSTATION PRINTER</td>
</tr>
</tbody>
</table>

Example:

```
list pools poolname
```

Use this command to show detailed configuration information about a single LU pool. This command allows you to see how the LUs in a pool are distributed among dependent PUs, how they are named, and what type they have. For full information about the LUs under a particular PU, use the `list pu name` command.

Example:

```
TN3270E > li pools pool1
TN3270E Implicit Pool Pool Name : POOL1 Pool Class : WORKSTATION
Station Name : PU1
LU Name Mask : 002LU
Number of lus : 200
Model Type : 3270 mod 2
```

Example:
**APPN Monitoring Commands**

```
TN3270E > li pools pool2
TN3270E Implicit Pool
----------------------------------------------------------------------------
Pool Name : POOL2 Pool Class : PRINTER
----------------------------------------------------------------------------
Station Name : PU1
LU Name Mask : @03LU
LU Address Range : 5-10,78-99
Model Type : SCS

Station Name : PU1
LU Name: LU48
NAU Address : 48
Model Type : 3270
```

**Table 92. Output Description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Station name</td>
<td>For subarea host links, the link station name associated with the dependent PU. For DLUR host attachment, the local PU name.</td>
<td>--</td>
</tr>
<tr>
<td>LU name mask</td>
<td>For implicit LUs only, the configured name seed the router uses to generate LU names in the given address range or number.</td>
<td>--</td>
</tr>
<tr>
<td>LU address range</td>
<td>For implicit LUs only, the NAU address range the router uses to generate LUs in this pool under this PU.</td>
<td>--</td>
</tr>
<tr>
<td>Number of LUs</td>
<td>For implicit LUs only, the number of LUs the router generates under this PU.</td>
<td>--</td>
</tr>
<tr>
<td>LU name</td>
<td>For an individual explicit LU only, the configured LU name.</td>
<td>--</td>
</tr>
<tr>
<td>NAU address</td>
<td>For an individual explicit LU only, the 1-byte NAU address for the LU.</td>
<td>--</td>
</tr>
<tr>
<td>Model type</td>
<td>Configured type of the single LU or group of LUs.</td>
<td>For displays:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3270 mod 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3270 mod 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3270 mod 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3270 mod 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For printers:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3270</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCS</td>
</tr>
</tbody>
</table>

**list ports**

Use this command to display all the TCP ports that TN3270 clients can connect to, and the configured characteristics of each port.

**Example:**

```
TN3270E > li ports
TN3270E Server Ports
Port Number TN3270E Resource Name Disable Filtering
23        Y <DEFLT> N
45        Y <DEFLT> N
66        Y <DEFLT> Y
88        Y POOL1 N
99        Y <DEFLT> N
```
### Table 93. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Destination TCP port number in the router that clients connect to.</td>
<td>--</td>
</tr>
<tr>
<td>TN3270E</td>
<td>Whether this port is configured to support &quot;E&quot; clients or not.</td>
<td>Y = yes, N = no</td>
</tr>
<tr>
<td>Resource name</td>
<td>Configured pool name for clients connecting to this port.</td>
<td>&lt;DEFLT&gt; = the global default implicit pool, other names are user-configured</td>
</tr>
<tr>
<td>Disable filtering</td>
<td>Whether client IP address maps should be checked for clients connecting to this port.</td>
<td>Y = yes, N = no</td>
</tr>
</tbody>
</table>

**list pu**

Use this command to display all internal dependent PUs configured for TN3270 LUs, including those that use DLUR and those that use subarea host links.

**Example:**

```plaintext
TN3270E > list pu
```

<table>
<thead>
<tr>
<th>PU name</th>
<th>Status</th>
<th>Node ID</th>
<th>TOTAL LUs</th>
<th>DDDLU enabled</th>
<th>LUs active</th>
<th>LUs owned</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM30PU1</td>
<td>ACTPU_RCVD</td>
<td>07711111</td>
<td>249</td>
<td>N</td>
<td>249</td>
<td>5 244</td>
</tr>
<tr>
<td>VM30PU2</td>
<td>ACTPU_RCVD</td>
<td>07722222</td>
<td>249</td>
<td>N</td>
<td>249</td>
<td>5 244</td>
</tr>
</tbody>
</table>

### Table 94. Output Description

<table>
<thead>
<tr>
<th>Column title</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU name</td>
<td>For PUs associated with subarea links, the configured link station name of the host link. For PUs associated with DLUR, the configured local PU name.</td>
<td>--</td>
</tr>
<tr>
<td>Status</td>
<td>Current status of the SSCP-PU session</td>
<td>ACTPU_RCVD, NOT ACTIVE</td>
</tr>
<tr>
<td>Node ID</td>
<td>The internal configured node id that represents this dependent PU to VTAM.</td>
<td>--</td>
</tr>
<tr>
<td>Total LUs</td>
<td>The current number of LUs defined in the router under this PU. This includes both configured LUs and active host-initiated dynamic LUs.</td>
<td>--</td>
</tr>
<tr>
<td>DDDLU enabled</td>
<td>Whether this PU is configured for dynamic LU definition.</td>
<td>Y = yes, N = n</td>
</tr>
<tr>
<td>LUs active</td>
<td>Number of LUs that have been ACTLU’d from the host. This number can include both configured and host-initiated DDDLU LUs.</td>
<td>--</td>
</tr>
<tr>
<td>LUs owned</td>
<td>Number of LUs that are associated with client TCP connections.</td>
<td>--</td>
</tr>
</tbody>
</table>
### APPN Monitoring Commands

#### Table 94. Output Description (continued)

<table>
<thead>
<tr>
<th>LUs available</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of LUs that are active or DDDLU-capable and are not owned, so are available for use by TN3270 clients. This number can include configured LUs whose PU is active and supports DDDLU, but does not include host-initiated DDDLU LUs unless they are active.</td>
<td>--</td>
<td></td>
</tr>
</tbody>
</table>

#### list pu pu-name

Use this command to display configuration and status information for all LUs under a particular dependent PU in the router. These LUs include:

- configured implicit LUs, whose names the router generates based on configured name seeds, and whose NAU addresses the router assigns based on configured numbers of LUs or address ranges
- configured explicit LUs, whose names and NAU addresses are completely configured
- host-initiated dynamic LUs, whose names and NAU addresses are set by the host

**Example:**

```
TN3270E > list pu vm30pu1
```

<table>
<thead>
<tr>
<th>LU Name</th>
<th>NAU add</th>
<th>Status</th>
<th>Own</th>
<th>Pool</th>
<th>SCCP LU</th>
<th>LU LU</th>
<th>Flags</th>
<th>Flags1</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUI1LU2</td>
<td>02</td>
<td>ACTIV</td>
<td>NO</td>
<td>PUBLIC</td>
<td>(04,20)</td>
<td>00</td>
<td>02</td>
<td>00</td>
</tr>
<tr>
<td>PUI1LU3</td>
<td>03</td>
<td>ACTIV</td>
<td>NO</td>
<td>PUBLIC</td>
<td>(04,20)</td>
<td>00</td>
<td>02</td>
<td>00</td>
</tr>
<tr>
<td>PUI1LU4</td>
<td>04</td>
<td>ACTIV</td>
<td>NO</td>
<td>PUBLIC</td>
<td>(04,20)</td>
<td>00</td>
<td>02</td>
<td>00</td>
</tr>
<tr>
<td>PUI1LU5</td>
<td>05</td>
<td>ACTIV</td>
<td>NO</td>
<td>PUBLIC</td>
<td>(04,20)</td>
<td>00</td>
<td>02</td>
<td>00</td>
</tr>
<tr>
<td>PUI1LU6</td>
<td>06</td>
<td>ACTIV</td>
<td>NO</td>
<td>PUBLIC</td>
<td>(04,20)</td>
<td>00</td>
<td>02</td>
<td>00</td>
</tr>
<tr>
<td>PUI1LU7</td>
<td>07</td>
<td>ACTIV</td>
<td>NO</td>
<td>PUBLIC</td>
<td>(04,20)</td>
<td>00</td>
<td>02</td>
<td>00</td>
</tr>
</tbody>
</table>

#### Table 95. Output Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU Name</td>
<td>Name of the LU as it is known to the router. This name is either fully configured at the router, generated by the router based on a configured seed value, or passed from the host for a host-initiated dynamic LU.</td>
<td>--</td>
</tr>
<tr>
<td>NAU add</td>
<td>The 1-byte SNA address for this LU under this PU. This value is either configured at the router, selected by the router, or passed from the host. The value is now displayed in decimal.</td>
<td>--</td>
</tr>
<tr>
<td>Status</td>
<td>Current status of this single LU</td>
<td>ACTIV, NOT ACT</td>
</tr>
<tr>
<td>Own</td>
<td>Whether this LU is associated with a TN3270 client TCP connection</td>
<td>YES, NO</td>
</tr>
</tbody>
</table>
**Table 95. Output Description (continued)**

<table>
<thead>
<tr>
<th>Pool name</th>
<th>Pool name through which a client may be assigned this LU.</th>
<th>Blank for explicit LUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCP_LU status, LU_LU status, Flags, flags1</td>
<td>Hex values of status fields for engineering use. To see these values decoded, use the <code>list lu name</code> command.</td>
<td>--</td>
</tr>
</tbody>
</table>

**list rejections**

Use this command to display a list of up to 99 of the most recently rejected TN3270 client connections. This can help you see and correct the reason for the rejections. The list is sorted with the most recent rejection at the top, and shows all rejections including multiple attempts by the same client.

**Example:**

```plaintext
TN3270E > li rej
Connection Rejection Table
------------------------------------------------------------------
1 Time : 7/23/1999 11:09:00
   Client : 15.170.99.210
   Reason : Client is not authorized by Filter entries
2 Time : 7/23/1999 11:08:59
   Client : 15.170.99.210
   Reason : Client is not authorized by Filter entries
3 Time : 7/23/1999 11:08:59
   Client : 15.170.99.32
   Reason : Client is not authorized by Filter entries
```

**Table 96. Output Description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Day and time the rejection occurred.</td>
<td>--</td>
</tr>
<tr>
<td>Client</td>
<td>IP address of the client.</td>
<td>--</td>
</tr>
</tbody>
</table>

**Reason**

Text describing why the server rejected the client connection. There are currently over 40 reasons defined.

Example reasons include:

- Node is terminating
- Couldn’t get memory
- No LUs available
- Requested LU not found/available
- LU type validation failed
- LU capping value reached
- LU Pool depleted
- APPN memory constrained

**list status**

Use this command to display a summary of configuration and current status information for the TN3270 server function.

**Example:**

```plaintext
TN3270E > li st
TN3270E Server Status Summary
TN3270E IP Address: 9.37.179.142
NetDisp Advisor Port Number: 10008
Keepalive type: NOP Frequency: 60
Automatic Logoff: N
Client IP Address mapping : N
Number of connections : 10
Number of available LUA LU's : 498
Number of LUA LU's pending termination : 0
```
### APPN Monitoring Commands

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Key values</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address within the router to which the TN3270 clients connect</td>
<td>--</td>
</tr>
<tr>
<td>NetDisp advisor port number</td>
<td>TCP port number to which the Network Dispatcher load balancing function can connect to poll for load information on this server.</td>
<td>--</td>
</tr>
<tr>
<td>Keepalive type</td>
<td>Whether and how the server polls clients to see if they are still active.</td>
<td>None = server does not poll clients, and will discover client absence only when trying to send data, NOP = server polls clients at the TCP level, Timing mark = server polls clients at the TN3270 level</td>
</tr>
<tr>
<td>Frequency</td>
<td>Interval in seconds between keepalive polls</td>
<td>--</td>
</tr>
<tr>
<td>Automatic logoff</td>
<td>Whether or not the server disconnects clients after a period of inactivity (no data flowing in either direction).</td>
<td>Y = yes, N = no</td>
</tr>
<tr>
<td>Client IP address mapping</td>
<td>Whether the server is globally enabled to map incoming IP addresses to LU/pool names</td>
<td>Y = yes, N = no</td>
</tr>
<tr>
<td>Number of connections</td>
<td>Current number of active TCP connections to TN3270 clients</td>
<td>--</td>
</tr>
<tr>
<td>Number of available LUA LUs</td>
<td>Number of LUs that are currently activated from the host, or are dynamically capable of activation. This includes LUs that are in currently in use by TN3270 clients.</td>
<td>--</td>
</tr>
<tr>
<td>Number of LUA LU's pending termination</td>
<td>Number of LUs that are going down, and the router is waiting for host confirmation. These LUs are no longer associated with TN3270 client connections.</td>
<td>--</td>
</tr>
<tr>
<td>Number of defined LU's</td>
<td>Number of LUs that are either configured in the router or active host-initiated dynamic LUs.</td>
<td>--</td>
</tr>
<tr>
<td>Number of connections in SSCP-LU state</td>
<td>Number of active TCP connections associated with an LU in SSCP-LU state. When the LU associated with a connection is bound by an application and enters LU-LU state, this number is decremented (even though the SSCP-LU connection is still active).</td>
<td>--</td>
</tr>
<tr>
<td>Number of connections in LU-LU state</td>
<td>Number of active TCP connections associated with an LU in LU-LU state.</td>
<td>--</td>
</tr>
</tbody>
</table>
APPN Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

APPN supports the CONFIG (Talk 6) delete interface command with the following considerations:

- When an interface is deleted, the ports and links defined over this interface are deleted when APPN is restarted.
- If an activate_new_config from Talk 6 or a restart from Talk 5 is issued before a device reload, any of the interfaces greater than the interface deleted will not be redefined successfully.

GWCON (Talk 5) Activate Interface

APPN supports the GWCON (Talk 5) activate interface command with the following consideration:

When an interface is activated, the ports and links in APPN SRAM for this interface are defined to the APPN node and activated.

All APPN interface-specific commands are supported by the GWCON (Talk 5) activate interface command.

GWCON (Talk 5) Reset Interface

APPN supports the GWCON (Talk 5) reset interface command with the following consideration:

- When an interface is reset, the ports and links defined over this interface are taken down. If the link is a subarea TN3270E link, the APPN node will be restarted. For a normal port, the port and link definitions are deleted. After the interface becomes active, the port definitions and link definitions are redefined and activated.

All APPN interface-specific commands are supported by the GWCON (Talk 5) reset interface command.

GWCON (Talk 5) Component Reset Commands

APPN supports the following APPN-specific GWCON (Talk 5) reset commands:

GWCON, Protocol Appn, Restart Command

Description:
This command restarts the APPN node.

Network Effect:
The APPN data flowing through this node will be disrupted. APPN is stopped and restarted.

Limitations:
The changes made to the APPN configuration (Talk 6) will also be reflected.

All APPN commands are supported by the GWCON, protocol appn, restart command.
**APPN Monitoring Commands**

### CONFIG (Talk 6) Activate Commands

APPN supports the following CONFIG (Talk 6) **activate** commands:

- **CONFIG, Protocol APPN, Activate_new_config Command (OR)**
- **CONFIG, Protocol APPN, TN3270E, Activate_new_config Command**

**Description:**

This command activates any changes made to APPN config.

**Network Effect:**

If the change cannot be activated dynamically, APPN is restarted.

**Limitations:**

- If the change cannot be activated dynamically, APPN is restarted. Examples of this are changes to any of the node parameters, the default DLUR parameters, or the global tn3270e parameters. Some of the deletion commands also restart the APPN node. Deletion of link stations or ports does not restart the APPN node except if the link stations are subarea tn3270e links.
- If the changes are made to the tuning parameters, a device reload or restart is required.

All APPN commands are supported by the **CONFIG, protocol appn, activate_new_config (OR) CONFIG, protocol appn, tn3270e, activate_new_config** command.
Chapter 4. Using AppleTalk Phase 2

This chapter describes the AppleTalk Phase 2 (AP2) configuration commands and includes the following sections:

- "Basic Configuration Procedures"
- "AppleTalk 2 Zone Filters" on page 278
- "Sample Configuration Procedures" on page 279

Basic Configuration Procedures

This section outlines the initial steps required to get the AppleTalk Phase 2 protocol up and running. Information on how to make further configuration changes will be covered in the command sections of this chapter. For the new configuration changes to take effect, the router must be restarted.

Enabling Router Parameters

When you configure a router to forward AppleTalk Phase 2 packets, you must enable certain parameters regardless of the number or type of interfaces in the router. If you have multiple routers transferring AppleTalk Phase 2 packets, specify these parameters for each router.

- Globally Enable AppleTalk Phase 2: To begin, you must globally enable the AppleTalk Phase 2 software using the AppleTalk Phase 2 configuration command. If the router displays an error in this step, there is no AppleTalk Phase 2 software present in your load. If this is the case, contact your customer service representative.

- Enable Specific Interfaces: You must then enable the specific interfaces over which AppleTalk Phase 2 is to send the packets. Use the enable interface command to do this.

Note: When enabling AppleTalk over ATM, you must enable the specific emulated LAN interfaces over which AppleTalk is to send packets. You must not enable AppleTalk over the physical ATM interface. All further uses of the word “interface” in this chapter refer to the emulated LAN interface, not the ATM physical interface.

- Enable Checksumming: You can then determine whether the router will compute DDP checksums of packets it originates. Checksum software does not work correctly in some AppleTalk Phase 2 implementations, so you may not want to originate packets with checksums for compatibility with these implementations. Normally, however, you will want to enable the generation of checksums. Any packet forwarded with a checksum will have its checksum verified.

Setting Network Parameters

You must also specify certain parameters for each network and interface that sends and receives AppleTalk Phase 2 packets. After you have specified the parameters, use the AppleTalk Phase 2 list configuration command to view the results of the configuration.

- Set the Network Range for Seed Routers: Coordinating network ranges and zone lists for all routers on a network is simplified by having specific routers designated as seed routers. Seed routers are configured with the network range and zone list while all other routers are given null values. Null values indicate that the router should query the network for values from the seed routers. For every network (segment) of your interconnected AppleTalk internet, at least one router interface must be configured as the seed router for that network. There are...
Using AppleTalk Phase 2

usually several seed routers on a network in case one of them fails. Also, a router can be a seed router for some or all of its network interfaces. Use the `set net-range` command to assign the network range in seed routers.

- Set the Starting Node Number: Use the `set node` command to assign the starting node number for the router. The router will AARP for this node, but if it is already in use, a new node will be chosen.
- Add a Zone Name: You can add one or more zone names for each network in the internetwork. You can add a zone name for a given network in any router connected to that network; however, only the seed router needs to contain the zone name information for a connected network. Attached routers dynamically acquire the zone name from adjacent routers using the ZIP protocol. Apple recommends that, for a given network, you choose the same seed router for the network number and the zone name. The zone name cannot be configured for a network unless the network number is also configured. To add a zone name for each network number, use the AppleTalk Phase 2 configuration `add zone name` command.

AppleTalk over PPP

There are two modes for AppleTalk over PPP, full-router and half-router. In full-router mode, the point-to-point network is visible to other AppleTalk routers. In half-router mode, the point-to-point network is invisible to other routers, but it still transmits AppleTalk routing information and data packets.

To set up your network for full-router mode, give each router on the PPP link a common network number, a common zone name, and a unique node number. If you configure one end of the PPP link with a non-zero network number, you must also configure that end to have a non-zero node number and to have a zone name. In this case, the other end of the link must have either:

- The same network number and zone name and a different node number.
- Network and node numbers set to zero. The router will learn network and node numbers from the configured router.

To set up your network for half-router mode, configure both routers on the PPP link so that network and node numbers are set to zero and no zone name is used.

AppleTalk 2 Zone Filters

Zone name filtering, although not required for AppleTalk, is a very desirable feature for the security and administration of large AppleTalk Internetworks. There are also provisions for restricting access to networks by net numbers.

General Information

AppleTalk is structured so that every network is identified in two ways. The first is a network number or range of consecutive network numbers that must be unique throughout the internet. The network number combined with the node number uniquely identifies any end station in the internet.

The second identifier for the network is one or more zone names. These zone name strings are not unique throughout the internet. The end station is uniquely identified by a combined `object:type:ZoneName-string`.

A router first learns about a network when the new net range appears in the RTMP routing update from a neighboring router. The router then queries the neighbor for
the zone names of the new network. Note that the net range is repeated in every new RTMP update but that the zone names are requested only once.

The end stations obtain the network numbers from the broadcasted RTMP (routing information) packets and then choose a node number. This net/node pair is then AARPed for (AARP Probe) to see if any other end station has already claimed its use. If another station responds, another net/node pair is chosen by the end station and the process repeated until no responses are received.

Why Zone Name Filters?

When the typical AppleTalk end station wants to use a service (printer, file server) on the Apple Internet, it first looks at all available zones and selects one. It then chooses a service type and requests a list of all names advertising the type in the chosen zone. Several problems arise from this mechanism.

- A large internet may have many zones. Presenting the user with a long list to choose from obscures the needed ones (thereby inhibiting usability of the list).
- The server may not want to make itself available throughout the internet (for security reasons). If the zone that the service is in is not visible to the client, security is enhanced.
- Restricting the zones that are visible from a department to the rest of the internet will allow the internet administration to let the department control (or not) its own domain while not increasing the overhead for the rest of the internet (reducing administration).

The filtering of network numbers further enhances the security and administration of the internet. Network access is only indirectly controlled by zone filtering. An unregulated department could add networks with the same zone names but new net numbers that conflict with other departments. Network number filtering can be used to prevent these random additions of zone names and net numbers from impacting the rest of the network.

How Do You Add Filters?

The router is configured with an exclusive (meaning block the specified zones) or inclusive (meaning allow only these zones) list of zones for each direction on each interface. The specified interface will not readvertise filtered zone information in the defined direction. If all zones in a network’s zone list are filtered, network information will also be filtered across the interface.

- Use configuration commands `add` and `delete`, to create the filter list for an interface.
- Use configuration commands `enable` and `disable` to specify how the filter list is applied.

Use similar commands to create network number filters.

Other Commands:
You can use the `AP2 CONFIG>` `list` command to display all filter information for the interfaces. In addition, the `list` command accepts an `interface#` as an argument so that you can list information for only an interface.

Sample Configuration Procedures

This section covers the steps required to get AP2 up and running. For information on how to make further configuration changes, see "AppleTalk Phase 2 Configuration Commands" on page 285. For the configuration changes to take effect, you must restart the router.
Using AppleTalk Phase 2

To access the AP2 configuration environment, enter `protocol ap2` at the Config> prompt.

Enabling AP2
When you configure a router to forward AP2 packets, you must enable certain parameters. If you have multiple routers transferring AP2 packets, specify these parameters for each router. To enable AP2:

1. Use the `enable ap2` command to globally enable AP2 on the router. For example:
   
   AP2 config> enable ap2

2. Enable the specific interfaces over which AP2 is to send packets. For example:
   
   AP2 config> enable interface 1

Setting Network Parameters
To set up your router as a seed router, you must set the network range, a starting node number, and at least one zone name. You can configure some interfaces on a router as seed routers and leave other interfaces as non-seed routers. You must have at least one seed router for each AppleTalk network, and you should configure several seed routers on a network in case one of them fails.

Note: Do not set a network range or a node number for half routers.

1. Use the `set net-range` command to set the Network Range. For example:
   
   AP2 config> set net-range
   Interface # [0]? 1
   First Network range number (1-65535, or 0 to delete) []? 1
   Last Network range number (1-65535) []? 5

   Enter the same first and last values for a single-numbered network.

2. Use the `set node-number` command to set the Starting Node Number for the interface. The router will AARP for this node. If the number is already in use, the router will choose a new number. For example:
   
   AP2 config> set node-number
   Interface # [0]? 1
   Node number (1-253, or 0 to delete) []? 1

3. Use the `add zone` command to add one or more zone names for the network attached to the interface. If you define a network range for an interface, you should also define the zone names for the interface. If you did not define a network number, do not define zone names. For example:
   
   AP2 config> add zone
   Interface # [0]? 1
   Zone name []? Finance

After you have specified the parameters, you can use the `list` command at the AP2 config> prompt to view your configuration.

Setting Up Zone Filters
Zone filtering lets you filter zones in each direction on each interface. To filter incoming packets, set up an input filter. To filter outgoing packets, set up an output filter. The interface will not readvertise filtered zone information in the direction that you define. Follow these steps to set up a zone filter:

1. Add zone filters to an interface. Use the `add zfilter in` command to add an input zone filter to an interface. Use the `add zfilter out` command to add an output zone filter to an interface. For example:
   
   AP2 config> add zfilter in
   Interface # [0]? 1
   Zone name []? Admin
2. Enable the zone filters that you added. This turns on the filter and controls whether the filter is inclusive or exclusive. Inclusive filters forward only the zone information in that filter. Exclusive filters block only the zone information in that filter. For example:

```plaintext
AP2 config> enable zfilter in exc
Interface # [0]?  1
```

The following are some examples that explain how to set up zone filters in the internet shown in Figure 11.

**Figure 11. Example of Zone Filtering**

**Example 1**

The following is an example of how to filter the Manufacturing zone from all other networks. To do this, you would set up an input filter on Interface 1 of Router A to exclude the Manufacturing zone.

1. On Router A, add an input zone filter to Interface 1.

   ```plaintext
   AP2 config> add zfilter in
   Interface # [0]?  1
   Zone name []? Manufacturing
   ```

2. Enable the input zone filter and make the filter exclusive.

   ```plaintext
   AP2 config> enable zfilter in exc
   Interface # [0]?  1
   ```

   This excludes Manufacturing zone information from entering Router A, thereby filtering the zone from the rest of the internet.

**Example 2**

The following example shows how to filter the Manufacturing zone from Network 11-15, but still allow the Manufacturing zone to be visible on Network 1-5. To do this, you would set up an output filter on Interface 3 of Router A to exclude Manufacturing zone information from being forwarded out of Interface 3. The interface will continue to advertise Manufacturing zone information over interfaces 1 and 2 on Router A, making it visible on Network 1-5.

1. Add an output zone filter to Interface 3.

   ```plaintext
   AP2 config> add zfilter out
   Interface # [0]?  3
   Zone name []? Manufacturing
   ```
2. Enable the output zone filter and make the filter exclusive.

```
AP2 config> enable zfilter out exc
Interface # [0]? 3
```

This filter excludes Manufacturing zone information from the output of Interface 3.

**Example 3**

The next example shows how to set up a filter so that the Admin zone is visible on all networks, but the Finance zone is not visible to the rest of the internet.

1. Add an input zone filter to Interface 2 on Router A.

```
AP2 config> add zfilter in
Interface # [0]? 2
Zone name []? Admin
```

2. Enable the input zone filter and make it inclusive.

```
AP2 config> enable zfilter in inc
Interface # [0]? 2
```

By setting up this input filter as inclusive, only Admin zone information is forwarded through Interface 2 to the rest of the internet.

**Setting Up Network Filters**

Network filters are similar to zone filters, except they let you filter an entire network. To set up a network filter:

1. Add a network filter. Use the `add nfilter in` command to add an input network filter to an interface. Use the `add nfilter out` command to add an output network filter to an interface. For example:

```
AP2 config> add nfilter out
Interface # [0]? 2
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 15
```

The network range you enter here must match the range that you assigned to that network.

2. Enable the network filter that you added and make it either inclusive or exclusive. Inclusive filters forward only network information in that filter. Exclusive filters block only network information in a filter, and they allow all other network information to be forwarded.

```
AP2 config> enable nfilter in exc
Interface # [0]? 2
```

Following are some examples that explain how to set up network filters in the internet, as shown in Figure 12 on page 283.
The following steps show how to filter Network 6-10 so that it is not visible to Network 16-20 as shown in Figure 12.

1. Add an output network filter for Network 6-10 to Interface 2 on Router B.
   ```
   AP2 config>
   add nfilter out
   Interface # [0]? 2
   First Network range number (decimal) [0]? 6
   Last Network range number (decimal) [0]? 10
   ```

2. Enable the output network filter as exclusive.
   ```
   AP2 config>enable nfilter out exc
   Interface # [0]? 2
   ```

   This filter excludes all information on Network 6-10 from being forwarded through Interface 2 to Network 16-20.

---

**Figure 12. Example of Network Filtering.**

The following steps show how to filter Network 6-10 so that it is not visible to Network 16-20 as shown in Figure 12.

1. Add an output network filter for Network 6-10 to Interface 2 on Router B.
   ```
   AP2 config>
   add nfilter out
   Interface # [0]? 2
   First Network range number (decimal) [0]? 6
   Last Network range number (decimal) [0]? 10
   ```

2. Enable the output network filter as exclusive.
   ```
   AP2 config>enable nfilter out exc
   Interface # [0]? 2
   ```

   This filter excludes all information on Network 6-10 from being forwarded through Interface 2 to Network 16-20.
Using AppleTalk Phase 2
Chapter 5. Configuring and Monitoring AppleTalk Phase 2

This chapter describes the AppleTalk Phase 2 (AP2) configuring and monitoring commands. It includes the following sections:

- "Accessing the AppleTalk Phase 2 Configuration Environment"
- "AppleTalk Phase 2 Configuration Commands"
- "Accessing the AppleTalk Phase 2 Monitoring Environment" on page 292
- "AppleTalk Phase 2 Monitoring Commands" on page 292

Accessing the AppleTalk Phase 2 Configuration Environment

To access the AppleTalk Phase 2 configuration environment, enter the following command at the Config> prompt:

```
Config> ap2
```

AP2 Protocol user configuration

AP2 Config>

AppleTalk Phase 2 Configuration Commands

This section describes the AppleTalk Phase 2 configuration commands.

The AppleTalk Phase 2 configuration commands allow you to specify network parameters for router interfaces that transmit AppleTalk Phase 2 packets. The information you specify with the configuration commands becomes activated when you restart the router.

Enter the AppleTalk Phase 2 configuration commands at the AP2 config> prompt. Table 98 shows the commands.

Table 98. AppleTalk Phase 2 Configuration Commands Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxvii.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds zone names, network filters, and zone filters to an interface.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the zone names, interfaces, network filters, and zone filters.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables interfaces, checksumming, split-horizon routing, network filters, or zone filters, or globally disables AppleTalk Phase 2.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables interfaces, checksumming, split-horizon routing, network filters, zone filters, or globally enables AppleTalk Phase 2.</td>
</tr>
<tr>
<td>List</td>
<td>Displays the current AppleTalk Phase 2 configuration.</td>
</tr>
<tr>
<td>Set</td>
<td>Sets the cache size, network range, and node number.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxviii.</td>
</tr>
</tbody>
</table>

Add

Use the add command to add the zone name to the interface zone list or to add the zone name to the interface zone list as the default for the interface or to add network and zone filters.

**Syntax:**

```
add zone . . .
```
AppleTalk Phase 2 Configuration Commands (Talk 6)

defaultzone . . .
ţfilter in . . .
ţfilter out . . .
zfilter in . . .
zfilter out . . .

zone interface# zonename
Adds the zone name to the interface zone list. If you define a network number for an interface, you should also define the zone names for the interface. If you did not define a network number, do not define zone names.

Example:

   ap2config>add zone
   Interface # [0]? 0
   Zone name []? Finance

defaultzone interface# zonename
Adds a default zone name for the interface. If a node on the network requests a zone name that is invalid, the router assigns the default zone name to the node until another zone name is chosen. If you add more than one default to an interface, the last one added overrides the previous default. If you do not add a default, the first zone name added using the zone command is the default.

Example:

   ap2config>add defaultzone
   Interface # [0]? 0
   Zone name []? Headquarters

ţfilter in interface# first network# last network#
Adds a network filter to the input of the interface. The network range that you enter must match the network range you set for that interface. You cannot filter only a portion of a network range. For example, if you set a network range of 1–10, and you set up a filter for 5–8, the router filters the full network range of 1–10.

Example:

   ap2config>add nfilter in
   Interface # [0]? 0
   First Network range number (decimal) [0]? 1
   Last Network range number (decimal) [0]? 10

ţfilter out interface# first network# last network#
Adds a network filter to the output of the interface. The network range that you enter must match the network range you set for that interface. You cannot filter only a portion of a network range. For example, if you set a network range of 1–0, and you set up a filter for 5–8, the router filters the full network range of 1–10.

Example:

   ap2config>add nfilter out
   Interface # [0]? 0
   First Network range number (decimal) [0]? 11
   Last Network range number (decimal) [0]? 20

zfilter in interface# zone name
Adds a zone name filter to the input or output of the interface.

Example:

   ap2config>add zfilter in
   Interface # [0]? 0
   Zone name []? Marketing

zfilter out interface# zone name
Adds a zone name filter to the output of the interface.
Delete

Use the **delete** command to delete a zone name from the interface zone list, network or zone name filters, or all AppleTalk Phase 2 information from an interface.

**Syntax:**

```plaintext
delete

zone interface# zonename

Delete a zone name from the interface zone list.

Example:

```plaintext
ap2config>delete zone 2 newyork
```

*nfilter in* interface# first network# last network#

Deletes a network filter from the input of the interface. You must enter the same network range numbers you set using the **add nfilter in** command.

**Example:**

```plaintext
ap2config>delete nfilter in

Interface # [0]? 0
First Network range number (decimal) [0]? 1
Last Network range number (decimal) [0]? 12
```

*nfilter out* interface#

Deletes a network filter from the output of the interface. You must enter the same network range numbers you set using the **add nfilter out** command.

**Example:**

```plaintext
ap2config>delete nfilter out

Interface # [0]? 0
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 20
```

*zfilter in* interface# zone name

Deletes a zone name filter from the input of the interface.

**Example:**

```plaintext
ap2config>delete nfilter in

Interface # [0]? 1
Zone name []? Marketing
```

*zfilter out* interface# zone name

Deletes a zone name filter from the output of the interface.

**Example:**

```plaintext
delete zfilter out

Interface # [0]? 1
Zone name []? Marketing
```

**interface**

Use this command to delete an interface. This is the only way to delete zone names that have non-printing characters.

**Example:**

```plaintext
ap2config>delete interface 1
```
**AppleTalk Phase 2 Configuration Commands (Talk 6)**

**Disable**

Use the `disable` command to disable AP2 on all interfaces or on a specified interface, checksumming, filtering, APL/AP2 translation, or split horizon routing.

**Syntax:**

```
  disable
  ap2
  checksum
  interface...
  nfilter in...
  nfilter out...
  zfilter in...
  zfilter out...
  split-horizon-routing...
```

**ap2** Disables the AppleTalk Phase 2 packet forwarder for all interfaces.

**Example:**

```
ap2config>disable ap2
```

**checksum**

Specifies that the router will not compute the checksum in packets it generates. The router usually checksums all packets it forwards. This is the default.

**Example:**

```
ap2config>disable checksum
```

**interface** `interface#`

Disables all AP2 functions on the specified network interface. The network continues to remain available for all other protocols.

**Example:**

```
ap2config>disable interface 2
```

**nfilter in** `interface#`

Disables, but does not delete, the input network filters on this interface.

**Example:**

```
ap2config>disable nfilter in
  Interface # [0]? 2
```

**nfilter out** `interface#`

Disables, but does not delete, the output network filters on this interface.

**Example:**

```
ap2config>disable nfilter out
  Interface # [0]? 2
```

**zfilter in** `interface#`

Disables, but does not delete, the input zone filters on this interface.

**Example:**

```
ap2config>disable zfilter in
  Interface # [0]? 1
```

**zfilter out** `interface#`

Disables, but does not delete, the output zone filters on this interface.

**Example:**

```
ap2config>disable zfilter out
  Interface # [0]? 1
```

**split-horizon-routing** `interface#`

Disables split-horizon-routing on this interface. You need to disable
AppleTalk Phase 2 Configuration Commands (Talk 6)

split-horizon routing only on Frame Relay interfaces that are on a hub in a partially-meshed Frame Relay network. Disabling split-horizon routing causes all of the routing tables to be propagated on this interface.

Example:

```
ap2config>disable split-horizon-routing 0
```

Enable

Use the `enable` command to enable the checksum function, to enable a specified interface, to enable AppleTalk 2 gateway function, or to globally enable the AppleTalk Phase 2 protocol.

**Syntax:**

```
enable
```

- `ap2` Enables the AppleTalk Phase 2 packet forwarder over all of the interfaces.
  
  **Example:**
  
  ``ap2config>enable ap2
  
  checksum` Specifies that the router will compute the checksum in packets it generates. The router checksums all AP2 packets it forwards.

  **Example:**

  ```ap2config>enable checksum
  
  interface` Enables the router to send AppleTalk Phase 2 packets over specific interfaces.

  **Example:**

  ```ap2config>enable interface 3
  
  nfilter in` Enables network input filters and controls how the filter is applied to the interface. Inclusive forwards matches. Exclusive drops matches.

  **Example:**

  ```ap2config>enable filter in inc
  Interface # [0]?: 1
  
  nfilter out` Enables network output filters and controls how the filter is applied to the interface. Inclusive forwards matches. Exclusive drops matches.

  **Example:**

  ```ap2config>enable filter out exec
  Interface # [0]?: 1
  
  split-horizon-routing` Enables split-horizon routing on the interface. The default is `enabled`.

  **Example:**

  ```ap2config>enable split-horizon-routing 1
  
  zfilter` Enables zone filters assigned to an interface. Must specify if filter is “in” or
AppleTalk Phase 2 Configuration Commands (Talk 6)

“out” and if the filter is inclusive or exclusive. Inclusive means that only packets matching the filter will be routed. Exclusive means that all packets matching the filter will be discarded.

Example:

```
ap2config>enable zfilter in inc
Interface # [0]?
```

Example:

```
ap2config>enable zfilter out exec
Interface # [0]? 0
```

List

Use the list command to display the current AP2 configuration. In the example, the router is a seed router on interfaces 0 and 1

Note: The list command accepts an interface# as an argument.

Syntax:

```
list
```

Example:

```
ap2config>list
APL2 globally enabled
Checksumming disabled
Cache size 500
List of configured interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>netrange</th>
<th>node</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1000-1000</td>
<td>1</td>
<td>&quot;SerialLine&quot;(Def)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Input ZFilters disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Output ZFilters disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Split-horizon-routing enabled</td>
</tr>
<tr>
<td>1</td>
<td>10-19</td>
<td>52</td>
<td>&quot;EtherTalk&quot;, &quot;Sales&quot;(Def)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Input ZFilters disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Output ZFilters (inclusive)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Output NFilters disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Split-horizon-routing enabled</td>
</tr>
<tr>
<td>2</td>
<td>unseeded net</td>
<td>0</td>
<td>Split-horizon-routing disabled</td>
</tr>
</tbody>
</table>

APL2 globally
Indicates whether AppleTalk Phase 2 is globally enabled or disabled.

Checksumming
Indicates whether checksum is enabled or disabled.

Cache size
Number of fastpath cache entries.

List of configured interfaces
Lists each interface number and its network range, node number, and zone name(s) as well as the default zone.

For each interface also lists whether or not input and output zone filters and network filters and enabled or disabled. If they are enabled, indicates whether or not they are inclusive or exclusive.
Input/output Zfilters
Indicates zone filters assigned to an interface. Inclusive means that only packets matching the filter will be routed. Exclusive means that all packets matching the filter will be discarded. The name of the zone filtered is displayed. Input means that the filter is applied to traffic coming into the interface. Output means that filter is applied to traffic going out to the interface.

Input/output Nfilters
Indicates net filters assigned to an interface. Inclusive means that only packets matching the filter will be routed. Exclusive means that all packets matching the filter will be discarded. The range of networks filtered is displayed. Input means that the filter is applied to traffic coming into the interface. Output means that filter is applied to traffic going out to the interface.

Split-horizon-routing
Shows whether or not split-horizon routing is enabled or disabled on each interface.

Set
Use the set command to define the cache-size of fastpath or specific AppleTalk Phase 2 parameters, including the network range in seed routers and the node number.

Syntax:
set cache-size . .
net-range . .
node . .
cache-size value
Cache-size corresponds to the total number of AppleTalk networks and nodes that can simultaneously communicate through this router using the fastpath feature. (Fastpath is a method of precalculating MAC headers to forward packets more quickly.) The default is 500, which allows up to 500 networks and nodes to simultaneously communicate through the router and still use fastpath. If the number of networks and nodes becomes greater than the cache size, the router still forwards the packets, but it does not use fastpath. Valid values for cache size are: 0 (disable), 100 to 10 000. Although not recommended, setting the cache-size to zero disables the fastpath feature and no memory is used for the cache. You need to change this default only for very large networks. Each cache-size entry uses 36 bytes of memory.

Example:
ap2config>set cache-size 700

net-range interface# first# last#
Assigns the network range in seed routers using the following:
• interface# - Designates the router interface to operate on.
• first# - Assigns the lowest number of the network range. Legal values are 1 to 65279 (10xFEFF hexadecimal).
• last# - Sets the highest number of the network range. Legal values are first# to 65279.
AppleTalk Phase 2 Configuration Commands (Talk 6)

A single numbered network has the same first and last values. A first value of zero deletes the netrange for the interface and turn the “seeded” interface into an “unseeded” interface. First# and last# are inclusive in the network range.

Setting the first value to zero on a Point-to-Point (PPP) interface allows that interface to operate in "half-router" mode. In half-router mode, neither of the two ends of a PPP network is configured with a network range or a zone list which reduces the amount of configuration needed. Both routers on a PPP network must operate in the same mode.

Note: When connecting a 2210 to an IBM 6611 using a PPP interface, set the 2210 for “half-router” mode which is the only mode of operation supported by the IBM 6611 for AppleTalk communications over a PPP interface.

Example:
ap2config>set Net-Range 2 43 45

node interface# node#
Assigns the starting node number for the router. The router will AARP for this node but if it is already in use, a new node will be chosen. The following explains each argument that is entered after this command:
• interface# - Designates the router interface to operate on.
• node# - Designates the first attempted node number. Legal values are 1 to 253. A node# value of zero deletes the node number for the interface and forces the router to choose one at random.

Example:
ap2config>set node 2 2

Accessing the AppleTalk Phase 2 Monitoring Environment

To access the AppleTalk Phase 2 monitoring environment, enter the following command at the + (GWCON) prompt:

+ protocol ap2

AP2>

AppleTalk Phase 2 Monitoring Commands

This section describes the AppleTalk Phase 2 monitoring commands which allow you to view the parameters and statistics of the interfaces and networks that transmit AppleTalk Phase 2 packets. Monitoring commands display configuration values for the physical, frame, and packet levels. You also have the option of viewing the values for all three protocol levels at once.

Enter the AppleTalk Phase 2 monitoring commands at the AP2> prompt. Table 99 shows the commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See <a href="#">Getting Help on page xxviii</a>.</td>
</tr>
<tr>
<td>Atecho</td>
<td>Sends echo requests and watches for responses.</td>
</tr>
<tr>
<td>Cache</td>
<td>Displays the cache table entries.</td>
</tr>
</tbody>
</table>
### Atecho

The **atecho** command sends AppleTalk Echo Requests to a specified destination and watches for a response. This command can be used to verify basic AppleTalk connectivity and to isolate trouble in the AppleTalk internetwork.

**Syntax:**

```
atecho dest_net dest_node
```

- **dest_net**
  - Specifies the destination AppleTalk network number, in decimal. This is a required parameter.

- **dest_node**
  - Specifies the destination AppleTalk node number, in decimal. This is a required parameter.

**Note:** For many AppleTalk nodes, the network address (network number and node number) is dynamically assigned and might not be readily available. However, there are still a number of ways to use the **atecho** command effectively:

1. The AppleTalk address for router nodes is statically configured in many cases. Connectivity between router nodes is critical to overall network connectivity.
2. By setting the atecho destination node number to 255, you can query all nodes on the specified network number on a directly attached AppleTalk network. The received responses will indicate the node’s node number. These node numbers can then be used to echo these nodes from distant routers to verify connectivity.

- **src_net**
  - Source AppleTalk network number. This is an optional parameter. If not specified, the router uses its interface network number on the outgoing interface leading to the destination network. If the outgoing interface is an unnumbered half-router PPP interface, the router uses any one of its LAN interface network nodes.

- **src_node**
  - Source AppleTalk node number. This is an optional parameter. If not specified, the router uses its interface node number on the outgoing interface leading to the destination network. If the outgoing interface is an unnumbered half-router PPP interface, the router uses any one of its LAN interface network nodes.

- **size**
  - Number of bytes to use in the AppleTalk echo requests. This is an optional parameter. Default is 56 bytes.
AppleTalk Phase 2 Monitoring Commands (Talk 5)

rate  Rate of sending AppleTalk echo requests. This is an optional parameter. Default is one second.

Note: If you enter atecho with no parameters, you are prompted for all the parameters. Enter values for the required parameters and either enter values for the optional parameters or accept defaults.

Cache

The cache command displays information about the cache-size entries.

Syntax:
cache

Example: cache

<table>
<thead>
<tr>
<th>Destination</th>
<th>Interface</th>
<th>Usage</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>122/22</td>
<td>1</td>
<td>1</td>
<td>27/5</td>
</tr>
<tr>
<td>138/51</td>
<td>0</td>
<td>1</td>
<td>27/5</td>
</tr>
<tr>
<td>23/7</td>
<td>1</td>
<td>1</td>
<td>Direct</td>
</tr>
</tbody>
</table>

Destination  
AppleTalk node address (network number/node number).

Net  
Number of the interface used to forward to the destination node.

Usage  
Number of times this cache entry has been used in this aging period, which is five seconds. An unused entry is deleted after 10 seconds.

Next Hop  
The AppleTalk address of the next hop router used to forward a packet to the destination node, or Direct if the destination node is directly connected to the interface.

Clear Counters

The clear-counters command clears all cache usage counters and packet overflow counters.

Syntax:
clear-counters

Counters

Use the counters command to display the number of packet overflows on each network that sends and receives AppleTalk Phase 2 packets. This command displays the number of times the AppleTalk Phase 2 forwarder input queue was full when packets were received from the specified network.

Syntax:
counters

Example: counters

<table>
<thead>
<tr>
<th>Net</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>FR/0</td>
<td>0</td>
</tr>
<tr>
<td>Eth/0</td>
<td>4</td>
</tr>
<tr>
<td>PPP/0</td>
<td>22</td>
</tr>
</tbody>
</table>
Dump

Use the `dump` command to obtain routing table information about the interfaces on the router that forwards AppleTalk Phase 2 packets.

**Note:** `dump interface#` displays the part of the overall network and zone information that is visible on that interface.

**Syntax:**

`dump`

**Example:**

```
Dest Net Cost State Next hop Zone
10-19 0 Dir 0/0 "Ethertalk", "Sales"
40-49 1 Good 10/13 "Marketing", "CustomerSer", "TokenTalk"
20-29 2 Sspct 10/13 "Fuchsia", "Backbone", "Engineering", "MKTING"  
3 entries
```

You can also use the `dump` command with a specific interface to display the routes that are visible on that interface. You can use this feature to make sure filters are configured correctly because it shows whether or not filtered zones or networks are visible to an interface.

**Example:**

```
dump 0
```

```
View for interface 0

Dest net Cost State Next hop Zone
214-214 1 Good 152/152 "eth-214"
153-153 0 Dir "eth153"
152-152 0 Dir "ser152"
3 entries
```

**Dest Net**  
Specifies the destination network number, in decimal.

**Cost**  
Specifies the number of router hops to this destination network.

**State**  
Specifies the state of the entry in the routing table. It includes the following:

- *Next hop*  
  Specifies the next hop for packets going to networks that are not directly connected. For directly-connected networks, this is node number 0.

- *Zones*  
  Specifies the human-understandable name for that network. The zone names are enclosed in double quotes in case there are embedded spaces or non-printing characters. If the zone name contains characters beyond the 7-bit ASCII character set (they are 8-bit), the zone name that displays will depend on the characteristics of your monitoring terminal.

Interface

Use the `interface` command to display the addresses of all the interfaces in the router on which AppleTalk Phase 2 is enabled. If the interface is present in the router but is disabled, this command shows that status.

**Note:** `interface interface#` displays the active filtering for that interface. It displays net, node, default zone, and active filters for one interface.

**Syntax:**

Chapter 5. Configuring and Monitoring AppleTalk Phase 2  295
AppleTalk Phase 2 Monitoring Commands (Talk 5)

interface

Example: interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Addresses</th>
<th>Default Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP/0</td>
<td>0/1 on net 1000-1000</td>
<td>&quot;Serial Line&quot;</td>
</tr>
<tr>
<td>Eth/0</td>
<td>10/52 on net 10-19</td>
<td>&quot;Sales&quot;</td>
</tr>
<tr>
<td>PPP/1</td>
<td>0/0 in startup range</td>
<td></td>
</tr>
<tr>
<td>TKR/0</td>
<td>0/0 on net 20-29</td>
<td>&quot;Backbone&quot;</td>
</tr>
</tbody>
</table>

You can also enter the interface command followed by a specific interface number to view the AP2 configuration of that interface.

Example: interface 1

Eth/0 1/30 on net 1-5 default zone "marketing"

Input Net filters inclusive 1-5
Output Zone filters inclusive "finance"
Output Net filters exclusive 1-5
Chapter 6. Using VINES

This chapter describes the commands to configure the Banyan VINES protocol and includes the following sections:

- “VINES Overview”
- “VINES Network Layer Protocols” on page 298
- “Basic Configuration Procedures” on page 303
- “Accessing the VINES Configuration Environment” on page 305
- “Running Banyan VINES on the Bridging Router” on page 303
- “VINES Configuration Commands” on page 305.

Note: If you need more detailed information on VINES Protocols, consult the Banyan publication: VINES Protocol Definition, order number: 003673

VINES Overview

VINES Over Router Protocols and Interfaces

The VINES protocol routes VINES packets over the following interfaces and protocols:

- PPP Banyan Vines Control Protocol (PPP BVCP)
- Frame Relay
- Ethernet/802.3
- 802.5 Token Ring
- X.25
- Ethernet ATM LAN Emulation Client
- Token-Ring ATM LAN Emulation Client

It also supports packets across an 802.5 Source Routing Bridge (SRB).

The VINES protocol is implemented at the network layer (Layer 3) of the OSI model. VINES routes packets from the transport layer in one node to the transport layer in another node. As VINES routes the packets to their destination nodes, the packets pass through the network layers of the intermediate nodes where they are checked for bit errors. A VINES IP packet can contain up to 1500 bytes including the network layer header and all higher layer protocol headers and data.

Service and Client Nodes

The VINES network consists of service nodes and client nodes. A service node provides address resolution and routing services to the client nodes. A client node is a physical neighbor on the VINES network. All routers are service nodes. A Banyan node can be a service node or client node.

Each service node has a 32-bit network address and a 16-bit subnetwork address. The IBM 2210 has a configurable network address. This address identifies the router as a service network node for Vines. Banyan has assigned the range 30800000 to 309FFFFF to IBM for use in its routers. This router uses the range 30900000 to 3097FFFF.

Note: It is extremely important that no two routers be assigned the same network address. The network address for a Banyan service node is the 32-bit hexadecimal serial number of the service node. The subnetwork address for all service nodes is 1.
Using VINES

The network address for each client node is generally the network address of the service node on the same network. However, if a client node is on a LAN that has more than one service node, it is assigned the network address of the service node that responds first to the client node’s address assignment request. The subnetwork address for each client node is a hexadecimal value of 8000 to FFFE.

VINES Network Layer Protocols

This implementation of VINES consists of the following four network layer protocols. The next sections describe these protocols and their implementations.

- "VINES Internet Protocol (VINES IP)". Routes packets through the network.
- "Routing Update Protocol (RTP)" on page 299. Distributes topological information to support the routing services provided by VINES IP.
- "Internet Control Protocol (ICP)" on page 302. Provides diagnostics and support functions to certain transport layer protocol entities, such as providing notification on some network errors and topological conditions.
- "VINES Address Resolution Protocol (VINES ARP)" on page 302. Assigns VINES internet addresses to client nodes that do not already have addresses.

VINES Internet Protocol (VINES IP)

The VINES IP protocol routes packets through the network using the destination network number in the VINES IP header. VINES IP consists of an 18-byte network layer header which prefixes each packet. Table 100 summarizes the fields within this header.

VINES IP Implementation

When VINES IP receives a packet, it checks the packet for size and exception errors. A size error is a packet that is less than 18 bytes or greater than 1500 bytes. If it contains a size error, VINES IP discards the packet. An exception error is, for example, a bad checksum or a hop count that has expired.

If the packet does not contain size or exception errors, VINES IP checks the destination address and forwards the packet as follows:

- If the destination address equals the local VINES IP address and the checksum is valid, the local node accepts the packet.
- If the destination address equals the broadcast address and the checksum is valid, VINES IP accepts the packet, processes it locally, and checks the hop count field of the IP header. If the hop count is greater than 0, VINES IP decrements the hop count by one and rebroadcasts the packet on all local media except the one on which the packet was received.
- If the destination address does not equal the local VINES IP address or the broadcast address, VINES IP checks its routing tables for the next hop. If the hop count equals 0, VINES IP discards the packet. Otherwise, it decrements the hop count by one and forwards the packet to the next hop.

If the destination VINES IP address is not in the routing table and the error bit in the transport control field is set, VINES IP drops the packet and returns an ICP Destination Unreachable message to the source. If the error bit in the transport control field is not set, VINES IP discards the packet and does not return a message to the source.

Table 100. Vines IP Header Fields Summary

<table>
<thead>
<tr>
<th>VINES IP Header Field</th>
<th># of Bytes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checksum</td>
<td>2</td>
<td>Detects bit-error corruption of a packet.</td>
</tr>
</tbody>
</table>
Table 100. Vines IP Header Fields Summary (continued)

<table>
<thead>
<tr>
<th>VINES IP Header Field</th>
<th># of Bytes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Length</td>
<td>2</td>
<td>Indicates the number of bytes in the packet including the VINES IP header and data.</td>
</tr>
<tr>
<td>Transport Control</td>
<td>1</td>
<td>Consists of the following five subfields:</td>
</tr>
<tr>
<td>Class</td>
<td></td>
<td>Determines the type of nodes to which VINES IP broadcast packets are sent.</td>
</tr>
<tr>
<td>Error</td>
<td></td>
<td>If the error bit is set, an exception notification packet is sent to the transport layer protocol entity when a packet cannot be routed to a service or client node.</td>
</tr>
<tr>
<td>Metric</td>
<td></td>
<td>Requests that the service node of the destination client node return to the source a routing cost from the service node to the destination client node.</td>
</tr>
<tr>
<td>Redirect</td>
<td></td>
<td>Indicates whether the packet contains an RTP message specifying a better route to use.</td>
</tr>
<tr>
<td>Hop Count</td>
<td></td>
<td>Specifies the range a packet can travel. The hop count can range from 0x0 to 0xf.</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>1</td>
<td>Specifies the VINES network layer protocol of the packet as VINES IP, RTP, ICP, or VINES ARP.</td>
</tr>
<tr>
<td>Destination Network Number</td>
<td>4</td>
<td>A 4-byte network number in the VINES IP address of the destination.</td>
</tr>
<tr>
<td>Destination Subnetwork Number</td>
<td>2</td>
<td>A 2-byte subnetwork number in the VINES IP address of the destination.</td>
</tr>
<tr>
<td>Source Network Number</td>
<td>4</td>
<td>A 4-byte network number in the VINES IP address of the source.</td>
</tr>
<tr>
<td>Source Subnetwork Number</td>
<td>2</td>
<td>A 2-byte subnetwork number in the VINES IP address of the source.</td>
</tr>
</tbody>
</table>

Routing Update Protocol (RTP)

RTP gathers and distributes routing information that VINES IP uses to compute routes throughout the network. RTP enables each router to periodically broadcast routing tables to all of its neighbors. The router then determines the destination neighbor it will use to route the packet.

Service nodes maintain two tables: a routing table and a neighbor table. Both of these tables have timers that age their contents to eliminate out-of-date entries. Routing updates for X.25 interfaces occur when there is a change in the routing database, for example, when a node goes up/down or the metric changes.

Routing Table

The routing table contains information about the service nodes. Figure 13 on page 300 shows a sample routing table. Descriptions of the fields in this table follow the figure.
Using VINES

<table>
<thead>
<tr>
<th>Net Address</th>
<th>Next Hop Nbr Addr</th>
<th>Nbr Intf</th>
<th>Metric</th>
<th>Age (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S 30622222</td>
<td>30622222:0001</td>
<td>Eth/0</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>H 0027AA21</td>
<td>0027AA21:0001</td>
<td>Eth/1</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>P 0034CC11</td>
<td>0034CC11:0001</td>
<td>X.25/0</td>
<td>45</td>
<td>0</td>
</tr>
</tbody>
</table>

3 Total Routes

S \( \Rightarrow \) Entry is suspended,  
H \( \Rightarrow \) Entry is in Hold-down,  
P \( \Rightarrow \) Entry is permanent

Figure 13. Sample Routing Table

Routing Table Field Description

**Net Address**  
The Net Address is a unique 32-bit number. An S, H, or P preceding the Net Address field indicates the following:

- **S** Indicates the service node is in suspended state and is advertised, for 90 seconds, as being down. After 90 seconds, the router removes the entry for this service node from the routing table.
- **H** Indicates the service node is in hold-down state and is advertised, for 2 minutes, as being down. After 2 minutes, the router advertises the service node as operational. If a service node is in suspended state and it receives an RTP packet, the service node enters the hold-down state.
- **P** Indicates that the X.25 interface enters permanent state for 4-1/2 minutes after initialization. After 4-1/2 minutes, the neighbor enters the permanent state and its age stays at 0 while in this state. If the X.25 interface goes down, the entry is removed from the routing table.

**Next Hop Nbr Addr**  
The address of the neighbor service node that is the next hop on the least-cost path to the network.

**Nbr Intf**  
The medium to which the next hop neighbor service node is attached.

**Metric**  
An estimated cost, in 200-millisecond increments, to route the VINES packet to the destination service node.

**Age (secs)**  
The current age, in seconds, for the entry. If a router does not receive an update about a service node that is in the routing table at least every 360 seconds (6 minutes), the router removes the entry for that service node from the routing table.

**Neighbor Tables**  
The neighbor table contains information about the neighbor service nodes and client nodes connected to the router. Figure 14 on page 301 shows a sample neighbor table and descriptions of the fields in this table follow the figure.
Neighbor Table Field

**Nbr Address**
The address of the neighbor node. In Figure 14, the address 30633333:0001 is a service node and address 0035CC10:8000 is a client node.

**Intf**
The medium to which the neighbor node is attached.

**Metric**
An estimated cost, in 200-millisecond increments, to route the VINES packet to the neighbor node.

**Age (secs)**
The current age, in seconds, for the entry. If a router does not receive a routing update from a neighbor at least every 360 seconds (6 minutes), the router removes the entry for that neighbor from the neighbor table and, if the neighbor is a service node, from the routing table.

**H/W Addr**
The node’s LAN address if the neighbor is connected to a LAN. If the Frame Relay protocol is running, the H/W Addr is the Data Link Connection Identifier (DLCI). For X.25 interfaces, the H/W Addr is the X.25 address of the neighbor.

**RIF**
Routing Information Field. A sequence of segment and bridge numbers, in hexadecimal, which indicate a path through the network between two stations. RIF is required for source routing.

RTP Implementation
RTP entities issue the following packets:

- **RTP request packets.** Requests to the service nodes to obtain the current network topology. On initialization, an X.25 interface generates routing request packets every 90 seconds to each X.25 destination on the X.25 interface. When the X.25 interface receives a routing response packet, three full routing database updates, spaced 90 seconds apart, are sent to the services nodes that sent the routing response packets. Once the X.25 interface receives routing response packets from all of the X.25 destination nodes, routing requests are no longer sent to those X.25 addresses.

- **RTP update packets.** Packets sent by client nodes to the service nodes to notify the service nodes of their existence. RTP update packets are also sent by the service nodes to notify other nodes of their existence and to advertise their routing databases.

- **RTP response packets.** Packets service nodes send in response to RTP request packets.

- **RTP redirect packets.** Informs the nodes of the best paths between them for routing packets.

<table>
<thead>
<tr>
<th>Nbr Address</th>
<th>Intf</th>
<th>Metric</th>
<th>Age(secs)</th>
<th>H/W Addr</th>
<th>RIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>30633333:0001</td>
<td>TKR/0</td>
<td>4</td>
<td>30</td>
<td>0000C0095012</td>
<td></td>
</tr>
<tr>
<td>0035CC10:8000</td>
<td>Eth/1</td>
<td>2</td>
<td>120</td>
<td>0000C0078221</td>
<td></td>
</tr>
</tbody>
</table>

2 Total Neighbors

Figure 14. Sample Neighbor Table
Using VINES

Unless connected by a permanent circuit, every client and service node broadcasts an RTP update every 90 seconds. This notifies the neighbors of the node’s existence and its type (service or client node) and, in the case of service nodes, advertises their routing databases. When a router receives an update packet from a service node, RTP extracts the VINES IP address and looks in the routing table for an existing entry on that service node. If it exists, RTP updates the entry and resets the entry’s timer. If an entry does not exist, RTP creates one and initializes the timer for that entry.

Internet Control Protocol (ICP)

ICP generates network information messages on two types of packets destined for the local router:
- Destination unreachable packet. Indicates a packet could not reach its destination and was returned to its source. The router then issues an ELS message and flushes the packet.
- Delay metric packet. A request packet from a source node for the routing metric from the destination service node to the destination client node.

VINES Address Resolution Protocol (VINES ARP)

The VINES ARP protocol assigns unique VINES IP addresses to the client nodes. VINES ARP includes the following packet types:
- Query request packet. Packets the client nodes broadcast on initialization.
- Query response packet. The service node’s response to a query request packet.
- Assignment request packet. The client node’s response to a query response packet.
- Assignment response packet. Includes the network and subnet addresses the service node assigned to a client node.

To assign a VINES IP address to a client node, VINES ARP implements the following algorithm:
1. The client node broadcasts a query request packet.
2. Service nodes respond with a query response packet containing the destination MAC address of the client node and a broadcast VINES IP address.
3. The client node issues an assignment request packet to a service node that responded with a query response packet.
4. The service node responds with an assignment response packet that contains the VINES network and subnetwork addresses.

Each client node maintains a timer that has a default setting of two seconds. The timer starts when a client node transmits a query request or assignment request packet. The client node stops and resets the timer when it receives a query response packet. When a timeout period exceeds two seconds, the client node initializes, broadcasts a query request packet, and resets the timer. Table 101 summarizes the states the service and client nodes enter during VINES ARP implementation.

<table>
<thead>
<tr>
<th>Table 101. Client and Service Node VINES ARP States</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Node States</strong></td>
</tr>
<tr>
<td>Initialization</td>
</tr>
<tr>
<td>Query</td>
</tr>
</tbody>
</table>
Table 101. Client and Service Node VINES ARP States (continued)

<table>
<thead>
<tr>
<th>Request</th>
<th>The client node received a query response packet from a service node and is transmitting an assignment request packet to the service node it heard from.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned</td>
<td>The client node received an assignment response packet containing the VINES network and subnetwork addresses.</td>
</tr>
</tbody>
</table>

Service Node States

<table>
<thead>
<tr>
<th>Initialization</th>
<th>The VINES ARP protocol is initializing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen</td>
<td>The service node is waiting for query request packets from the client nodes.</td>
</tr>
<tr>
<td>Service</td>
<td>The service node received a query request packet and sent a query response packet.</td>
</tr>
<tr>
<td>Assignment</td>
<td>The service node issues an assignment response packet containing the VINES network and subnetwork addresses.</td>
</tr>
</tbody>
</table>

Basic Configuration Procedures

The steps to initially configure each router that sends and receives VINES packets are as follow:

1. Assign a unique 32-bit hexadecimal address to each router in the VINES network. Using the set network-address hex # command, enter a network address from 30900000 to 3097FFFF. The network address for Banyan servers is the 32-bit hexadecimal serial number of the service node. This number is automatically read from the node server key.

2. Globally enable the VINES protocol using the enable VINES command.

3. Enable the interface cards that are to transmit and receive the VINES packets using the enable interface interface# command.

For configuration changes to take effect you must restart the router. Enter restart or reload after the OPCON prompt (*) and answer yes to the following prompt:

Are you sure you want to restart (or reload) the router? (Yes or No): yes

To view the configuration, enter the list command after the VINES config> prompt.

Running Banyan VINES on the Bridging Router

Banyan VINES servers must have this Banyan option to communicate with other servers or routers:

- Server-to-server LAN.

To communicate across X.25 WANs, VINES servers directly connected to the WAN need these two options:

- Server-to-server WAN
- X.25 support on the server (hardware and software).

Running Banyan VINES over WAN Links

When you set up a PPP, Frame Relay, or X.25 link for use with VINES, you must set the HDLC speed of the link, even if you set the clocking to external.

If you set the HDLC speed to zero, VINES assumes that the speed is 56 kbps. Do not set the speed to a value that is faster than the line.
Chapter 7. Configuring and Monitoring VINES

This chapter describes the VINES configuring and monitoring commands and includes the following sections:

- "Accessing the VINES Monitoring Environment" on page 308
- "VINES Monitoring Commands" on page 309

Accessing the VINES Configuration Environment

To access the VINES configuration environment, enter the following command at the Config> prompt:

```
Config> protocol vin
VINES Protocol user configuration
VINES Config>
```

VINES Configuration Commands

This section summarizes and then explains the VINES configuration commands. Enter these commands at the VINES config> prompt.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxviii.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds an X.25 address translation.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes an X.25 address translation.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables the VINES protocol on all interfaces or a single interface and disables checksumming.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables the VINES protocol on all interfaces or a single interface and enables checksumming.</td>
</tr>
<tr>
<td>List</td>
<td>Displays the current VINES configuration.</td>
</tr>
<tr>
<td>Set</td>
<td>Assigns the network addresses to routers in the VINES network and sets the maximum number of physical neighbor client and service nodes.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxviii.</td>
</tr>
</tbody>
</table>

Add

Adds an X.25 address translation.

**Syntax:**

```
add
_add
#  Specifies the interface number.
remote-X.25-addr
 Handles can include up to 15 digits. If the virtual circuit connection has been configured as PVC, the VINES remote-X.25-addr must match the PVC address configured at the X.25 prompt. If the addresses do not match, the system defaults to a switched virtual circuit (SVC).
handle
     user-configurable name that uniquely identifies each remote server.
```

**Example:** `add interface 0 4508907898 test`
VINES Configuration Commands (Talk 6)

Delete

Deletes an X.25 address translation.

Syntax:
```
delete
```
```bash
interface ...
```

# Specifies the interface number.

```
remote-X.25-addr
```
Can include up to 15 digits. If the specified interface has not been configured using the VINES add interface command, the terminal displays the message That X.25 address has not been configured.

Example: delete interface 1 4799999999 compress

Disable

Use the disable command to disable the VINES protocol on all interfaces or a single interface, or to disable checksumming.

Syntax:
```
disable
```
```bash
checksuming ...
interface ...
```
```
vines
```

```
checksuming interface#
```
Disables checksumming on packets that the specified interface generates, broadcast packets excluded. For all interfaces, the default is checksumming disabled.

Example: disable checksuming 0

```
interface interface#
```
Disables the VINES protocol on the specified interface.

Example: disable interface 1

```
vines
```
Disables the VINES protocol on all interfaces.

Example: disable vines

Enable

Use the enable command to enable the VINES protocol on all interfaces or a single interface, or to enable checksumming.

Syntax:
```
enable
```
```bash
checksuming ...
interface ...
```
```
vines
```

```
checksuming interface#
```
Enables checksumming on packets that the specified interface generates.

Example: enable checksuming 0

```
interface interface#
```
Enables the VINES protocol on the specified interface.

Example: enable interface 1

```
vines
```
Globally enables the VINES protocol. If you receive an error message after...
entering this command, contact your customer service representative. The VINES software may not be in your software load.

**Example:** `enable vines`

**List**

Use the `list` command to display the current VINES configuration.

**Syntax:**

`list`

**Example:** `list`

```
VINIES:  enabled/disabled
VINIES network number (hex):
Maximum Number of Routing Table Entries:
Maximum Number of Neighbor Service Nodes:
Maximum Number of Neighbor Client Nodes:

List of interfaces configured for VINIES:

  intf 0  (checksumming enabled/disabled)
  intf 1  (checksumming enabled/disabled)
  intf 2  (checksumming enabled/disabled)

VINIES X.25 Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Remote X.25 Address</th>
<th>Remote Handle</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>450807898</td>
<td>test</td>
</tr>
</tbody>
</table>

VINIES config>```

**VINIES** Indicates whether VINES is globally enabled or disabled.

**VINIES network number (hex)**

A configurable 32-bit hexadecimal address for routers in the VINES network.

**Maximum Number of Routing Table entries**

A configured value specifying the maximum number of entries allowed in the VINES routing table.

**Maximum Number of Neighbor Service Nodes**

A configured value specifying the maximum number of neighbor service nodes connected to the router.

**Maximum Number of Neighbor Client Nodes**

A configured value specifying the maximum number of client nodes connected to the router.

**List of interfaces configured for VINES**

Displays the interfaces that have VINES enabled and whether checksumming is enabled or disabled.

**VINIES X.25 Configuration**

This information represents the following:

**Interface**

The interface that is configured for X.25.

**Remote X.25 Address**

The DTE address of the remote server.

**Remote Handle**

A user-configurable name that uniquely identifies the remote server.
 VINES Configuration Commands (Talk 6)

Set

Use the `set` command to assign network addresses to routers in the VINES network and to specify the maximum number of client and service nodes.

**Syntax:**
```
set
  client-node-neighbors ...  
  network-address ...  
  routing-table-size ...  
  service-node-neighbors ... 
```

`client-node-neighbors #`
- Specifies the maximum number of client nodes on your network. `client-node-neighbors` includes all of the nodes on each network directly connected through the router. The range is 1 to 65535, and the default is 25.

**Note:** It is recommended that you set this number significantly higher than the number of nodes in your network. This will enable your network to continue functioning without reconfiguring and restarting the routers when additional nodes are added. The increase in this number depends on the size of your network and the amount of anticipated growth. As a rule, set `client-node-neighbors` 25% higher than the actual number of client stations on LANs that are local to the router.

**Example:** `set client-node-neighbors 20`

`network-address hex#`
- Assigns a network address to each router in the VINES network. *Hex#* is a 32-bit hexadecimal value from 30900000 to 3097FFFF.

**Example:** `set network-address 30922222`

`routing-table-size #`
- Specifies the maximum number of service nodes and routers in the VINES network. The range is 1 to 65535, and the default is 300.

**Note:** Make sure that the number you specify is large enough to accommodate additional VINES servers and 2210s as your network grows.

**Example:** `set routing-table-size 250`

`service-node-neighbors #`
- Specifies the maximum number of physical neighbor service nodes. This number includes VINES servers and 2210s that are the first point-of-contact after crossing a WAN. The range is 1 to 65535, and the default is 50.

**Example:** `set service-node-neighbors 100`

Accessing the VINES Monitoring Environment

To access the VINES monitoring environment, enter:
```
* t 5
```

Then, enter the following command at the `+` prompt:
```
+ protocol vin
VINES>
```
VINES Monitoring Commands

This section describes the VINES monitoring commands. Enter these commands at the VINES> prompt.

Table 103. VINES Monitoring Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxviii.</td>
</tr>
<tr>
<td>Counters</td>
<td>Displays routing errors and the number of times the VINES input queue was full when packets were received from the specified interface.</td>
</tr>
<tr>
<td>Dump</td>
<td>Displays the current contents of the VINES routing and neighbor tables.</td>
</tr>
<tr>
<td>Route</td>
<td>Displays an entry from the VINES routing table.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxviii.</td>
</tr>
</tbody>
</table>

Counters

Use the counters command to display routing errors and the number of times the VINES input queue was full when packets were received from the specified interface.

Syntax:

counters

Example: counters

Routing Errors

<table>
<thead>
<tr>
<th>Count</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>Net Unreachable</td>
</tr>
<tr>
<td>3</td>
<td>Hop Count Expired</td>
</tr>
<tr>
<td>3</td>
<td>Routing Update from Orphan Client</td>
</tr>
<tr>
<td>0</td>
<td>Routing Redirect Received</td>
</tr>
<tr>
<td>0</td>
<td>Routing Response Received</td>
</tr>
</tbody>
</table>

VINES Input Packet Overflows

<table>
<thead>
<tr>
<th>Net</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth/0</td>
<td>5</td>
</tr>
<tr>
<td>Eth/1</td>
<td>1</td>
</tr>
</tbody>
</table>

Net Unreachable

The number of times the router received a packet destined for a node that was not found in the routing table.

Hop Count Expired

The number of times the router discarded a packet because its hop count expired.

Routing Update from Orphan Client

The number of times the router received an update packet from a client node whose service node does not exist. A routing update from an orphan client can occur when the router boots and hears from the client node first rather than the service node, or when a client’s service node is down and an entry has been removed from the routing table database.

Routing Redirect Received

The number of times the router received redirect packets from the service nodes.
VINES Monitoring Commands (Talk 5)

Routing Response Received
The number of times response packets were generated as a result of request packets initiated by the router.

VINES input packet overflows
The number of times the VINES forwarder input queue was full when packets were received from the specified interface. The packets are subsequently discarded.

Dump

Use the `dump` command to display the contents of the VINES routing and neighbor tables.

Syntax:
```
dump neighbor-tables
```
```
dump routing-tables
```

neighbor-tables
Displays information about each neighbor service and client node connected to the router.

Example: `dump neighbor-tables`

<table>
<thead>
<tr>
<th>Nbr Address</th>
<th>Intf</th>
<th>Metric</th>
<th>Age(secs)</th>
<th>H/W Addr</th>
<th>RIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>30622222:0001</td>
<td>TKR/0</td>
<td>4</td>
<td>30</td>
<td>0000C00</td>
<td>95012</td>
</tr>
<tr>
<td>0035CC10:8000</td>
<td>Eth/0</td>
<td>2</td>
<td>120</td>
<td>0000C00</td>
<td>76221</td>
</tr>
</tbody>
</table>

2 Total Neighbors

Nbr Address
The address of the neighbor node. In the above example, address 30622222:0001 is a service node and address 0035CC10:8000 is a client node.

Intf
The medium to which the neighbor node is attached.

Metric
An estimated cost, in 200-milliseconds, to route the VINES packet to the neighbor node.

Age (secs)
The current age, in seconds, for the entry. If a router does not receive a routing update from a neighbor at least every 360 seconds (6 minutes), the router removes the entry for that neighbor from the neighbor table and, if the neighbor is a service node, from the routing table.

H/W Addr
The node’s LAN address if the neighbor is connected to a LAN. If the Frame Relay protocol is running, the H/W Addr is the Data Link Connection Identifier (DLCI). For X.25 interfaces, the H/W Addr is the X.25 address of the neighbor.

RIF
Routing Information Field. A sequence of segment and bridge numbers, in hexadecimal, which indicate a path through the network between two stations. RIF is required for source routing.

routing-tables
Displays information about each service node known by the router.

Example: `dump routing-table`

<table>
<thead>
<tr>
<th>Net Address</th>
<th>Next Hop Nbr Addr</th>
<th>Nbr Intf</th>
<th>Metric</th>
<th>Age (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S 30622222</td>
<td>30622222:0001</td>
<td>Eth/0</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>H 0027AA21</td>
<td>0027AA21:0001</td>
<td>Eth/1</td>
<td>2</td>
<td>120</td>
</tr>
</tbody>
</table>
Net Address

The Net Address is a unique, configurable 32-bit hexadecimal value from 30900000 to 3097FFFF. This range of numbers is assigned to IBM by Banyan. It is very important that no two routers on a network are assigned the same Net Address. The Net Address for a Banyan service node is the 32-bit hexadecimal serial number of the service node. An S, H, or P preceding the Net Address field indicates the following:

S: The service node is in suspended state and is advertised, for 90 seconds, as being down. After 90 seconds, the router removes the entry for this service node from the routing table.

H: The service node is in hold-down state and is advertised, for 2 minutes, as being down. After 2 minutes, the router advertises the service node as operational. If a service node is in suspended state and it receives an RTP packet, the service node enters the hold-down state.

P: After initialization, the X.25 interface enters permanent state for 4 1/2 minutes. After 4 1/2 minutes, the neighbor enters the permanent state and its age stays at 0 while in this state. If the X.25 interface goes down, the entry is removed from the routing table.

Next Hop Nbr Addr

The address of the neighbor service node that is the next hop on the least-cost path to the network.

Nbr Intf

The medium to which the next hop neighbor service node is attached.

Metric

An estimated cost, in 200-milliseconds, to route the VINES packet to the destination service node.

Age (secs)

The current age, in seconds, for the entry. If a router does not receive a routing update about a service node that is in the routing table at least every 360 seconds (6 minutes), the router removes the entry for that service node from the routing table.

Route

Use the route command to view an entry from the routing table.

Syntax:

```
route given address
```

given address

The network address of the service node.

Example: route 30622222
### VINES Monitoring Commands (Talk 5)

<table>
<thead>
<tr>
<th>Net Address</th>
<th>Next Hop Nbr Addr</th>
<th>Nbr Intf</th>
<th>Metric</th>
<th>Age (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30622222</td>
<td>30622222:0001</td>
<td>Eth/0</td>
<td>2</td>
<td>30</td>
</tr>
</tbody>
</table>
Chapter 8. Using DNA IV

This chapter describes IBM's implementation of Digital Network Architecture Phase IV (DNA IV) and includes the following sections:

- "DNA IV Overview"
- "IBM's Implementation of DNA IV" on page 316
- "Configuring DNA IV" on page 325
- "DNA IV Configuration and Monitoring Commands" on page 329

DNA IV Overview

DNA IV is a collection of software components that transfer information between networks connected by physical media. By transferring information, DNA IV software facilitates communication between network devices, such as personal computers, file servers, and printers.

DNA IV protocol is the underlying protocol for Digital Equipment Corporation’s DECnet software products as well as DNA-compatible products. DNA IV protocol includes the following:

- Routing software for DNA IV protocol networks.
- NCP, an implementation of the DNA IV Network Control Program. For more information, refer to the appropriate DECnet-VAX documentation, published by Digital Equipment Corporation.

DNA IV performs two major functions:

- Maintains a complete routing database on all nodes in its area. (If the router is operating as a level 2 router, it maintains the database for all areas as well.)
- Routes incoming DECnet data packets to the appropriate destinations based on its own routing database. It ignores packets that are addressed to the router that are not hello packets or routing packets.

DNA IV supports the following:

- Multiple areas on an Ethernet or Token-Ring network.
- Basic MOP operations. DNA IV responds to a MOP Request ID message with a MOP System ID message. DNA IV also sends a MOP system ID Message when a circuit comes up. You can monitor MOP messages using the Ethernet configuration module under DECnet-VAX NCP. The router NCP does not include an Ethernet configuration module.
- LAT Protocol. LAT protocol is not part of the DNA IV protocol family. It is an Ethernet-only protocol intended only for short-distance (limited round-trip time) communications. (CTERM protocol provides wide-area terminal support using DNA IV protocols across routers. The set host command in DECnet-VAX provides the CTERM protocol.)

Special consideration should be given to the following DNA IV restrictions:

- DNA IV does not support the NSP, Session, or NICE protocols.
- DNA IV does not support the DDCMP line protocol on its directly connected synchronous lines.
- DNA IV does not provide any Phase III compatibility features because it does not support the DDCMP data link protocols used by all Phase III nodes.
Using DNA IV

- NCP (the router’s implementation of the DECnet Network Control Program) implements a subset of the original NCP commands and functions.

DNA IV Terminology and Concepts

This section contains a brief description of DNA IV terminology.

Addressing

Each node has a 16-bit node address, which is the same for all interfaces on that node. An address consists of 2 fields: 6 bits of area number and 10 bits of node number. Addresses are printed in decimal with a period separating the area and the node, such as 1.7 is node 7 in area 1. If no area is given, area 1 is assumed. Any address in the range 1.1 to 63.1023 is legal. Both nodes and areas should be numbered starting from 1, with few, if any, gaps. This is because the maximum node number and the maximum area numbers are configuration options and control the size of many of the routing data structures.

There is no direct correlation between addresses and physical cabling. Routes are computed to nodes, not wires.

Ethernet Data Link Addressing

Each Ethernet interface is set to the same 48-bit physical address, which is the concatenation of a 32-bit prefix (AA-00-04-00) and the 16-bit DNA IV node address. The node address is byte-swapped (to convert from PDP11 to Ethernet byte order). Thus, DNA IV node 1.1 has Ethernet Address AA-00-04-00-01-04.

Multicast (not broadcast) is also used in routing. The three multicast addresses used by DNA IV are AB-00-00-02-00-00, AB-00-00-03-00-00, and AB-00-00-04-00-00.

802.5 Token-Ring Data Link Addressing

The implementation of DNA over IEEE 802.5 Token Ring conforms to the DECnet Digital Networking Architecture (Phase IV) Token-Ring Data Link and Node Product Functional Specification, Version 1.0.0, that includes support for Arbitrary MAC Addresses (AMA).

There are two types of MAC addressing, conventional DNA IV addressing, which is the concatenation of a 32-bit prefix (AA-00-04-00) and the 16-bit DNA IV area/node address or AMA that allows the DNA protocol to run on IEEE 802.5 nodes without their MAC addresses being changed by the DNA protocol. This is necessary if you follow certain IBM protocol conventions. You can select the type of addressing that you are using through the DNA configuration process (NCP>).

Another type of addressing representation is native bit-order. This type of address is byte-flopped when sent over the physical layer. For example, the canonical 32-bit prefix shown above (using dashes) is expressed as 55:00:20:00 in native bit-order with colons separating each byte.

Note: When configuring DNA IV to run over ATM LAN Emulation, the AMA must be used.

X.25 Data Link Addressing

The router supports DECnet Phase IV over X.25 and can interoperate with routers running Digital’s implementation of DECnet Phase IV over X.25.

You set up the local and the remote DTE address with the set/define circuit command when you set up a DECnet circuit. In the call-userdata parameter you
specify the local DTE address in hexadecimal octets (characters). In the
*DTE-address* parameter you specify the remote address in hexadecimal octets.
Both the local and remote DTE addresses can be up to 14 hexadecimal octets in
length with two ASCII characters representing one hexadecimal octet.

### Routing

DNA IV handles both forwarding of DNA IV data packets and automatic routing with
other DNA IV nodes. The router performs the following DNA IV functions:
- Announces its presence by sending hello messages on each network that has
  DNA IV enabled.
- Maintains a list of adjacent DNA IV nodes from the hello packets it receives from
  other DNA IV nodes.
- Exchanges routing information with other routers.
- Forwards packets between nodes.

All end and routing nodes periodically broadcast hello messages to the all-routers
multicast address. This allows each router to locate other nodes in its area.

On each broadcast network (for example, Ethernet, Token-Ring), one router
declares itself the designated router for that wire. The designated router broadcasts
its presence so that the end-nodes know to use it as their default gateway. Any
end-node sending a packet to a node not on that wire automatically sends it to the
designated router for forwarding.

In a multi-area DNA, assign priorities to routers in such a way that the designated
router is a level 2 router, or is likely to be the best next hop to commonly-used
destinations. This reduces the possibility of traffic from end-nodes having to take an
extra hop.

Routing decisions are based on a least-cost algorithm. Each link (e.g.,
point-to-point, broadcast network, hop) has a cost. Every router broadcasts (to other
routers only) its cost and the number of hops to get to every node in its area. In this
way, each router finds the cheapest path, subject to a maximum hop count.

### Routing Tables

A router forwards any DNA IV data packet it receives to the proper node based on
its routing table. To maintain its routing table, a router listens to and sends level 1
updates to every node in its area. If the router’s type is set to AREA, it also
exchanges level 2 routing updates.

Each router maintains a routing table with an entry for every node (up to the
maximum address) and every possible next hop (all circuits and up to the maximum
broadcast routers). Each entry in this table contains the cost and hop to reach a
node via one circuit or next hop node. Once a second the routing table sends out a
broadcast routing timer.

### Area Routers

If the router is configured as an area router, it maintains a similar database for all of
the areas up to the maximum area, and can exchange area routing information with
other area routers. Areas are handled almost exactly the same as nodes, except
messages give costs to areas, but not nodes.

The areas concept results in two types of routing nodes:
Using DNA IV

- A level 1 router only knows about one area, so it keeps track of nodes in its area. Also, it ignores adjacencies across areas.
- A level 2 router keeps an area routing database, and can have cross-area adjacencies. Level 2 routers advertise routes to all other areas, so level 1 routers send all foreign-area traffic to the level 2 routers.

End-nodes simply pass packets on to a router.

A level 2 router that can reach other areas advertises a route to node 0 within its area. When level 1 routers need to send a packet to another area, they route it toward the closest node 0. This is not necessarily the best route to that area. From there, the level 2 routing algorithm sends the packet to its destination area.

Configuring Routing Parameters

In each system you can set the following routing parameters:

- Maximum number of nodes in the area
- Maximum number of routers adjacent to this router
- Maximum number of networks on any given node
- Maximum number of end-nodes one hop away from this end-node
- Cost of a hop on each network to which this node is attached
- Values of several timers involved in sending hello messages and expecting them from other nodes

IBM’s Implementation of DNA IV

The main user interface program for the router’s implementation of DNA IV is called NCP. The router’s NCP is a limited subset of the DECnet Network Control Program (NCP) commands. The router’s NCP enables you to view and modify the various operating arguments of DNA IV and to read various DNA-specific counters.

Some of the features of the router’s NCP include the following:

- NCP implements new entities: module access-control and module routing-filter.
- NCP has no set executor buffer size command because the router does not originate any DECnet traffic. The router can forward the largest packet any DECnet implementer can generate. It honors the buffer size restrictions of all adjacent nodes.
- NCP allows an all qualifier on the node, area, and circuit subcommands.

The router NCP is similar to NCP on DECnet-VAX, with the following differences:

- Router NCP does not include the set node name command, and therefore cannot assign names to nodes, or display node names with addresses.
- Router NCP does not include the clear or purge commands, nor do the set commands have an all argument. The permanent database is always copied to the volatile database when the router starts, restarts, or boots.
- A router NCP command can have only one argument.
- NCP does not have the concept of lines. To see the data that a DECnet-VAX NCP show line command displays, use the GWCON interface and network commands.
- Router NCP does not support cross-network commands:
  - Router NCP does not include the tell command, which requests NCP commands on other nodes.
– Similarly, router NCP does not support protocol requests from other DNA routers to execute NCP commands at the router on their behalf.

**Important**

Before configuring DNA IV, you need to be aware of the optional security features discussed in:

- "Managing Traffic Using Access Control"
  – Provides additional security by limiting access within routers in the network.
- "Managing Traffic Using Area Routing Filters" on page 320
  – Limits access to group of areas from other areas
  – Allows blending of two DECnet address spaces

If you already are familiar with these topics, skip these two sections and begin reading at "Configuring DNA IV" on page 325.

**Managing Traffic Using Access Control**

Access control protects one group of nodes from other nodes on the network. Routers make all nodes on a network accessible to each other. Usually, the main forms of security are passwords and conservative use of DNA IV proxy access at the host level.

However, due to differences in the security level of machines, you might need to provide additional security by limiting access within the routers in the network. The DNA forwarder enables you to do this using access controls.

Generally, access controls are not recommended due to the following liabilities:

- Access controls affect performance of the router because every packet is tested. The more complicated the access control configuration, the greater the performance impact.
- Access controls are difficult to configure and errors in configuration are difficult to diagnose.
- Access controls cannot hide a node from the routing protocols. The node remains visible from all routers in its area.

**Note:** Access controls do not guarantee security; they only make intrusion more difficult. The DNA IV routing protocols used on Ethernet and other broadcast media do not have built-in security features.

Access control prevents the forwarding of DNA IV (Long Format) data packets on the basis of source address, destination address, and interface. Access control does not affect routing packets, because they use a different packet format. This makes configuring access control safer, because you cannot break the routing protocol.

To implement access control, addresses are masked and compared. That is, the address in question is masked with 1s in the bit positions to be tested, and 0s in the free area. The address is then compared to a fixed value. For example, you could use a mask of 63.1023 (all 1s), and compare it to a result of 6.23 which would be true only for node 6.23. You could use a mask of 63.0 and a result of 9.0 which would be true for any node in area 9.
These mask and compare values come in pairs for source and destination address. They are then formed into lists for an interface. Each interface can have one access control list, which is applied to packets received on that interface. This list may be inclusive or exclusive. An inclusive list is a set of address pairs that designates a corridor for traffic flow. An exclusive list is a set of address pairs that does not allow traffic flow.

In an inclusive list, the source and destination addresses are tested using the mask and compare values. If any entry’s source and destination matches, the packet is forwarded. In an exclusive list, the source and destination addresses are tested using the mask and compare values. If any entry’s source and destination matches, the packet is dropped. The choice between exclusive and inclusive should be made on the basis of which list will be shorter. However, exclusive access control is usually easier to configure.

When packets are dropped due to access controls, the Return to Sender Request (RQR) bit is set in the Long Format Data Packet header and the packet is returned. Then, the connect request immediately fails, because NSP Connect Initiate packets are normally sent with the RQR bit set.

**Configuring Access Control**

Access control limits access to a particular host or group of hosts. You must assign access control to all routes to that host, not just the preferred route. Otherwise, access control functions when the primary route is up, but fails when the secondary route is in use.

On your network map, draw a line to isolate the secure region from the rest of the network. Ideally the line should cross the minimum possible set of adjacencies so that the least number of interfaces are running with access control. For broadcast networks (Ethernet and Token-Ring), draw the line through the drop cable to the node, to identify the interface to filter. For each interface crossed by the access control line, use NCP to define the same access control list.

**Note:** Because all DECnet applications use the NSP protocol, which requires bidirectional connectivity, you do not need to define access controls in both directions.

**Inclusive Access Control**

In Figure 15 on page 319, node 1.13 wants to communicate with nodes 1.2 and 1.4 only. Access control allows you to secure nodes from all nodes connected by routers. Therefore, in Figure 15 on page 319 you can protect node 1.13 from all nodes except node 1.9 because these two nodes share the same physical network. To configure the desired access control for this example, build an inclusive filter on interface Eth/0 of router 1.19 as shown in the bottom of Figure 15 on page 319.
The first and second entries of the inclusive filter information shown in Figure 15 allow nodes 1.2 and 1.4 to send packets to node 1.13. The third entry allows any node to send to node 1.9 (you are not trying to secure node 1.9).

To configure the example given for router 1.19, enter the following NCP commands and parameters:

```
NCP> def mod access-cont circ eth/0 type inclusive
NCP> def mod access-cont circ eth/0 filter 1.2 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 1.4 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 0.0 0.0 1.9 63.1023
NCP> def mod access-cont circ eth/0 state on
```

**Exclusive Access Control**

**Figure 16 on page 320** shows how exclusive access control isolates node 4.4 from the rest of the campus.
Configure the desired access control for this example by building an exclusive filter on the PPP/0 interface of router 4.3 as shown in Figure 16. To configure the example given for router 4.3 in Figure 16, enter the following NCP commands and parameters:

```
NCP> def mod access-cont circ ppp/0 type exclusive
NCP> def mod access-cont circ ppp/0 filter 0.0 0.0 4.4 63.1023
NCP> def mod access-cont circ ppp/0 state on
```

**Managing Traffic Using Area Routing Filters**

Area routing filters allow special configurations of your DNA network. Because this is an advanced topic, very few DNA IV networks need routing filters. There are two primary applications for area filtering in DNA IV:

- Security, limiting access to some group of areas from other areas.
- Allowing the blending of two DECnet address spaces.

**Note:** Area Routing Filters are very tricky and subtle to configure. It is very easy to completely break your area routing. If you do not understand how DECnet routing works, especially at the area level, do not try to use routing filters. Documentation on the DECnet routing protocol can be found in *DECnet Digital Network Architecture Phase-IV Routing Layer Functional Description*, Order Number AAX435ATK, December 1983, Digital Equipment Corporation, Maynard, Massachusetts.

Area routing filters allow you to configure a router to control the information about DECnet areas that are sent or accepted in level 2 routing messages. You may
configure separate incoming and outgoing filters for each interface. Each filter specifies which areas routing information will be passed to or accepted from.

When a network sends a level 2 routing update and there is a routing filter, the entry (RTGINFO) for any area not in the filter has the cost of 1023 and a hop count of 63. Any area in the filter has the correct cost and hops placed in the entry.

When the network receives a level 2 routing message and there is a routing filter, any entry for an area not in the filter is treated as if the cost is 1023 and the hop count is 63 (unreachable). Any routing entry from the packet that is in the filter is processed normally.

The routing filters affect the processing of level 2 routing messages only. There are no filters for level 1 routing messages. Routing filters have no effect on router hello processing, and do not prevent area routers from developing adjacencies. They affect the area routing database. If the filters prevent an area router from learning about another area, they would prevent the router from becoming attached, and then the router could not advertise as an area router.

Security by Area Filtering
Like access controls, routing filters provide security. However, routing filters have some disadvantages compared to access controls:

- Area filtering is less flexible than access controls because it requires the assignment of areas to correspond to the desired security architecture.
- Area filtering is more difficult to understand and configure.
- The level of security is lower because a host that ignores the lack of routing information can send the packets to the correct router anyway.

However, area filtering is more efficient because there is no need to check every packet. In the following example area filtering occurs in an area that contains workstations that are part of a large network that contains machines with confidential information. There might be one machine outside the area that the confidential machines need to reach for information.

In Figure 17 on page 322, area 13 contains workstations that need to be able to reach area 7. Node 13.1 is the router, and the other nodes are the workstations. Node 13.1 has a filter to accept only routes to area 7. Therefore, if node 13.1 receives a packet from any node in area 13 not destined for area 7, node 13.1 cannot forward the packet and sends the sending node an error message.

To configure router 13.1 in Figure 17 on page 322, enter the following NCP commands and parameters:

```
NCP> def mod routing-filter circ eth/1 incoming area 7
NCP> def mod routing-filter circ eth/1 incoming state on
```
Blending DECnet Domains

DECnet has a 16-bit node address space with a fixed hierarchy of 6 bits of area and 10 bits of node. By comparison, IP has a 32-bit node address space with a flexible multilevel hierarchy. Many established networks have now grown to the point where they use all 63 areas. The problem is that as different facilities connect to each other, they want to connect their DECnet networks but cannot due to area number conflicts.

The only solution is to redesign the DECnet architecture. (This is addressed by DECnet Phase V.) However, by using area routing filters, it is possible to allow some overlap between two DECnet domains.

Domain is not a standard DECnet term; it is used here as a name for a DECnet wide-area network, presumably one with many areas. The goal is to blend two of these domains, so that there is a common area that can reach parts of both domains. However, there are more than 63 areas in the union of the two domains. Because area filtering is not simple to administer and is restrictive, you should not consider using it if there are enough area numbers available for the union of the two domains.

To configure the overlap of two domains, first you must decide which areas to intersect. These areas are the ones that will be able to participate in both domains. These area numbers must not be used elsewhere in the two domains.
In designing the intersection, be careful that neither domain relies on routes through the intersection to maintain connectivity between areas that are not in the intersection. Because the routes in and out of the intersection are filtered, they probably do not offer normal reachability between all areas in the domain.

To decide how to configure the routing filters, draw a concise map of the configuration. On this map, locate all of the areas and outline the two domains. Then decide upon the filtering fence that you need to establish. Carefully go around the intersection of the two domains and locate all level 2 adjacencies that cross the filtering fence. These are one hop communications paths between level 2 routers that cross between areas.

In the example, there are six adjacencies that cross the fence, 1.18 to 5.7, 1.18 to 5.8, 1.18 to 8.3, 2.17 to 3.12, 2.21 to 4.7, and 2.21 to 4.9.

The first step in designing the area filters is to set up filters that keep the areas in one domain from being propagated into the other domain. The only area routes that should leave the intersection are those for areas in the intersection. In the example, these are areas 1 and 2. Therefore, only routes for areas 1 and 2 should be sent from nodes such as 2.17 and 3.12.

On point-to-point links such as 2.17 and 3.12, it does not matter which end filters, but it is probably safer to filter on the sending end. Therefore there would be a filter on the interface of 2.17, allowing forwarding only routes from areas 1 and 2. The same would occur on the two interfaces of 2.21 and the link from 1.18 and 8.3.

When the hop between two areas is an Ethernet or other broadcast media, such as 1.18 to 5.7 and 5.8, you should make the decision on another basis. Most Ethernets have most of the level 2 routing nodes in one area, and a few in the second area. Here, the filtering should be on the few, rather than the many. In the example, node 1.18 is the interloper on the Ethernet in area 5, so it should filter. Mode 1.18 would send routers only for areas 1 and 2 on the Ethernet.

You can filter on both ends of an adjacency. This adds an extra layer of security against accidental reconfiguration. However, if you set up only one end for filtering, then only that end filters.

Given these filters, the two domains cannot contaminate each other. However, for a node in the intersection, it is not clear which area 3 will be reached when a connection is attempted to node 3.4. It depends on the current route and the circuit costs. Clearly, this is not ideal. It does not matter that there might only be a node 3.4 in domain A and not in domain B. Routing between areas is done solely on the basis of area; only the routers inside an area know the routes to nodes in that area.

Thus, you must establish a second set of filters to decide which instance of an area (domain A or B) is reachable from the intersection for each area not in the intersection. Therefore, you could decide that nodes in the intersection could reach areas 3 and 4 in domain A and area 5 in domain B. In the example, this would be
Using DNA IV

done by configuring routers 1.18 and 2.21 to only accept routes to areas 3, 4, 6, and 8 from domain A. Routers 2.17 and 2.21 would only accept routes for areas 5 and 9 from domain B.

Therefore, nodes in the intersection see a universe that contains areas 1 and 2 from the intersection, areas 3, 4, 6, and 8 from domain A, and areas 5 and 9 from domain B.

To configure router 1.18 in Figure 18, enter the following NCP commands and parameters:

```
NCP> def mod routing-filter circ eth/0 outgoing area 1,2
NCP> def mod routing-filter circ eth/0 outgoing state on
NCP> def mod routing-filter circ eth/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ eth/0 incoming state on
NCP> def mod routing-filter circ ppp/0 outgoing area 1,2
NCP> def mod routing-filter circ ppp/0 outgoing state on
NCP> def mod routing-filter circ ppp/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ ppp/0 incoming state on
```

\[Figure 18. \text{Example of Blending DECnet Domains}\]
There is still no way that a node in domain A area 5 can communicate directly to a node in domain B area 5. For nodes in these two areas to communicate, you must do a series of application-level relays using the set host command. For example:

- Run the set host command to remotely login from a node in the domain A area 5 to a node in domain A area 8.
- Run the set host command to remotely login from a node in domain A area 8 to a node in area 1 or 2.
- Run the set host command to remotely login from a node in area 1 or 2 to a node in domain B area 5.

**Configuring DNA IV**

The DNA IV protocol runs over Token-Ring, Frame Relay, Ethernet, PPP, Token-Ring ATM LAN Emulation clients, Ethernet LAN Emulation clients, and X.25 interfaces. The following sections describe the procedures for configuring the DNA IV protocol to work over Token-Ring and X.25 interfaces.

**Note:** When operating in mixed DNA IV and DNA V networks, all DNA IV configuring and monitoring must be done from the process described in this chapter.

**DNA IV and DNA V Algorithm Considerations**

DNA IV uses a distance-vector routing algorithm. DNA V can use either a distance-vector or a link-state routing algorithm. The algorithm that the bridging router selects is according to what protocol is enabled and disabled, and any combinations that can result from these two protocols. See Table 104 for details.

<table>
<thead>
<tr>
<th>DECnet IV Status</th>
<th>OSI/DNA V Status</th>
<th>Algorithm Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>Distance-vector (automatically)</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>Link-state (automatically)</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enabled</td>
<td>Use the set algorithm command to configure this information into SRAM.</td>
</tr>
</tbody>
</table>

**Configuring DNA IV For Token Ring**

The procedure to run the DNA IV protocol over 802.5 Token Ring (TR) involves commands from the DNA IV and Token-Ring configuration processes.

1. From the OPCON prompt (*) enter the configuration process.
   ```
   * talk 6
   Config>
   ```

2. Enter `list device` to see the interface numbers for the Token-Ring interfaces. Note the interface number of each Token-Ring interface.
   ```
   Config> list device
   ```

3. Use the `network` command with the interface number of the Token-Ring interface you want to configure. This places you in the Token-Ring configuration process.
   ```
   Config> network 0
   TKR config>
   ```

4. Use the `list` command to verify the Token Ring configuration information.
   ```
   TKR config> list
   ```

Token-Ring configuration:

- Packet size (INFO field): 2052
- Speed: 4 Mb/sec
- Media: Shielded
RIF Aging Timer: 120
Source Routing: Enabled
Mac Address 000000000000

5. Exit the Token-Ring configuration process and enter the DNA NCP configuration process.
   TKR config> exit
   Config> protocol DN
   NCP>

6. Use the define command to define a DNA circuit on the Token-Ring interface:
   NCP> define circuit tkr/0 state on

7. Optionally use the define command to set the routing type for the circuit. For bilingual or Phase IV support, you need to change the routing type from the default (standard) to either bilingual or AMA.
   NCP> define circuit tkr/0 router type bilingual
   or-
   NCP> define circuit tkr/0 router type AMA

8. Use the list command to check the parameters.
   NCP> list circuit tkr/0 characteristics

   Circuit Permanent Characteristics
   Circuit = TKR/0
   State = On
   Cost = 4
   Router priority = 64
   Hello timer = 15
   Max routers = 16
   Router type = Standard

9. Restart the router, so that all configured parameters take effect.

   Note: If you want to disable source-routing or set the RIF-timer to a value other than the default value, use the source-routing command and the set RIF-timer command in the Token-Ring configuration process.

Configuring DNA IV for X.25
The procedure to run the DNA IV protocol over X.25 circuits involves commands from the X.25 and DNA IV configuration processes.

   1. From the OPCON prompt (*) enter the configuration process. Go to “t 6” and enter X.25 config (net #). If this is the first time X.25 is being configured then do the following:
   a. DEFINE the router’s DTE address.
      X.25 Config> set address
   b. DEFINE each protocol that will be supported over X.25:
      X.25 Config> add protocol
      IP It is usually a good idea to add this protocol so that you can verify the general X.25 configure is OK
      DN
      Note: Allow protocol parameters to default.
   c. DEFINE protocol remote address to the remote X.25 address mapping for the protocols that require this:
      X.25 Config> add address
      for IP:
      * IP address = 128.185.247.22
• X.25 address = 22
for DN:
• DN address = 5.22
• X.25 address = 22
d. VERIFY that one end of the X.25 circuit is a DTE and the other end is a DCE.

```
X.25 Config> list all
```

Check the National Personality field for device type. For a national personality type of GTE-Telenet you see:

```
National Personality: GTE Telenet (DTE)
```

- or -

```
National Personality: GTE Telenet (DCE)
```

To change the device type to DCE, enter:

```
X.25 Config> set equipment-type dce
```

Lists all parameters configured for X.25

National Personality: GTE Telenet (DTE) National Personality: GTE Telenet (DCE)

If not, then chose one router to act as a DCE and modify as such,

```
X.25 Config> set national-personality dce
```
e. RESTART the router, so that all configured parameters take effect.
f. To VERIFY that the configuration is valid after a restart, go to the monitor side and observe if the link is coming up.

```
* t 5
+ c
```

This gives you the state of the link at that time. If you see the state of the X.25 link transitions from “testing” to “down”, go to ELS messages and see if there is an obvious error. If the state of the X.25 link transitions from “testing” to “up”, then chances are the x.25 configuration is valid.

2. To VERIFY that the X.25 link is operational:
a. TRY to PING each end of the X.25 link from the IP monitor:

```
IP> interface
```

Verify that the correct X.25 addresses had been configured in the IP protocol.

```
IP> ping IP address of remote X.25 link
```

3. To CONFIGURE DECnet PhaseIV on the Router:
a. DEFINE DECnet Executor parameters:

```
NCP> define exec address area.node
   Router’s DECnet address
```

```
NCP> define exec type DEC ROUTING-IV
   Configures the router as a LEVEL 1 DEC type router
```

**Note:** This example is for configuring a router to interoperate with other routers supporting the DEC-routing standard over X.25 networks. A router supporting the standard must be defined
Using DNA IV

as type DEC-ROUTING-IV (level 1) or DEC-AREA (level 2). The default routing type is ROUTING-IV and AREA which allows interoperation with many existing IBM 2210 and other compatible routers.

NCP> define exec state on

Restart the router so that when you configure the X.25 circuit, all DEC specific parameters are visible. To verify executor configuration, NCP> show executor characteristics

b. DEFINE PhaseIV X.25 circuits.

You must configure the X.25 circuit as either a PVC or SVC. If this circuit is configured as a PVC then the other end must also be a PVC. If this circuit is configured as an IN-SVC, then the other end must be configured as an OUT-SVC

NCP> define cir x25/0 usage IN-SVC
NCP> define cir x25/0 DTE-address "remote X.25 DTE"
NCP> define cir x25/0 call-data
NCP> define cir x25/0 verification enabled

Enabling verification is optional.

c. DEFINE circuits to the active state:
   - for Token-Ring
     NCP> define cir TKR/0 router type bilingual
   - for ALL circuits
     NCP> define cir xxx state on

Restart the router so that all of the DECnet parameters become effective, VERIFY the X.25 configuration within the DECnet protocol is as you want it.

NCP> list circuit x25/0 characteristics
Chapter 9. Configuring and Monitoring DNA IV

DNA IV Configuration and Monitoring Commands

This section describes the NCP configuration and monitoring commands. Enter the commands at the `NCP>` prompt. All NCP commands can be accessed from either the configuration or monitoring environments.

Table 105. NCP Configuration and Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page xxvii.</td>
</tr>
<tr>
<td>define</td>
<td>Defines items in the nonvolatile (permanent) database, including:</td>
</tr>
<tr>
<td></td>
<td>- Access control lists and routing filters</td>
</tr>
<tr>
<td></td>
<td>- Circuit items</td>
</tr>
<tr>
<td></td>
<td>- Arguments global to DNA</td>
</tr>
<tr>
<td></td>
<td>- Configuration data from the nodes</td>
</tr>
<tr>
<td>purge module</td>
<td>Removes access control lists and routing filters from the permanent database.</td>
</tr>
<tr>
<td>set</td>
<td>Sets or changes items in the volatile database, including:</td>
</tr>
<tr>
<td></td>
<td>- Circuit items</td>
</tr>
<tr>
<td></td>
<td>- Arguments global to DNA</td>
</tr>
<tr>
<td></td>
<td>- Configuration data from the nodes</td>
</tr>
<tr>
<td>show</td>
<td>Displays the status of the volatile database and volatile nodes in the routing database.</td>
</tr>
<tr>
<td>show/list</td>
<td>Displays items in the volatile (show) or permanent (list) database, including:</td>
</tr>
<tr>
<td></td>
<td>- The current state of the specified circuits</td>
</tr>
<tr>
<td></td>
<td>- The current state of the volatile/permanent database for DNA</td>
</tr>
<tr>
<td></td>
<td>- DECnet access control lists that have been defined in the permanent database for the router</td>
</tr>
<tr>
<td></td>
<td>- DECnet area routing filters that have been defined in the permanent database for the router</td>
</tr>
<tr>
<td>zero</td>
<td>Clears circuit counters in the volatile database, global counters in the volatile database, and counters in the access control list module. Does not clear the argument settings made with set or define commands.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxvii.</td>
</tr>
</tbody>
</table>

Note the following information about the commands:

1. The define commands do not take effect until the next time the router is started.
2. The list, define, and purge commands modify or display data in the permanent (router’s Static RAM) database. The permanent database is stored in the configuration, and remains in effect across restarts, software loads, and power cycles.
3. The show and list commands are the most useful for monitoring the DNA IV protocol.
4. Use set, show, and zero to modify, display, or clear data in the volatile database.
5. The zero command clears statistics saved in the volatile database, but does not clear the argument settings made with set or define commands.
Define/Set

This section explains both the **define** and the **set** commands.

Use the **define** command to define access control lists and routing filters, and to define circuit, executor, and node parameters. **Define** is used to set SRAM (needs reboot).

**Syntax:**

```
define circuit-specifier ... 
  executor ... 
  module access-control ... 
  module routing-filter ... 
  node ... 
```

**Set** can be used for volatile RAM (immediate change, no reboot).

**Syntax:**

```
set circuit-specifier ... 
  executor ... 
  node ... 
```

circuit-specifier argument

The circuit-specifier options include the following:

**active circuits**

Specifies all circuits who are up and whose state is on (set only).

**all circuits**

Specifies all circuits on the router.

**circuit name**

The name of the circuit. For example: Eth/0, TKR/0, PPP/1.

**known circuits**

(set only) Specifies all circuits on the router.

The arguments include the following:

**call-userdata**

Used during circuit initialization of static X.25 circuits. When a circuit is defined as an outgoing SVC, the initial and all subsequent call requests contain the defined call-userdata when the circuit is enabled. When a circuit is defined as an incoming SVC, one of the criteria for accepting an incoming call request is a match of the defined call-userdata.

Currently the call-userdata must be set to the DTE of your local router for both incoming and outgoing SVCs.

Enter an even number of hexadecimal characters (octets) up to a maximum of 14 characters.

**cost [range]**

Sets the cost to receive a packet on this circuit. This is used by the
DNA IV Configuration and Monitoring Commands

Routing algorithm to determine the cost of a circuit in choosing routes (cost is not the same as an IP metric). Range: 1 to 25. Default: 4.

The following values are suggested starting points:

<table>
<thead>
<tr>
<th>Circuit type</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>4</td>
</tr>
<tr>
<td>Token-Ring 4/16</td>
<td>4/16</td>
</tr>
<tr>
<td>Sync 56 Kb</td>
<td>6</td>
</tr>
<tr>
<td>Sync T1</td>
<td>5</td>
</tr>
<tr>
<td>X.25</td>
<td>25</td>
</tr>
</tbody>
</table>

Example:

`define circuit tkr/0 cost 5`

DTE Address

Specifies the address of the remote DTE on the X.25 circuit. This is always the address of the remote system. This is a decimal number of up to 14 characters.

Hello timer [range]

Specifies how often (in seconds) router hellos are sent on this circuit. Range: 1 to 8191 seconds. Default: 15 seconds (recommended).

Maximum recalls

(define only) Specifies how many attempts the router makes to reestablish an outgoing static SVC call after an initial call failure. After the maximum number of recalls, the router makes no further attempts to establish the SVC without your intervention. Valid values are in the range of 1 to 20, the default is 1. See also the recall timer argument.

Maximum routers [range]

(define only) Specifies how many other routers there may be on this circuit. Range: 1 to 33. Default: 16.

Note: This parameter is not user-configurable on an X.25 circuit when the executor type is set to DEC-routing-IV or DEC-area. In this case the maximum number of routers is 1.

If this is a level 1 router, only routers on this circuit in the same area count. If this is a level 2 router, all routers on this circuit count. The local router does not count against the limit.

The router’s efficiency and memory requirements are improved by keeping this number low. Set this argument to equal a few more than the total number of adjacent routers on the circuit. Do not set this argument to less than the number of routers on the circuit; this can result in anomalies in routing.

Note: For a point-to-point (synchronous line) circuit, set this argument to 1. The result is significant memory savings on a router with multiple point-to-point lines.
DNA IV Configuration and Monitoring Commands

The sum of maximum routers over all circuits should be less than the executor maximum broadcast routers argument, although this limit is not strongly enforced.

**recall timer**
Determines the delay in seconds between call attempts to establish an X.25 outgoing static circuit.

For `define`, valid values are in the range 1 to 60 seconds. The default is 1 second. See also the argument maximum recalls.

For `set`, valid values are in the range 0 to 65595 seconds. The default is 60 seconds.

**router priority [range]**
Specifies the router’s priority in bidding to become the designated router for the end-nodes on this circuit. Range: 1 to 127, where 127 is the highest priority. Default: 64.

If two routers have the same priority, the one with the higher node address wins. The router priority has no effect on area routing decisions, or in reaching the closest attached level 2 router.

Use the router priority to choose the designated router to be the one that is most likely to be the best next hop for the end-nodes on the circuit. If there are two routers on a circuit, one with 500 nodes behind it, the other with 20 nodes behind it, the one with 500 nodes should have the higher router priority. This is not required, however, because once a packet from an end-node packet reaches a router, it will be forwarded toward its destination.

This argument is irrelevant on point-to-point lines, where there will be no end-nodes. (A designated router is selected anyway.)

**router type**
Specifies the kind of routing that the router needs to perform, standard, AMA, or bilingual.

- **Standard.** Specifies that the router is using conventional phase IV addressing where the MAC address is built from the area and node number. The router defaults to this type.

- **AMA.** Specifies that the router can route packets that use phase IV addressing where the MAC address is arbitrary and learned from the data link layer.

- **Bilingual.** Specifies that the router can route packets that use both conventional and phase IV with AMA addressing.

**state**
When set to `on` specifies that the circuit is enabled for use by DNA. When set to `off` specifies that the circuit is disabled for use by DNA. `off` is the default.

**usage**
Specifies whether an X.25 circuit is:

- PVC: A permanent virtual circuit
- OUT-SVC: An outgoing static circuit
- IN-SVC: An incoming static circuit

This parameter applies when the executor type is set to `DEC-routing-IV` or `DEC-area`. (See `circuit executor type` for more information.)
verifications
Specifies whether the router compares a verification string on the router to verification data in an incoming initialization message. If they do not match, the X.25 circuit must be reinitialized. Specify enabled or disabled.

executor argument
Defines or sets arguments (that is, the executor) global to DNA in the permanent (define) or volatile (set) database.

Most of these arguments reduce the efficiency of the router, and increase the load on the circuits, as they are made larger. They can also increase memory requirements. They should not be used unnecessarily in excess of the values required for the actual network configuration.

For set, the executor must be in the off state to modify numeric arguments or type in the volatile database. (Unlike DECnet-VMS, the set executor state on command is valid when the executor state is off.) These changes take place immediately without rebooting the router.

address [area.node]
Sets the executor’s node address, the node ID of this router. Area range: 1 to 63. The area and the node must be less than executor maximum area. Node range is 1 to 1023. The default 0.0 is illegal.

Note: DNA will not be enabled if the executor address is not set to a legal value.

area maximum cost [number]
Maximum cost allowed between this level 2 router and any other level 2 router. If the best route to an area is more costly than this, that area will be considered unreachable. Maximum: 1022. Default: 1022. This argument does not apply to level 1 routers. It should be greater than the maximum legal cost to the most distant area. A suggested value is 25 times “area maximum hops”.

area maximum hops [number]
Maximum number of hops allowed between this level 2 router and any other level 2 router. If the best route to an area requires more hops than this, that area will be considered unreachable. Maximum: 30. Default: 30. This argument does not apply to level 1 routers. It should be about twice the longest path length (in hops) that is expected.

The hop count is used by routing only to speed the decay of routes to unreachable areas. The area maximum hops may be reduced to cause unreachable areas to become unreachable more quickly.

broadcast routing timer [range]
Specifies how often level 1 (and 2 in a level 2 router) routing messages are sent, in seconds. This is how often they will be sent in the absence of any cost or adjacency changes. This protects the routing database from corruption. At least partial routing updates are sent automatically if any cost or adjacency changes. Range: 1 to 65535. Default: 180. Lower values increase the overhead for this and all adjacent routers. Larger values increase the time required to correct the routing database if a partial routing update message is lost.
maximum address number [range]

(define only) Is the highest node address (within this area) for which routes will be kept by this router. The routing database will not include routes to nodes in this area with a higher node part of their address. Range: 1 to 1023. Default: 32. It should be higher than the highest node address in the router’s area. Setting it excessively large will affect the efficiency of the router, and will use excess memory. This argument does not take effect until the router is restarted.

maximum area number [number]

(define only) Is the highest area for which routes will be kept, if this is a level 2 router. The routing database will not include routes to areas higher than this. Maximum: 63. Default: 63. It should be higher than the highest area number in the overall network. This argument does not take effect until the router is restarted.

maximum broadcast nonrouters [number]

(define only) Maximum number of end-nodes that can be adjacent (one hop away) to this router. This is the sum over all broadcast circuits. If there are more end-nodes, some of those end-nodes will not be reachable by this router, which may cause unpredictable routing problems. This argument does not take effect until the router is restarted. Range: 1 to 1023. Default: 63.

maximum broadcast routers [number]

(define only) Maximum number of routers than can be adjacent (one hop away) to this router. This is the sum over all broadcast circuits. If there are more routers, routes will not be accepted from the excess routers. This may cause unpredictable routing problems. This argument does not take effect until the router is restarted. Default: 32. Maximum: 33 times the number of circuits. This value should be greater than or equal to the sum of “circuit maximum routers” over all circuits, although this is not strongly enforced. This parameter has a strong effect on memory utilization, and should not be set much larger than required. Because the default is rather high, you may need to reduce the value if you have set a large “maximum address.”

maximum cost [number]

Maximum cost allowed between this router and any other node in the area. If the best route to a node is more costly than this, that node will be considered unreachable. Maximum: 1022. Default: 1022. It should be greater than the maximum legal cost to the most distant node. A suggested value is 25 times “maximum hops”.

maximum hops [number]

Maximum number of hops allowed between this router and any node in the area. If the best route to a node requires more hops than this, that node will be considered unreachable. Maximum: 30. Default: 30. It should be about twice the longest path length (in hops) that is expected. The hop count is used by routing only to speed the decay of routes to unreachable nodes. The maximum number of hops may be reduced to cause unreachable nodes to become unreachable more quickly.

maximum visits [number]

Specifies that any packet forwarded by this router that has been forwarded by more than maximum visits routers will be dropped.
This is used to detect packets which are in routing loops, which occur when routes decay. The maximum visits is 63. This is the default. This argument should be larger, by a factor of two, than both maximum hops and area maximum hops.

state on
Enables DNA. May be issued at any time, providing the router has a valid node address.

state off
Disables DNA. May be issued at any time. The default state is off.

For set, set executor will be inhibited if the DNA initialization failed for lack of available memory for the routing tables.

type (define only) On X.25 circuits, causes the router to act in one of four ways, depending on the value selected. The options are:

DEC-routing-iv
configures the router as a DEC-compatible Level 1 router.

DEC-area
configures the router as a DEC-compatible Level 2 (area) router.

Routing-iv
configures the router as a Level 1 router without DEC compatibility on X.25 circuits. This is the default.

Area
configures the router as a Level 2 (area) router without DEC compatibility on X.25 circuits.

A Level 2 router accepts adjacencies with routers in other areas, and maintains routes to all areas. If it can reach other areas, it also advertises itself to Level 1 routers as a route to other areas.

For Level 1 routers, adjacencies are accepted only to routers in the same area.

Example:
define executor state on
define executor type DEC-area
define executor maximum broadcast routers 10

type area
(set only) Causes the router to act as a level 2 router. It will accept adjacencies with routers in other areas, and will keep routes to all areas. If it can reach other areas, it will also advertise itself as a route to other areas to level 1 routers.

The DNA state must be set to off before changing the type.

type routing-IV
(set only) Causes the router to act as a level 1 router, which is the default. Adjacencies will be accepted only to routers in the same area.

The DNA state must be set to off before changing the type.

Example:
set executor state on
DNA IV Configuration and Monitoring Commands

set executor maximum broadcast routers 10

module access-control circuit-specifier argument

(\texttt{define} only) Defines access control lists, which are used to restrict the forwarding of packets between certain origins and destinations. Each access list is associated with one circuit, and applies to DECnet Long Format Data Packets received on that circuit. Access control does not apply to any routing or hello packets.

The arguments for the circuit-specifiers include the following:

- \textbf{all circuits}
  - Specifies all circuits on the router.

- \textbf{circuit name}
  - Specifies the named circuit.

- \textbf{known circuits}
  - Specifies all circuits on the router.

The following items are the arguments you select from after you enter the \texttt{define module access-control} command and the circuit-specifier:

- \textbf{state on}
  - Enables the access control list on this circuit.

- \textbf{state off}
  - Disables the access control list on this circuit.

- \textbf{type exclusive}
  - Specifies that any packets matching one or more of the filters in the access control list for this interface will be dropped.

- \textbf{type inclusive}
  - Specifies that only packets matching one or more of the filters in the access control list for this interface will be forwarded.

- \textbf{filter [source-result source-mask dest-result dest-mask]}
  - Adds a filter to the list for the specified circuit. The filter is added to the end of the existing list.

  The source address is masked with the source-mask, and compared to the source-result. The same is done with the dest-mask and dest-result. The action depends on what type of access control is in use on the circuit.

The following items are the options you select from after you enter the \texttt{define module access-control} command and the \texttt{filter} circuit-specifier:

- \textbf{source-result}
  - Address that the source address is compared to after masking.

- \textbf{source-mask}
  - Mask used for the source address.

- \textbf{dest-result}
  - Address that the destination address is compared to after masking.

- \textbf{dest-mask}
  - Mask used for the destination address.

\textbf{Example:} define module access-control circuit eth/0 state on
module routing-filter circuit-specifier argument

(define only) Defines routing filters, which are used to restrict the sending of Area routes by level 2 (Executor Type Area) routers.

all circuits
  Specifies all circuits on the router.

circuit name
  Specifies the named circuit.

known circuits
  Specifies all circuits on the router.

The following items are the direction options you select from after you enter the define module routing-filter command and the circuit-specifier:

incoming
  Affects the filter on routing information received on this circuit.

outgoing
  Affects the filter on routing information sent on this circuit.

The following items are the arguments you select from after you enter the define module routing-filter command and the circuit-specifier:

area [area-list]
  Specifies that the filter allows routing information to pass for the set of areas in the area-list. The area-list is a comma-separated list of areas or ranges of areas. A range is specified by two area numbers separated by a dash. The area-list can also be none, specifying that information will be passed on no areas. The following are area-list examples:

  1,4,9,60
    Areas 1, 4, 9, and 60

  1-7,9-13,23
    Areas 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, and 23

state on
  Specifies that the filter is active.

state off
  Specifies that the filter is disabled, but continues to be stored in the permanent database. The only way to remove the filter is by using the purge command.

Example: define module routing-filter circuit eth/0 state on

node argument
  Allows defining or setting configuring information on nodes into the volatile (set) or permanent (define) database. The only node for which any information is kept is the executor node, because node names are not stored. The node specifies the router’s (executor’s) node address. See the define executor command description.

Example: define node state on

Example: set node state on
DNA IV Configuration and Monitoring Commands

Purge

Use the purge command to remove access control lists and routing filters from the permanent database.

Syntax:

```
 purge module access-control ...
 module routing-filter ...
```

- `module access-control circuit-specifier`
  - Removes access control lists from the permanent database. You can delete an entire access control list; you cannot delete one filter.
    - `all circuits`
      - Specifies all circuits on the router.
    - `circuit name`
      - Specifies the named circuit.

Example: `purge module access-control all circuits`

- `module routing-filter circuit-specifier`
  - Removes routing filters from the permanent database. You can purge a specified filter or you can purge them all.
    - `all`
      - Specifies all routing filters in the configuration memory.
    - `circuit name`
      - Specifies the routing filter for the named circuit.

Example: `purge module routing-filter all`

Set

Use the set command to add, set, or modify circuit specifiers, global arguments, data link modules, or nodes in the volatile DNA database.

Syntax:

```
 set circuit ...
 executor ...
 node ...
```

For a description of the options for these arguments, see "Define/Set" on page 330.

Show

Use the show command to show the status of the volatile database and volatile nodes in the routing database.

Syntax:

```
 show area-specifier ...
 node-specifier ...
```

- `area-specifier argument`
  - Examines the status of the volatile area routing database. This lets you find out what areas are reachable, and what the routes are to various areas.
The options for the area-specifiers include the following:

**active areas**
Provides information on those areas which are currently reachable.

**all areas**
Provides information on all areas (up to the executor maximum area).

**area**
Provides information on the specified area. If the area is not provided, you will be prompted for it.

**known areas**
Provides information on those areas which are currently reachable.

The following items are the subcommand options you select from after you enter the `show` command and the area specifier:

**characteristics**
Shows the current state of the specified area. (The same as summary.)

**status**
Provides detailed information on the specified areas, including cost and hops.

**summary**
Shows the current state of the specified areas. This is the default.

Example:
```
show active areas
```
```
Active Area Volatile Summary
Area State Circuit Next Node
  1 reachable Eth/0 1.22
  2 reachable 2.26
  3 reachable X25/0 2.30
```

Example:
```
show active areas status
```
```
Active Area Volatile Status
Area State Cost Hops Circuit Next Node
  1 reachable 3 1 Eth/0 1.22
  2 reachable 0 0 2.26
  3 reachable 2 1 PPP/0 3.0
  6 reachable 12 3 PPP/0 3.0
  3 reachable 11 1 X25/0 2.30

Area Volatile Status
Area State Cost Hops Circuit Next Node
  5 unreachable 1023 31
```

The following items define the information displayed when you use the `show` command.

**area**
Indicates the area for this line of the display.

**circuit**
Indicates which circuit the next hop to this node will go over. No circuit is given for the router’s own area.

**cost**
Indicates the cost to this area.

**hops**
Indicates the hops to this area.

**next node**
Indicates the router that will be the next hop (intermediate destination) to the specified area.

**state**
Indicates that this will be reachable or unreachable.
node-specifier argument

Shows the status of the volatile node routing database; this includes information on the reachable nodes and the routes to them.

The node-specifiers can be any of the following:

active nodes
Provides information on all nodes that are currently reachable.

all nodes
Provides information on all nodes (up to the executor maximum address). An all nodes display includes information on the “pseudo-mode” area.0. A route to node area.0 is advertised by any level two router which reaches other areas. Level one routers use these routes to forward all packets to the nearest level one router that knows how to get that packet to the correct area. There is no other way to examine node 0, because it is not a legal node address.

node node
Provides information on the specified node. If the node is not provided, you will be prompted.

known nodes
Provides information on those nodes which are currently reachable.

The arguments include the following:

classifiers/ summary
Both subcommand options show the current state of the specified nodes.

status
Provides detailed information on the specified nodes, including cost and hops.

Example:
show node status
This example shows the detailed status of a specific node.

Example:
show active nodes
This example shows the reachable nodes.

Example:
show adjacent nodes status
This example shows the detailed routing information on all adjacent nodes. Only nodes with one hop will be shown. The node type is known and displayed for adjacent nodes only since this information is contained in hello messages only.
Show/List

Use the show circuit command to retrieve information on the current state of the specified circuits from the volatile database. The list circuit command retrieves the data that is stored in the permanent data base for circuits.

Syntax:

```
show all
   area
   circuit . .
   executor . .
   known argument
   module argument
   node argument
```

```
list all
   area
   circuit argument
   executor argument
   module
   node argument
```

circuit-specifier argument

Where the circuit-specifiers options are the following:

active circuits
   Specifies all circuits that are currently on (per the volatile database).

all circuits
   Specifies all circuits on the router.

circuit name
   Specifies the named circuit.

known circuits
   Specifies all circuits on the router.

The following items are the subcommand options you select from after you enter the command and the circuit specifier:

characteristics
   Provides detailed information on all of the argument settings for the circuit.
**DNA IV Configuration and Monitoring Commands**

**counters**
Shows counters for the circuit.

**status**  Shows detailed information on the circuit from the volatile database.

**summary**  Shows summary information on the circuit from the volatile database. This is the default if no argument is supplied.

**Example:**
```
show all circuits
```
Circuit Volatile Summary

<table>
<thead>
<tr>
<th>Circuit State</th>
<th>Adjacent Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>X25/0 on</td>
<td>5.25</td>
</tr>
<tr>
<td>Eth/0 on</td>
<td>1.22</td>
</tr>
<tr>
<td>Eth/0</td>
<td>2.14</td>
</tr>
<tr>
<td>Eth/0</td>
<td>1.13</td>
</tr>
<tr>
<td>PPP/0 off</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**
```
list circuit eth/0 characteristics
```
Circuit Permanent Characteristics

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Eth/0</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>On</td>
</tr>
<tr>
<td>Cost</td>
<td>4</td>
</tr>
<tr>
<td>Router priority</td>
<td>64</td>
</tr>
<tr>
<td>Hello timer</td>
<td>15</td>
</tr>
<tr>
<td>Maximum routers</td>
<td>16</td>
</tr>
<tr>
<td>Router type</td>
<td>Standard</td>
</tr>
</tbody>
</table>

**Example:**
```
show active circuits status
```
Active Circuit Volatile Status

<table>
<thead>
<tr>
<th>Circuit State</th>
<th>Adjacent Node</th>
<th>Block Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth/0 on</td>
<td>1.22</td>
<td>1498</td>
</tr>
<tr>
<td>Eth/0</td>
<td>2.14</td>
<td>1498</td>
</tr>
<tr>
<td>Eth/0</td>
<td>1.13</td>
<td>1498</td>
</tr>
<tr>
<td>X25/0 on</td>
<td>5.25</td>
<td>1498</td>
</tr>
</tbody>
</table>

**Example:**
```
show all circuits characteristics
```
This example shows the current characteristics of the circuits on this machine. This includes all of the configuration arguments, as well as the current adjacencies, and the Listen timer (three times the adjacency's hello timer).

Circuit Volatile Characteristics

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Eth/0</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>on</td>
</tr>
<tr>
<td>Designated router</td>
<td>2.26</td>
</tr>
<tr>
<td>Cost</td>
<td>4</td>
</tr>
<tr>
<td>Router priority</td>
<td>64</td>
</tr>
<tr>
<td>Hello timer</td>
<td>15</td>
</tr>
<tr>
<td>Maximum routers</td>
<td>16</td>
</tr>
<tr>
<td>Adjacent node</td>
<td>1.22</td>
</tr>
<tr>
<td>Listen timer</td>
<td>45</td>
</tr>
<tr>
<td>Adjacent node</td>
<td>2.14</td>
</tr>
<tr>
<td>Listen timer</td>
<td>45</td>
</tr>
<tr>
<td>Adjacent node</td>
<td>2.30</td>
</tr>
<tr>
<td>Listen timer</td>
<td>90</td>
</tr>
<tr>
<td>Circuit</td>
<td>PPP/0</td>
</tr>
<tr>
<td>State</td>
<td>off</td>
</tr>
<tr>
<td>Designated router</td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td>4</td>
</tr>
<tr>
<td>Router priority</td>
<td>64</td>
</tr>
<tr>
<td>Hello timer</td>
<td>15</td>
</tr>
<tr>
<td>Maximum routers</td>
<td>8</td>
</tr>
</tbody>
</table>
Example:

```
show circuit eth/0 counters
```

This example shows the counters that are kept for the circuits. Note that some counters kept by DECnet-VAX are not kept here, but are instead read through the `network` command of GWCON.

```
Circuit Volatile Counters
Circuit = Eth/0
525249 Seconds since last zeroed
0 Terminating packets received
0 Originating packets sent
3693 Transit packets received
4723 Transit packets sent
0 Transit congestion loss
0 Circuit down
0 Initialization failure
0 Packet corruption loss
```

**adjacent node**

Node ID of a node that has an adjacency with this node on the circuit being displayed. While adjacencies with end-nodes automatically make that node reachable, a router adjacency does not automatically make that node reachable. A router is not considered reachable unless a routing message has been received over an active adjacency from that router. Thus, nodes may show as adjacent in the circuit database, but will not be in the reachable nodes database (show active nodes).

**block size**

Maximum data block size that the associated adjacent node is willing to receive. This is typically 1498 bytes, which is the standard 1500 bytes of an Ethernet packet, less the 2-byte length field used with DECnet.

**circuit**

Circuits to which this data applies.

**designated router**

Displays what this node believes to be the designated router for this area on this circuit. (There may be some transient disagreements when a new router starts up.) This normally will be the same for all routers on the circuit. End-nodes send all packets for destinations not on the local circuit to their designated router.

**hello timer**

Hello timer for this circuit. Router hello messages are sent this often on the circuit.

**listen timer**

Amount of time designating how often router or end-node hellos must be received from this adjacency on this circuit. It is three times the hello timer set for this circuit on the adjacent machine.

**router priority**

Router priority for this circuit, used in vying for designated router status.

**router type**

Router type for this circuit - standard, phase IV with AMA, or Bilingual.

**maximum routers**

Maximum number of routers allowed on this circuit.
DNA IV Configuration and Monitoring Commands

**state**  Either ON or OFF. In the volatile database, the state will be ON if the circuit is enabled, and is passing self-test. If the circuit has failed self-test, or the device is not present, the state will be OFF.

In the permanent database, this tells if DNA will try to enable the circuit.

**executor argument**

Retrieves information on the current state of the volatile database for DNA with the show executor command. The **list executor** command retrieves the data which is stored in the permanent data base for DNA.

The following lists the subcommand options or arguments you select from after you enter the show/list executor command:

**characteristics**

The detailed information on the settings of all of the adjustable arguments of the routing database.

**counters**

Gives the global event and error counters for DNA. There are no permanent counters, so the **list executor counters** command is irrelevant.

**status**

Gives key information on the state of DNA.

**summary**

Gives a brief summary on the state of DNA. This is the default.

**Example:**

```
show executor
Node Volatile Summary
Executor node = 2.26 (gato)
State = on
Identification = DECnet-MC68360 V1 R2.0 NP00523 [P10]
```

**Example:**

```
show executor characteristics
```

This example shows the full configuration of the router’s database. The **list executor characteristics** command produces essentially the same display.

```
Node Volatile Characteristics
Executor node = 2.26 (gato)
State = on
Identification = DECnet-MC68360 V1 R2.0 NP00523 [P10]
Physical address = AA-00-04-00-1A-08
Type = DEC-area
Routing version = V2.0.0
Broadcast routing timer = 180
Maximum address = 64
Maximum cost = 1022
Maximum hops = 30
Maximum visits = 63
Maximum area = 63
Max broadcast nonrouters = 64
Max broadcast routers = 32
Area maximum cost = 1022
Area maximum hops = 30
Maximum buffers = 103
Buffer size = 2038
```

**Example:**

```
list executor status
```

This example shows the status of the router in the permanent database:

```
Node Permanent Status
Executor node = 2.26 (gato)
State = on
Type = DEC-area
```

**Example:**

```
show executor counters
```

This example shows the counters that DNA keeps.
Node Volatile Counters
Executor node: 2.26 (gato)
525948 Seconds since last zeroed
0 Aged packet loss
0 Node unreachable packet loss
0 Node out-of-range packet loss
0 Oversized packet loss
0 Packet format error
0 Partial routing update loss
0 Verification reject

The following items define the fields that are displayed when you use the show/list executor command.

area maximum cost
   Maximum allowed cost to an area.

area maximum hops
   Maximum allowed hops to an area.

broadcast routing timer
   Frequency of sending routing messages in the absence of any changes.

buffer size
   Buffer size for the router.

executor node
   Node address and node name. The node name is the name set by the CONFIG set hostname command.

identification
   Identification of the router software, as sent in MOP System ID messages.

maximum area
   Highest area to which routes are kept.

maximum broadcast nonrouters
   Maximum number of end-nodes that can be adjacent to this router.

maximum broadcast routers
   Maximum number of routers that can be adjacent to this router.

maximum buffers
   Number of packet buffers in the router.

maximum cost
   Maximum allowed cost to a node.

maximum hops
   Maximum allowed hops to a node.

maximum visits
   Maximum number of routers a packet may be routed through between source and destination.

physical address
   Physical Ethernet address set on all Ethernet circuits when DNA starts. Derived from the node ID.

routing version
   Version is always Version 2.0.0.

state
   The state of DNA, on or off.

type
   Either ROUTING IV or AREA, corresponding to level 1 and level 2.
DNA IV Configuration and Monitoring Commands

module access-control circuit-specifier argument
Lists the DECnet access control lists that have been defined in the permanent database for the router, as well as the counters of their use. The options for the circuit-specifiers include the following:

all circuits
   Specifies all circuits on the router.

circuit [name]
   Specifies the named circuit.

known circuits
   Specifies all circuits on the router.

The following items are the arguments you select from after you enter the show/list module access-control command and the circuit-specifier:

counters
   Gives counters on the use of the access control lists.

status
   Shows detailed information on the access control lists, including the filters in the access control list.

summary
   Shows summary information on the state of the access control lists. This is the default.

Example:
   show module access-control circuit eth/0 counters

Example:
   list module access-control circuit eth/0 counters

Module Access-Control Volatile Counters
Circuit = Eth/0
6337   Seconds since last zeroed
   0   Packets processed
   0   Packets rejected
   0   Access control loop iterations

module routing-filter circuit-specifier argument
Lists the DECnet area routing filters that have been defined in the permanent database for the router.

all circuits
   Specifies all circuits on the router.

circuit [name]
   Specifies the named circuit.

known circuits
   Specifies all circuits on the router.

The following items are the arguments you select from after you enter the show/list module routing-filter command and the circuit-specifier:

status
   Shows detailed information on the routing filters, including the area list.

summary
   Shows summary information on the state of the routing filters. This is the default.

Example: show module routing-filter circuit eth/0 status
Zero

Use the **zero** command to clear circuit counters in the volatile database, global counters in the volatile database, and counters in the access control list module.

**Syntax:**

```
zero circuit-specifier
  executor
    module access-control circuit-specifier
```

**circuit-specifier**

- **all circuits**
  Specifies all circuits on the router.

- **circuit [name]**
  Specifies the named circuit.

- **known circuits**
  Specifies all circuits on the router.

**Example:** `zero all circuits`

**executor**

Sets all global counters in the volatile database to a zero value. There are no options.

**Example:** `zero executor`

**module access-control circuit-specifier**

- **all circuits**
  Specifies all circuits on the router.

- **circuit [name]**
  Specifies the named circuit.

**Example:** `zero module access-control all circuits`
DNA IV Configuration and Monitoring Commands
Chapter 10. Using OSI/DECnet V

This chapter describes the router’s implementation of the International Standards Organization’s (ISO) Open Systems Interconnection (OSI) Connectionless Network Layer. DECnet Phase V supports OSI (hereafter called DECnet V/OSI) and users of DNA V networks can use this chapter for information about the ISO OSI protocols. This chapter contains the following sections:

- **OSI Overview**
- “NSAP Addressing” on page 350
- “Multicast Addresses” on page 352
- “OSI Routing” on page 353
- “IS-IS Protocol” on page 353
- “ESIS Protocol” on page 361
- “X.25 Circuits for DECnet V/OSI” on page 362
- “OSI/DECnet V Configuration” on page 363
- “Accessing the OSI Configuration Environment” on page 367
- “OSI/DECnet V Configuration Commands” on page 367

### OSI Overview

An OSI network consists of interconnected subnetworks. A subnetwork consists of connected hosts referred to as end systems (ESs) and routers referred to as intermediate systems (ISs), as shown in Figure 19.

*Figure 19. OSI Network*

ESs contain all the layers of the OSI reference model and contain the host applications. ISs perform the functions of the lower three layers of the OSI reference model and handle the routing of the network protocol data units (NPDU’s) between subnetworks. ISs logically attach to the subnetwork at the subnetwork point of attachment (SNPA). The SNPA is the access point into the data link layer.

Depending on the IS configuration, each IS can run three protocols: ES-IS, IS-IS, and Connectionless-Mode Network Protocol (CLNP).
The ES-IS protocol enables the ESs and ISs attached to the same subnetwork to
dynamically discover each other’s existence. An ES connected to the same
subnetwork as an IS is adjacent to the IS. The IS-IS routing protocol enables the
ISs to do the following:
- Dynamically discover the existence and availability of adjacent ISs.
- Exchange routing information with other ISs.
- Use the exchanged routing information to calculate routes based on the shortest
  path.

The CLNP protocol is a datagram protocol that transports packets between ISs.

NSAP Addressing

The NPDU contains OSI network addresses (also called NSAPs). The NSAP refers
to a point at the network layer where the user accesses the network layer. NSAPs
are unique points within a system that represent addressable endpoints of
communication through the network layer. The number of NSAPs may vary from
system to system.

An addressing authority, such as the United States government’s National Institute
of Standards and Technology (NIST), administers NSAP addresses and determines
how the addresses are assigned and interpreted within their domain. If desirable,
these authorities may further partition the domain into subdomains and designate
corresponding authorities to administer them.

There are two NSAP addresses within the NPDU, a destination address and a
source address. Each address can vary in length from 2 octets to 20 octets and is
usually represented in hexadecimal notation. The following is an example of a
6-octet NSAP that can be entered in the OSI configuration of the router.

AA000400080C

Because the address length is variable, portions of the PDU header called
Destination Address Length Indicator and Source Address Length Indicator are used
to indicate the length, in octets, of each address.

An NSAP address consists of two parts, an Initial Domain Part (IDP) and a Domain
Specific Part (DSP) as shown in Figure 20.

<table>
<thead>
<tr>
<th>IDP</th>
<th>DSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFI</td>
<td>IDI</td>
</tr>
</tbody>
</table>

Figure 20. NSAP Address Structure

IDP

The IDP consists of two parts, the Authority and Format Identifier (AFI) and the
Initial Domain Identifier (IDI).

The AFI specifies the type of IDI and the network addressing authority responsible
for allocating the values of the IDI.

The IDI specifies both the network addressing domain from which the values of the
DSP are allocated and the network addressing authority responsible for allocating
values of the DSP from that domain.
DSP

The network addressing authority identified by the IDI determines the DSP. However, what is important is that the DSP includes specific addressing information for the domain.

IS-IS Addressing Format

The IS-IS protocol divides the NSAP address into three portions; area address, system ID, and selector (see Figure 21). The area address and system ID, together with a selector of 0, are referred to as the Network Entity Title (NET). A NET is the address of the network layer itself and is assigned when you configure an IS into the OSI network.

<table>
<thead>
<tr>
<th>IDP</th>
<th>DSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Address</td>
<td>System ID</td>
</tr>
</tbody>
</table>

Figure 21. IS-IS NSAP Addressing Interpretation

Area Address

In the IS-IS protocol, the area address is that portion of the NSAP that includes all or a portion of the IDP and the portion of the DSP up to the system ID.

The area address is that portion of the NSAP that identifies a specific area within a domain. This address must be at least 1 octet long and all ESs and ISs in the same area must have the same area address.

System ID

The system ID is that portion of the NSAP that identifies a specific system within an area. System IDs must have the following attributes:

- 1 octet to 8 octets in length.
- Equal length throughout the domain. The routers use a default configuration length of 6 octets.
- Unique for each system throughout the domain.

Selector

The selector is a 1-octet field that acts as a selector for the entity that is to receive the PDU; for example, the transport layer or the IS network layer itself. The router sets this field to 0.

GOSIP Version 2 NSAPs

Government Open Systems Interconnection Profile (GOSIP) Version 2 provides for government use the NSAP addressing format illustrated in Figure 22 on page 352. The authorities responsible for the address have clearly defined the fields and specified the addressing format under the DSP set by the National Institute of Standards and Technology (NIST).
Using OSI/DECnet V

<table>
<thead>
<tr>
<th>IDP</th>
<th>DSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFI 47</td>
<td>Ver 80</td>
</tr>
<tr>
<td>IDI 0005</td>
<td>Auth.</td>
</tr>
<tr>
<td>Reserved</td>
<td>Domain</td>
</tr>
<tr>
<td></td>
<td>Area</td>
</tr>
<tr>
<td></td>
<td>Sys. ID</td>
</tr>
<tr>
<td></td>
<td>Selector</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Figure 22. GOSIP Address Format</th>
</tr>
</thead>
</table>

**AFI**
This 1-octet field has a 47 (hexadecimal) designation. This value signifies that the address is based on the ICD format and that the DSP uses a binary syntax.

**IDI**
This 2-octet field has a 0005 (hexadecimal) designation. This value is assigned to the U.S. Government and the format has been established by NIST.

**VER**
This 1-octet field has designation of 80 (hexadecimal). This value identifies the DSP format.

**Auth. (Authority)**
This 3-octet field identifies the authority that controls the distribution of the NSAP addresses.

**Reserved**
This 2-octet field is provided to accommodate future growth.

**Domain**
This 2-octet field contains the routing domain identifier.

**Area**
This 2-octet field contains the area ID.

**Sys. ID**
This 6-octet field identifies the system.

**Selector**
This 1-octet field selects the entity to receive the NPDU.

### Multicast Addresses

Multicast addressing is the method that level 1 (L1) and level 2 (L2) ISs use to distribute link-state updates (LSUs) and hello messages to other systems or LANs. When an LSU or a hello message is multicast, a group of destination stations receive the packet. For example, an L1 LSU is multicast only to other L1 ISs. An Intermediate System Hello (ISH) is multicast only to ESs on the same subnetwork.

You can configure multicast addresses for each subnet with the `set subnet` command. [Table 106] lists the multicast addresses for Ethernet and Token-Ring LANs.

<table>
<thead>
<tr>
<th>Table 106. IS-IS Multicast Addresses</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Destination</th>
<th>Ethernet 802.3</th>
<th>Token-Ring 802.5</th>
<th>Address Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ESs</td>
<td>09002B000004</td>
<td>C00000004000</td>
<td>For all end systems on the subnetwork.</td>
</tr>
<tr>
<td>All ISs</td>
<td>09002B000005</td>
<td>C00000008000</td>
<td>For all intermediate systems on the subnetwork.</td>
</tr>
<tr>
<td>All L2 ISs</td>
<td>0180C2000015</td>
<td>C00000008000</td>
<td>For all L2 intermediate systems on the subnetwork.</td>
</tr>
<tr>
<td>All L1 ISs</td>
<td>0180C2000014</td>
<td>C00000008000</td>
<td>For all L1 intermediate systems on the subnetwork.</td>
</tr>
</tbody>
</table>
OSI Routing

OSI routes packets using the IS-IS protocol. Routing with the IS-IS protocol is based on:

- A system ID for routing within an area
- An area address for routing within a domain
- The reachable address prefix for routing outside the domain

The IS-IS protocol uses routing tables to forward packets to their correct destinations. The routing table entries are built from information in the link state database or from user-configured reachable addresses. The link state database is built from information received in the link state update (LSU). Refer to the "Link State Databases" on page 357.

IS-IS Protocol

The IS-IS protocol is a link state dynamic routing protocol that detects and learns the best routes to reachable destinations. IS-IS can quickly perceive changes in the topology of a domain, and after a short convergence period, calculate new routes. To accomplish this, the IS uses the following packets:

- Link State Updates (LSU) that the IS uses to keep the link state database information current.
- Sequence Number PDU (SNP) to keep the database synchronized and to ensure that each adjacent IS knows what the most recent Link State Packet (LSP) from each other router was.
- Hello messages that ISs use to discover, initialize, and maintain adjacencies with neighboring ISs.

IS-IS Areas

An IS-IS area is a collection of systems on contiguous subnetworks. Each area’s topology is hidden from those of the other areas to reduce routing traffic. A level 1 (L1) IS is used to route within an area. A level 2 (L2) IS is used to route between areas or over the backbone. An IS that routes within an area and over the backbone is considered an L1/L2 IS.

IS-IS Domain

An IS-IS domain is a set of rules, administered by the same authority, that all ESs and ISs must follow to ensure compatibility. There are two types of domains that require discussion, administrative domain and routing domain.

Administrative Domain
An administrative domain controls the organization of ISs into routing domains as well as the NSAP and subnetwork addresses that those routing domains use.

Routing Domain
A routing domain is a set of ISs and ESs governed by the following rules:
- All devices use the same type of routing metric.
- All devices use the same routing protocol, such as IS-IS.
Synonymous Areas
When an L1 IS services more than one area, these additional areas are called synonymous areas. A router can support any number of synonymous areas, as long as there is an overlap of at least one area address between adjacent routers. For example, in Figure 24 on page 355, Area 1 and Area 2 are synonymous areas to each other and Areas 3 and 4 are also synonymous to each other.
L1_A IS in area 2 must have area 1’s address added to its configuration and the L1 IS in area 1 must have area 2’s address added to its configuration. For areas 3 and 4 to be synonymous, each area’s address must be added to the others L1 IS.

**IS to IS Hello (IIH) Message**

The IIH message enables an IS to determine the existence of other ISs and to establish adjacencies. There are three types of IIH messages: L1, L2, and point-to-point.

Each IS contains a local hello timer and holding timer. Each time the hello timer expires, an IIH is multicast over the IS’s interface to any adjacent ISs. When the hello message is received, the recipient establishes or updates (refreshes) the adjacency information. This information remains current for amount of time (seconds) specified by the holding timer. If the holding timer expires, the adjacency is brought down.

**L1 IIH Message**

The L1 IIH message is multicast over the interface when its local hello timer expires. The L1 IS places the following information in its IIH:

- Source ID
- Any manual area addresses that it services
- IS type (L1 only, or L1/L2)
- Priority
- LAN ID
Using OSI/DECnet V

- If applicable, the system ID of the L1 designated IS (pseudonode)

Upon receiving this message, the adjacent L1 IS extracts the source ID of the sending IS. This IS then constructs its own IIH message and places its source ID into the source ID field. The sender’s source ID is placed into the IS neighbors field. Returning the sender’s ID verifies to the sender that the adjacent IS is aware that it exists (2-way adjacency).

When the first IS receives the IIH, it too extracts the source ID and looks at the IS neighbor field. Upon discovering its own source ID in the IS neighbor field, this IS establishes an adjacency with the other IS.

**Note:** Before the adjacent L1 IS can accept the packet, the packet must have a common area address and the same system ID length as the adjacent IS.

**L2 IIH Message**

The L2 IIH is multicast over its interfaces for purpose of identifying itself to other L2 ISs. The L2 IS has the same function as an L1 IIH. The L2 IS places the following information in its IIH:
- Source ID
- Any manual area addresses that it services
- IS type (L2 only or L1/L2)
- Priority
- LAN ID
- If applicable, the system ID of the L2 designated IS

**Note:** Before the adjacent L2 IS can accept the packet, the packet must have the same system ID length as the adjacent IS.

**Point-to-Point IIH Message**

A point-to-point IIH message is sent out over an IS’s non-broadcast interface (Frame Relay or X.25) to identify itself to other ISs. This IS gives the IIH to contain the following information:
- Source ID
- Any manual area addresses that it services
- IS type (L1 only, L2 only, or L1/L2)
- Local circuit ID

**Designated IS**

A designated IS is selected among all ISs connected to the same LAN to perform additional duties. In particular it generates link state updates on behalf of the LAN, treating the LAN as a pseudonode. A pseudonode is a method of modeling the entire LAN as a node on the network with fewer logical links. Minimizing logical links throughout the domain lessens the computational complexity of the link-state algorithm.

When more than one IS exists on a LAN, each IS compares the following to determine which IS will become the designated IS:
- All ISs compare their priorities. The IS with the highest priority becomes the designated IS.
- If the ISs have the same priority, they compare their source MAC addresses. The IS with the numerically highest MAC address becomes the designated IS for that LAN and is indicated through the LAN ID.
Link State Databases

Each L1 and L2 IS contains a link state database. The primary element of the database is the link state update (LSU). The router is responsible for building its own LSU and processing other ISs’ LSUs to maintain the database. The L1 database contains information on ESs. Each L1 database is identical for all L1 ISs in the same area. The L2 database contains information on areas and reachable addresses. Each L2 database is identical for all L2 ISs configured in the IS-IS domain. With information from the databases, the Dijkstra routing algorithm calculates the shortest paths to all destinations and builds the routing tables.

Link State Flooding

To ensure that each L1 and L2 IS maintains an identical database, LSUs are flooded throughout an area or a backbone. Flooding is a mechanism that an L1 or L2 IS uses to propagate an LSU to all L1 or L2 ISs. An L1 IS floods LSUs to L1 ISs only. An L2 IS floods LSUs to L2 ISs only. An L1/L2 IS accepts both L1 and L2 LSUs.

L1 Link State Update (non-pseudonode)

The L1 LSU is flooded to all L1 ISs. The L1 IS gives the LSU the following information:

- Source ID
- Any manual area addresses that it services
- IS type (L1)
- System IDs and costs of reaching IS adjacencies
- If applicable, the system IDs adjacent pseudonodes
- System IDs for any manual ES adjacencies

L1 Link State Update (pseudonode)

The L1 pseudonode LSU is flooded to all L1 ISs located in the area. Any L1 IS located on the same LAN that receives the LSU propagates the LSU to all L1 ISs adjacent on all of its other subnetworks. The L1 IS places the following information in its LSU:

- Source ID
- IS type (L1)
- System IDs and cost of reaching all non-pseudonode ISs located on the LAN
- System IDs for any ES adjacencies learned through the ES-IS protocol

L2 Link State Update (non-pseudonode)

The L2 LSU is flooded to all L2 ISs. The L2 IS places the following information in its LSU:

- Source ID
- Set of area addresses that it services
- IS type (L2)
- System IDs and the cost of reaching IS adjacencies
- If applicable, the system ID of the pseudonode
- Address prefixes for ISs located in an external domain

L2 Link State Update (pseudonode)

The L2 pseudonode LSU is multicast over the interface and propagated to all L2 ISs located outside the subnetwork. Any L2 non-pseudonode IS located on the same subnetwork that receives the LSU relays the LSU to all L2s located outside the subnetwork. The L2 IS places the following information in its LSU:

- Source ID
- IS type (L2)
- System IDs and metrics for non-pseudonode ISs located on the same subnetwork
Attached and Unattached L2 IS
An attached L2 IS is a router that knows of other areas. An unattached L2 IS is a router that does not know of any areas other than its own.

When routing, an unattached L2 IS routes packets to the closest attached L2 IS.

Routing Tables
An L1-only IS uses one routing table, the level 1 routing table. An L2-only IS contains three routing tables: an L2 area-address routing table, an L2 internal-metric reachable-address-prefix routing table, and an L2 external-metric reachable-address-prefix routing table. An L1/L2 IS contains the L1 routing table and all L2 routing tables. The routing table entries are built from information in the link state database.

L1 Routing
The following summarizes L1 routing:
1. An L1 IS receives a packet and compares the area address portion of the destination address in the header of the packet to the set of area addresses in the router.
2. If the packet is destined for the router’s area, the router extracts the system ID from the address. Searching for a match, the router compares the system ID to the system IDs in the L1 routing table.
3. If a match occurs, the IS routes the packet to the ES or the next hop IS. If no match occurs, the packet is dropped.
4. If the packet is not destined for this area, the L1 forwards the packet to the nearest L2 IS or if this router is an L1/L2 IS, it checks its L2 routing tables as described in the next section. If the L1 cannot determine where to route the packet, the packet is dropped.

L2 Routing
An L2 IS contains three routing tables: an L2 area-address routing table, an internal-metric reachable-address-prefix table (internal), and an external-metric reachable-address-prefix table (external).

The following summarizes L2 routing:
1. An L2 IS receives a packet and compares the destination address in the header of the packet to the set of area addresses in the area address routing table. If a match exists, the packet is forwarded to the next hop backbone router. If no match exists, the router checks the internal routing table.
2. The internal routing table contains entries of reachable address prefixes that lead to other domains. If the internal routing table contains a match, the packet is forwarded along the backbone to the appropriate domain. If no match exists, the router checks the external routing table.
3. The external routing table contains entries to reachable address prefixes that also lead to other domains. If the external routing table contains a match, the packet is forwarded along the path to the appropriate domain. If no match exists, the packet is dropped.

Refer to “Internal and External Routing” on page 359 for a detailed explanation of the internal and external routing tables.

Routing Metric
A routing metric is a value associated with a function of the circuit to indicate the cost of routing over that circuit. For example, the routing metric based on the
monetary expense of a circuit would use a low number to indicate a low monetary expense and high number to indicate a high monetary expense of routing a packet over that circuit.

The IS-IS routing protocol uses four routing metrics: default metric, delay metric, expense metric, and an error metric.

The current implementation of the OSI protocol uses the IS-IS default metric only. The default metric, by convention, is intended to measure the circuit’s capacity to handle traffic. All ISs in the routing domain must be capable of calculating routes based on the default metric. The other routing metrics are optional. Though they are not used by this implementation of the OSI protocol, they are described below for informational purposes only.

- The delay metric measures the transit delay of the associated circuit.
- The expense metric measures the monetary cost of utilizing the associated circuit.
- The error metric measures the residual error probability of the associated circuit.

**Internal and External Routing**

Internal or external routing involves an L2 IS routing a packet between two separate domains. When a packet needs to be routed to another domain, the L2 IS tries to match the address to a reachable address prefix in the internal or external routing table. Internal and external routes are based on the cost (routing metric) to the destination. An internal route’s cost considers the cost of routing within the domain and the cost of routing to the destination. An external route’s cost is based only on the cost of routing to the destination outside the routing domain. The IS chooses the path with the lowest cost.

For example, a packet is destined to go from node A in domain 1 to node D in domain 2 ([Figure 25 on page 360](#)). Node A can choose two paths to send the packet, to node B and then on to D or to node C and then on to D. How nodes B and C advertise the cost of their routes to D determines how node A decides to route the packet, internally or externally. There are three possible options:

- Nodes B and C advertise the cost of their routes to D as internal. The internal cost of the route A-B-D is 35 which is the cost of routing from A to B, plus the cost of routing from B to D. The internal cost of the route A-C-D is 40, which is the cost of routing from A to C, plus the cost of routing from C to D. Node A in this case would choose to route over the A-B-D path because the cost is lower.
- Nodes B and C advertise the cost of their routes as external. The external cost for A-B-D is 30 which is the cost of routing from B to D. The external cost for A-C-D is 20. Node A in this case would choose to route over the A-C-D path because the cost of this route is lower.
- Nodes B and C advertise the cost of their routes as both internal and external. The internal and external cost of the routes are added to their respective routing tables. Because internal routes are preferred over external routes, the router chooses the internal route of A-B-D.

**Note:** Because there is no exterior routing protocol, all prefix routes between domains must be statically configured.
Address Prefix Encoding

When entering address prefix routes into the router, carefully consider the difference between encoding rules for NSAPs and for prefix routes. The following four examples illustrate address prefix encoding.

Encoding a Fixed Length IDI

For many address prefixes, encoding the prefix and the corresponding NSAP is the same. For example, you are using a GOSIP 1.0 address and you want to create a route to an organization in the DoD. The Org IDI is 1234 and the DoD IDI is 0006. The encoded NSAP address is

4700061234CC...CC

The encoded address prefix is a result of the truncation of the NSAP

4700061234

The encoding rules are about all NSAP formats having a fixed length IDI and to any address prefix ending after the IDP.

Encoding an AFI

An address prefix based entirely on the AFI is encoded only on the 1 octet AFI field. For example, if an address prefix is needed for all X.121 format addresses (used on X.25 networks), you would use the X.121 AFI of 37.

Encoding a Variable Length IDI

NSAP addresses that have variable length IDI formats, such as X.121, F.69, E.163, and E.164, use a more complicated encoding scheme. When variable length IDIs are encoded as an NSAP, the address is left padded with zeros; however, when the IDI is encoded as an address prefix, there is no left padding.

For example, you want to route X.25 calls from the U.S. to an X.25 carrier in the Netherlands. The carrier has a Data Network Identifier Code (NDIC) of 2041. The encoding of the address prefix would be

372041
An X.25 subscriber having a national telephone number (NTN) of 117010 on this carrier would have an NSAP of 3700002041117010

Notice that the IDI of the NSAP is left padded with zeros to 14 digits because the resulting international data number (2041117010) was less than 14 digits.

If, however, you want an address prefix that points only to this one X.25 subscriber, the encoding would then be the NSAP (3700002041117010), because the prefix does not end in the IDP.

Default Address Prefixes
A default address prefix is used when you want to originate a default route to all addresses outside your domain. Default address prefixes are of zero length, so there is nothing to encode.

Authentication Passwords
To provide a minimum layer of security to the network, OSI provides the option of authentication passwords. When authentication is enabled, any IS-IS packet that does not contain the proper password is not accepted by the IS. The authentication field of the NPDU contains the authentication passwords. There are two types of authentication passwords, transmit and receive.

A transmit password is added to IS-IS packets transmitted by the IS. A receive password is a listing of the transmit passwords that the IS accepts. For example, with authentication enabled, if a transmit password is not added to the packet, or a listing of the transmit password is not in the receive password database, the packet is dropped. There are three types of transmit and receive passwords: domain, area, and circuit.

A domain password provides security for L2 routing information. An area password provides security for L1 routing information. A circuit password provides security for IS-IS hello messages.

ESIS Protocol
The ES-IS protocol enables ESs and ISs attached to the same subnetwork to dynamically discover each other’s existence and availability. This information also permits ESs to obtain information about each other without an available IS.

Route redirection information enables an IS to inform an ES of a better route when forwarding NPDUs to a particular destination. For example, a better route could be another IS on the same subnetwork as the ES, or the destination ES located on the same subnetwork.

Hello Message
Addressing information is passed on to ESs and ISs through hello messages.

A local configuration timer (CT) and a holding timer (HT) is present on each ES and IS. Each time the CT expires, a hello message is multicast on the LAN. When the hello message is received, the recipient sets its HT value according to the value transmitted in the HT field of the message. The recipient is expected to retain this information until the HT expires to ensure correct operation of the ES-IS protocol.
End System Hello (ESH) Message

The ESH message is multicast from the ES to all L1 ISs when its local CT expires. The ES constructs this message to inform an IS of any NSAPs that it serves. Upon receiving this message the IS extracts the NSAP and SNPA information and stores the pair in its L1 routing table, replacing any other information currently stored there.

Intermediate System Hello (ISH) Messages

The ISH message is multicast to all adjacent ESs when its local CT expires. The IS constructs this message to inform the ES of its NET. Upon receiving of this message, the ES extracts the NET and SNPA information and stores the pair in one of its local routing tables, replacing any other information currently stored there.

X.25 Circuits for DECNets V/OSI

For X.25 networks, the router establishes X.25 switched virtual circuits (SVCs) on routing circuits.

Note: To enable DECNets V/OSI for X.25, you must enter the DECNets IV process and define your router to be a DEC-AREA or DEC-ROUTING-IV router. You must do this (and restart the router!) to enable the commands to do the DECNets V/OSI configuration. Use the define executor type command.

Routing Circuits

Routing circuits are point-to-point connections between nodes that implement the ISO CLNS protocol. The router employs these types of routing circuits:

- Static incoming circuits
- Static outgoing circuits
- Dynamically assigned circuits

Static incoming and static outgoing circuits have only one SVC associated with them, and they carry both user data and non-user data (such as routing protocol messages). You bring static circuits up and down explicitly using DECNets V/OSI configuration commands. Dynamically assigned routing circuits are established upon data arrival and are cleared when there is no data being transmitted or received. A dynamically assigned circuit can have multiple SVCs, but can carry only user data.

DECNets V/OSI controls calls for each of the types of routing circuits by using filters and templates. Filters are used to process incoming calls; templates are used to establish outgoing calls.

Filters

A filter is a collection of user-configurable parameters that define the criteria for accepting all incoming calls for the specified X.25 routing circuit.

The parameters defined in a filter include the calling DTE address, a filter priority, and call/user data.

Filters and Routing Circuits

Incoming calls can be on a static incoming circuit or a dynamically assigned (DA) circuit. One or more filters may be defined for the same routing circuit. For example, a DA circuit can have multiple adjacencies and more than one filter may be defined for that routing circuit.
Filter Priorities
The list of filters for static incoming circuits and DA circuits are intermixed and ordered by descending priority. When an incoming call is received, the router searches the list of filters, highest priority first. To prevent a static circuit from being erroneously assigned to a DA circuit, it is recommended that the filters of all static circuits be assigned a higher priority than the filters of all DA circuits.

Filter Constraints on Calls
For a static incoming circuit, the filter should specify a particular calling DTE address, but the first octet of the call/user data must contain the ISO 8473 Protocol Discriminator (129). For correct operation of multiple DA circuits, additional constraints should be configured for each defined filter. This ensures that the selection criteria specified in those filters permit the required distinction to be made between incoming calls.

Note: If a DA circuit should incorrectly connect to a static circuit, the architecture makes no attempt to identify the condition or rectify the problem. The usual “initialization failure” may be generated on the static side due to non-response to its link initialization queries. The static SVC is then subsequently cleared.

Templates
A template is a collection of user configurable parameters for outgoing calls. It sets the parameters so that the circuit on the remote router accepts the incoming calls. The parameters defined in a template include the calling DTE address and the call/user data.

You can define only one template per outgoing static routing circuit.

Link Initialization
Link initialization is a procedure proprietary to Digital Equipment Corporation (and is not part of OSI). Link initialization immediately follows SVC establishment. It is used primarily to establish the DECnet relationship with a remote system on a point-to-point link.

On receipt of an Initialization/XID message, verification can be performed on two levels: on a circuit basis or on a system basis. Basically, the process of verification compares the incoming verification data against data specified locally either for the circuit or for the calling system. The verification data appears in the verification data field of the XID message.

Note: This release of the router software does not support verification by the system.

OSI/DECnet V Configuration
Note: When operating DNA IV networks together with DNA V networks, all DNA IV configuring and monitoring must be done from the DNA IV NCP> configuration process. For information on configuring DNA IV, refer to Chapter 8, Using DNA IV on page 313. The use of the term “OSI” in this chapter refers to both the OSI and DNA V environments unless indicated otherwise.
Basic Configuration Procedure

This section outlines the minimum configuration steps that you are required to perform to get the OSI/DNA V protocol up and running over a LAN (Ethernet or Token-ring), X.25 packet switching networks, and Frame Relay. Before beginning any configuration procedure, use the list device command from the config process to list the interface numbers of the different devices. If you desire any further configuration command explanations, refer to the configuration commands described in this chapter.

Note: You must restart the router for new configuration changes to take effect.

Do the following basic configuration procedure before beginning the specialized procedures described in the following sections.

Setting the network entity title (NET)

Set the router’s NET using the set network-entity-title command. The NET consists of the router’s system ID and its area address. Use the list globals command to verify that the NET is configured correctly.

Globally enabling OSI

Enable the OSI software to run on the router using the enable OSI command. Use the list globals command to verify that the OSI protocol is enabled.

Configuring OSI Over an Ethernet or a Token-Ring LAN

To configure the OSI protocol to run over an Ethernet or over a Token-Ring LAN, set the subnet. There is a one-to-one correspondence between subnetworks and interfaces. Use the set subnet command to configure all LAN subnets (Ethernet and Token-Ring). Use the default multicast addresses for Ethernet. When configuring a token-ring, use these addresses:

Parameter

- Functional Address 802.5
  - All ESs [09002B000004]
  - C00000004000
  - All ISs [09002B000005]
  - C00000008000
  - All L1 ISs [0180C2000014]
  - C00000008000
  - All L2 ISs [0180C2000015]
  - C00000008000

Use the list subnet detailed or list subnet summary command to verify that you have configured the subnets correctly.

Configuring OSI Over X.25 or Frame Relay

To configure the OSI protocol to run over the X.25 or Frame Relay interface, do the following:

Set the subnet

Use the set subnet command to set the interface to X.25 or FRL (Frame Relay). Use the defaults for all the required information. Use the list subnet detailed or list subnet summary command to verify that you have configured the subnets correctly.
Set the virtual-circuit
Use the `set virtual-circuit` command to configure an X.25 or a Frame Relay virtual circuit.

Note: The router will prompt you for a DTE address. For frame relay, enter the DLCI (Data Link Control Identifier) number. For X.25 the enter the PSN’s DTE address.

Configuring a DNA V Router for a DNA IV Environment
When configuring a DNA V router, you may need to configure an interface to run in a DNA IV environment. For example, the router is attaching to both a DNA V and DNA IV network, or a DNA IV ES is attached to a DNA V router.

Before beginning the steps below, use the appropriate preceding section to configure OSI over a LAN, X.25, or Frame Relay.
1. Enter the DN configuration process. Exit `OSI config>` and enter `NCP>`. Use the `protocol DN` command.
2. Define the global DNA address. Use the `define executor address` command to configure the DNA node and area number of the router.
3. Globally enable DNA. Use the `define executor state` command to enable the DNA protocol to run on the router.
4. Enable inter-area routing. If the L2 routing algorithm is distance vector at level 2, use the `define executor type area` command to ensure that this router can exchange DNA IV level 2 routing information.
5. Enable the DNA IV circuit. Enable the circuit that the router will use to exchange the routing information. Use the `define circuit type state on` command.

DNA IV and DNA V Algorithm Considerations
DNA IV uses a distance-vector routing algorithm. DNA V can use either a distance-vector or a link-state routing algorithm. The algorithm is selected according to what is enabled and disabled, and combinations that can result from these two protocols:

DNA IV disabled and OSI/DNA V enabled
This combination is considered a pure OSI/DNA V environment and the algorithm is automatically set to link-state at both levels 1 and 2 regardless of how the `set algorithm` command is configured.

DNA IV enabled and OSI/DNA V disabled
This combination is considered a pure DNA IV environment and the algorithm is set automatically to distance-vector regardless of how the `set algorithm` command is configured.

DNA IV enabled and OSI/DNA V enabled
This is a mixed environment and the algorithm information is configured and read out of SRAM. Use the `set algorithm` command to configure this information into SRAM.
Using OSI/DECnet V
Chapter 11. Configuring and Monitoring OSI/DECnet V

This chapter describes the OSI/DECnet V configuring and monitoring commands and includes the following sections:

- "Accessing the OSI/DECnet V Monitoring Environment" on page 391
- "OSI/DECnet V Monitoring Commands" on page 391

Accessing the OSI Configuration Environment

For information on how to access the OSI configuration environment, refer to “Getting Started (Introduction to the User Interface)” in the Software User’s Guide.

OSI/DECnet V Configuration Commands

This section summarizes and then explains the OSI configuration commands. The OSI configuration commands enable you to create or modify an OSI configuration. Enter all the OSI configuration commands following the OSI Config> prompt. Defaults for any command and its parameters are enclosed in brackets immediately following the prompt.

The configuring commands manipulate the permanent OSI database (SRAM).

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See [Getting Help] on page xxviii.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds areas this node supports; receive passwords for authentication purposes; prefix addresses for other domains; and aliases</td>
</tr>
<tr>
<td>Change</td>
<td>Modifies some parameters set up with the add command.</td>
</tr>
<tr>
<td>Clear</td>
<td>Clears a receive password, transmit password, or SRAM.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes areas, PVCs, prefix-addresses, adjacencies, aliases, subnets, and X.25 routing circuit parameters.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables a subnet, the OSI protocol, or an X.25 routing circuit.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables a subnet, the OSI protocol, or an X.25 routing circuit.</td>
</tr>
<tr>
<td>List</td>
<td>Displays the current configuration of adjacencies, aliases, passwords, pvcs, prefix-addresses, subnets, algorithm, phaseivpfx, global information, or X.25 routing circuits.</td>
</tr>
<tr>
<td>Set</td>
<td>Configures the properties associated with OSI parameters (switches, globals, NETs, timers, subnets, transmit-password, prefix-addresses, adjacencies, pvc, algorithm, and phaseivpfx).</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See [Exiting a Lower Level Environment] on page xxvii.</td>
</tr>
</tbody>
</table>

Add

Use the add command to configure area and prefix addresses, receive passwords, and address aliases.

Syntax:

```
def add  alias
  area...
  filter...
```
alias  Adds an ASCII string that designates a particular area address or system ID. The ASCII string can be a-z, A-Z, 0-9, a few other characters including the hyphen ( - ), comma ( , ), and underscore ( _ ). Do not use escape characters.

The offset indicates the position, in semi-octets (nibbles), where the ASCII string begins within the address (aliases used for system IDs have an offset of 1). The string must be the same size or longer than the segment it is designating or you will receive an invalid segment length message. The maximum allowable alias is 20 bytes.

Note: When using an alias input, you must surround it with brackets. For example: l1_update 47[newname]99999900012341234.

Example:
add alias
Alias [ ]:
Segment [ ]:
Offset [1]:
Alias    The character string you want to use
Segment   The NSAP segment that the alias is replacing
Offset    The location of the alias (in 4-bit, semi-octets) within the NSAP. The offset is determined from the beginning (left) of the NSAP as it is displayed on the terminal.

area area-addr
Adds additional area addresses (18-byte maximum) that the node supports. An L1 node that supports other areas considers those synonymous areas. One area address is the area portion of the configured NET. If you try to add a duplicate area address, the router will display an error message.

Example:
add area 4700058099999900012341234

Note: When adding synonymous areas to an L1 node, use the set globals command to configure the maximum number synonymous areas allowed for this node. All routers within an area must use the same maximum number of synonymous areas. Adjacencies can not be established if they are different.

filter filter-name routing-circuit-name calling-DTE call-UserData priority
Adds parameters upon which the router bases its acceptance of incoming X.25 calls on an routing circuit, either a static incoming or dynamically assigned (DA) circuit.

The filter-name is the name you give the filter. The routing-circuit-name is the name of the routing circuit with which the filter is associated.

The calling-DTE is the address of the calling router.

The local router checks the DTE address of an incoming call against a prioritized list of filters for all circuits. A higher filter priority in the list means...
that a connection to that filter’s calling DTE address is made first. It is recommended that you assign a higher priority to filters for static circuits than for DA circuits. This can prevent an incoming static call from being assigned a DA circuit.

The call-UserData can have one of three values - osi, dec, or user:
- For osi, the router automatically configures an ISO protocol discriminator for the call data and requires the call to be from an OSI node.
- For dec, the router expects the incoming calls to be from a Digital Equipment Company router.
- For user, you are prompted for an additional entry of up to 16 octets. Enter text to constrain the acceptance of incoming calls. The call-UserData field of the incoming call must match the specified text.

Example:
```
add filter
Filter Name [ ]:
Routing Circuit Name [ ]:
DTE Address [ ]:
Call UserData (OSI/DEC/USER):
```

If you select user, and additional prompt appears for you to enter user data, followed by a Priority prompt:

```
(max 16 octets) [ ]?
Priority (1-10) [5]?
```

*prefix-address*

Adds static routes to destinations outside the IS-IS domain. This parameter prompts you for different information depending on the type of subnet (X.25, LAN, or FRL) that was configured using the *set subnet* command.

**Note:** If no Address Prefix is entered, the default prefix is assumed.

Example:

**LAN Subnet:**
```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
MAC Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]:
```

**X.25 Subnet:**
```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
Mapping Type[Manual]:
DTE Address[]:
Default Metric[20]:
Metric Type [Internal]:
State [ON]:
```

**Frame Relay Subnet:**
```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
DTE Address []:
Default Metric [20]:
Metric Type [Internal]:
State [ON]:
```
OSI/DECnet V Configuration Commands (Talk 6)

**Note:** If the subnet does not exist, you will receive the error message:
Subnet does not exist - cannot define a reachable address.

**Interface Number**
Defines the interface over which the address is reached

**Address Prefix**
Defines the NSAP prefix (20 bytes maximum).

**MAC Address**
Defines the destination MAC address. You must specify this address if the interface corresponds to a LAN subnet. This prompt will only appear if the interface is connected to a LAN subnet.

**Mapping Type**
Defines how the destination physical address is determined, manual or X.121.

- If manual, the protocol will prompt for the DTE address.
- If X.121, the protocol will not prompt you for the DTE address.
  
- The DTE address in this instance is extracted from the NSAP.

**DTE Address**
Defines the destination DTE address. You must specify this address if the interface is X.25 and the mapping type is manual. This prompt only appears if the interface is configured for X.25 and the mapping type is manual.

**Default Metric**
Defines the cost of the address.

**Metric Type**
Defines whether the metric cost is used for external (E) routing or internal (I) routing.

**State**
When set to ON, this prefix-address is advertised to other L2 routers. When set to OFF, this is a non-functional prefix-address.

**routing-circuit**
Adds a communications channel for X.25 switched virtual circuits (SVCs) that the routing layer uses to send and receive data.

The routing circuit parameter is only applicable if you configure your router as a DEC-type router. You can specify one of these types of routing circuit:
- static-in
- static-out
- dynamically-assigned

A static-in circuit handles incoming X.25 calls. A call filter (see add filter) specifies data the router uses to accept or reject incoming calls on the circuit. A static-out circuit initiates outgoing X.25 calls. The router uses a call template (see add template) to make outgoing calls. A dynamically-assigned circuit can have multiple SVCs running simultaneously. Unlike static circuits, the router uses a dynamically-assigned circuit only when there is traffic in or out of the router. It closes the dynamically-assigned circuit upon expiration of an idle timer.

The add routing-circuit command prompts you for values for its parameters.

**Example:**

---

370  MRS V3.4 Protocol Reference V2
If you select STATIC and OUT, the following additional prompts appear:

Recall Timer (0-65535) [60]?
Max Call Attempts (0-255) [10]?
Initial Min Timer (1-65535) [55]?
Enable IS-IS [YES]?
Enable Level 2 only [NO]?
External Domain [NO]?
Default Metric [20]?
ISIS Hello Timer [3]?
Enable DECnetV Link Initialization [YES]?
Modify Receive Verifier (YES/NO) [NO]?
Explicit Receive Verification (TRUE/FALSE) [TRUE]?

If you select STATIC and IN, the following additional prompts appear:

Initial Min Timer (1-65535) [55]?
Enable IS-IS [YES]?
Enable Level 2 only [NO]?
External Domain [NO]?
Default Metric [20]?
ISIS Hello Timer [3]?
Enable DECnetV Link Initialization [YES]?
Modify Receive Verifier (YES/NO) [NO]?
Modify Transmit Verifier (YES/NO) [NO]?
Explicit Receive Verification (TRUE/FALSE) [TRUE]?

If you select DA for the circuit type, the following additional prompts appear:

Recall Timer (0-65535) [60]?
Reserve Timer (1-65536) [600]?
Idle Timer (1-65536) [30]?
Max SVCs (1-65535) [1]?

**Interface Number**
- Specifies the logical X.25 interface for this routing-circuit.

**Circuit Name**
- Sets up the alphanumeric name of this routing-circuit record.

**Circuit Type**
- Specifies whether this routing circuit is either a STATIC circuit or a DYNAMICALLY ALLOCATED circuit.

**Circuit Direction**
- Specifies IN or OUT to determine whether the SVC of the static circuit will be established with an incoming call request or an outgoing call request. In both cases, the SVC is initially established upon operator action, but the circuit is not fully enabled until both ends of the circuit have initialized successfully.

**Recall Timer**
- Defines the time in seconds that an out-static circuit or a DA circuit must wait before attempting a new call request. This is a result of the initial call request failing or a subsequent call having been cleared.

**Max Call Attempts**
- If a call request fails, Max Call Attempts defines the maximum number of subsequent call requests that are attempted by the out-static circuit before no further attempts are made. At this point, a call failure is logged and operator intervention is required to activate the out-static circuit.
**OSI/DECnet V Configuration Commands (Talk 6)**

**Initial Min Timer**
Specifies the amount of time (in seconds) an out-static circuit waits for a link to be initialized (reception of either an ESH or an ISH) after the call request has been accepted. If the initial min timer expires before the link has been fully initialized, the SVC is cleared and an event generated that indicates initialization failure.

**Enable IS-IS**
Defines whether the IS-IS protocol is enabled on this routing-circuit. When set to ON, the IS-IS protocol is enabled; when set to OFF, the IS-IS protocol is not enabled.

**Level2 Only**
Specifies if this routing-circuit is used for Level2 routing only.

**External Domain**
Specifies whether the router transmits and receives messages to and from a domain outside its IS-IS routing domain.

**Default Metric**
Defines the cost of this address.

**ISIS Hello Timer**
Defines the time interval between transmission of ISIS hellos.

**Enable DECnetV Link Initialization**
Defines whether DEC-style link initialization for this circuit is enabled (YES) or not (NO).

**Modify Receive Verifier**
Specifies verification data to be checked against on receiving an XID when verifying by circuit.

**Modify Transmit Verifier**
Specifies verification data to be included in the XID.

**Explicit Receive Verification**
Defines whether verification is by circuit or by system. TRUE specifies verification by circuit, and FALSE specifies by system.

**Reserve Timer**
Defines the time after the idle timer expires during which the router still considers a remote node on a DA circuit as "active." The router can forward data on the DA circuit until the reserve timer expires.

**Idle Timer**
Defines the length of time a DA adjacency may be idle (no data transmission) before it is cleared.

**Max SVCs**
Defines the maximum number of SVC adjacencies supported by this DA circuit. If no call can be placed because the maximum SVC adjacencies has been reached, then an event "Exceed Max SVC adjacencies" is generated.

**receive-password**
Adds an ASCII character string (16 characters maximum) that authenticates all incoming packets. An incoming packet whose password matches one of the set of receive-passwords is processed through the IS; any incoming packets whose passwords do not match are dropped.

**Example:**
```
add receive-password
```
**OSI/DECnet V Configuration Commands (Talk 6)**

**Note:** You get an error message if you use an invalid *password type*.

Password type [Domain]:
Password [ ]:
Reenter password:

**Password type**
Designates one of the two types of passwords, *domain* or *area*.
Domain passwords are used with L2 LSPs (Level 2, Link State Packets) and SNPs (Sequence Number PDU).
Area passwords are used with L1 LSPs and SNPs.

**Password**
Designates the character string that you are using for authentication. Maximum allowable string is 16 characters.

**template**

```
template template-name routing-circuit-name destination-DTE call-UserData
```

Creates a template by which the router makes outgoing calls on a static-out routing circuit. Templates for static-out circuits are analogous to filters for static-in circuits.

The *template-name* is the name you give the template. The *routing-circuit-name* is the name of the routing circuit with which the template is associated.

The *destination-DTE* is an address for the remote router of up to 14 digits. The *call-UserData* must match the call data set up for a filter on the remote circuit. *Call-UserData* can have one of three values - *osi*, *dec*, or *user*:
- For *osi* the router automatically configures an ISO protocol discriminator for the call data and requires the call to go to an OSI router.
- For *dec* the user data identifies the outgoing calls as coming from a Digital Equipment Company router.
- For *user* you are prompted for an additional entry of up to 16 octets. Enter text to match the user data of the appropriate filter on a remote router.

**Example:**
```
add template
Template Name []?
Routing Circuit Name []?
DTE Address []?
Call UserData (OSI/DEC/USER) ?
```

If you choose *user* this additional prompt appears:
```
(max 16 octets) [] ?
```
Enter up to 16 octets of text for user data.

**Change**

Allows you to modify the parameters of ISO/DNV records created in the permanent database.

**Syntax:**
```
change
  filter
  prefix-address
  routing-circuit
  template
```
filter filter-name
Changes the values for routing circuit filter parameters. You can enter a
filter name or let the router prompt you for the filter name.

The values in brackets [ ] are the current values for the parameters; the
configured value read from the permanent database.

Example: change filter
Filter Name [currentvalue]?
DTE Address [currentvalue]?
Call Userdata (OSI/DEC/USER)? [currentvalue]?

If you select user, this additional prompt appears for you to enter user data;
followed by a Priority prompt:
(max 16 octets) [currentvalue]?

prefix-address
Changes the address data for subnets. The router prompts you for the
address data.

Example: change prefix-address

LAN Subnet:
Interface Number [0]:
Address Prefix [ ]:
MAC Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?

X.25 Subnet:
Interface Number [0]:
Address Prefix [ ]:
Mapping Type [Manual]:
DTE Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?

Frame Relay Subnet:
Interface Number [0]:
Address Prefix [ ]:
DTE Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?

Interface Number
Indicates the interface over which the address is reached.

Address Prefix
Indicates the destination NSAP prefix (20 bytes maximum).

MAC Address
Indicates the destination MAC address. You must specify this
address if the interface corresponds to a LAN subnet. This prompt
will only appear if the interface is connected to a LAN subnet.

Mapping Type
Indicates how the destination physical address is determined,
manual or X.121.
If manual, the protocol prompts you for the DTE address.
If X.121, the protocol will not prompt you for the DTE address.
The DTE address in this instance is extracted from the NSAP.

DTE Address
Defines the destination DTE address. You must specify this address
if the interface is X.25 and the mapping type is manual. This prompt only appears if the interface is configured for X.25 and the mapping type is manual.

**Default Metric**
Indicates the cost of the address.

**Metric Type**
Indicates whether the metric cost is used for external (E) routing or internal (I) routing.

**State**
When set to ON, this address will receive packets. When set to OFF, this is a non-functional address.

**routing-circuit routingcircuitname**
Changes the values of the configuration for a routing circuit. You can enter a routing circuit name or let the router prompt you for a name. The values in brackets [] are the current values taken from the permanent database.

**Example: change routing-circuit**
Routing Circuit Name [currentvalue]?
Recall Timer (0-65535) [currentvalue]?
Max Call Attempts (0-255) [currentvalue]?
Initial Min Timer (1-65535) [currentvalue]?
Enable ES-IS [currentvalue]?
Enable IS-IS [currentvalue]?
Level 2 only [currentvalue]?
External Domain [currentvalue]?
Default Metric [currentvalue]?
ESIS IS Hello Timer [currentvalue]?
ISIS Hello Timer [currentvalue]?
Enable DEChetV Link Initialization [currentvalue]?
Modify Receive Verifier (YES/NO) [currentvalue]?
Modify Transmit Verifier (YES/NO) [currentvalue]?
Explicit Receive Verification (TRUE/FALSE) [currentvalue]?

**template template-name**
Changes the values of the template for a static-out routing circuits. You can enter a template name or let the router prompt you for a template name. The values in brackets [] are the current values for the parameters; the configured values read from the permanent database.

**Example: change template**
Template Name [currentvalue]?
DTE Address [currentvalue]?
Call UserData (OSI/DEC/USER)? [currentvalue]

If you select user, this additional prompt appears for you to enter your user data; followed by a Priority prompt:

(max 16 octets) [currentvalue]?
Priority (1-10) [currentvalue]?

**Clear**
Use the clear command to erase SRAM or to remove the receive or transmit password.

**Syntax:**
```
clear _receive-password
     sram
     transmit-password
```

**receive-password**
Removes all of the receive-passwords previously configured using the add receive-password command.
OSI/DECnet V Configuration Commands (Talk 6)

Note: You will receive an error message if you use an invalid password type.

Example:
```
clear receive
```
Password Type [Domain]:

Password Type
Specifies the type of password being used, Domain or Area. Refer to the `add receive-password` command for description of these passwords.

SRAM
Use this parameter to erase the OSI configuration from SRAM.

Attention: Use this command only if you intend to erase the configuration.

Example:
```
clear sram
```
Warning: All OSI SRAM Information will be erased.
Do you want to continue? (Y/N) [N]

Transmit-password
Removes the transmit-password previously configured using the `set transmit-password` command. The output for this parameter is the same as that of the receive-password parameter.

Note: You will receive an error message if you use an invalid password type.

Example:
```
clear password transmit
```
Password Type [Domain]:

Delete
Use the `delete` command to remove parameters previously configured using the `set` or `add` command.

Syntax:
```
delete
  adjacency
  alias
  area
  filter (DEC configuration only)
  prefix-address
  routing-circuit
  subnet
  template (DEC configuration only)
  virtual-circuit
```

adjacency
Removes a statically configured ES adjacency previously configured with the `set adjacency` command.

Example:
delete adjacency
Interface Number [0]?
Area Address [ ]?
System ID [ ]?

Interface number
Indicates the interface of the adjacency.

Area address
Indicates the area address of the adjacency.

System ID
Indicates the portion of the NET that identifies the adjacency within the area.

alias
Removes the ASCII string that designates a portion of an area address or system ID.

Example:
```
delete alias
```

area address
Removes the area address (address) previously configured with the add area command.

Example:
```
delete area 47000580999999000012341234
```

filter filter-name
Removes a filter record from the permanent database.

Example:
```
delete p_systems
```

prefix-address
Removes the prefix-address previously configured with the set prefix-address command.

Example: delete prefix-address
```
Interface Number [0]?
Address Prefix [ ]
```

Interface number
Indicates the interface number over which the prefix-address is configured.

Address Prefix
Indicates the destination NSAP prefix.

Interface number
Indicates the interface number over which the PVC is configured.

DTE address
Indicates the DTE address of the X.25 network to which you are connecting or the DLCI of Frame Relay network to which you are connecting.

routing-circuit routing-circuit-name
Removes an X.25 routing circuit that was established with add routing-circuit from the permanent database.

Example:
```
delete routing-circuit p_system2
```
OSI/DECnet V Configuration Commands (Talk 6)

**subnet intfc#**

Removes a subnet that was previously configured with the *set subnet* command. *Intfc#* indicates the interface number of the configured subnet.

**Example:**

```
delete subnet 1
```

**template template-name**

Removes the template for a static outgoing routing circuit by which the router generates outgoing X.25 messages from the permanent database.

**Example:**

```
delete template x25_5
```

**virtual-circuit**

Removes an X.25 or a Frame Relay virtual circuit that was previously configured with the *set virtual-circuit* command.

**Example:**

```
delete virtual-circuit
```

**Interface number [0]?**

Interface number over which the virtual circuit is configured.

**DTE address [ ]?**

DTE address of the X.25 network to which you are connecting or the DLCI of Frame Relay network to which you are connecting.

---

**Disable**

Use the *disable* command to disable those features previously enabled using the *enable* command.

**Syntax:**

```
disable
```

**osi**

Disables the OSI protocol on the router.

**routing-circuit routing-circuit-name**

Disables the specified routing circuit.

Use the *add routing-circuit* command to set up routing-circuits.

**subnet interface#**

Disables the OSI protocol on the specified subnet (*interface#*).

**Example:**

```
disable subnet 0
```

---

**Enable**

Use the *enable* command to enable the OSI protocol or an OSI subnet.

**Syntax:**

```
enable
```

**osi**

Disables the OSI protocol on the router.

**routing-circuit...**
OSI/DECnet V Configuration Commands (Talk 6)

subnet...

osi Enables the OSI protocol on the router.

routing-circuit routing-circuit-name
Enables the specified routing circuit.

Use the add routing-circuit command to set up routing-circuits.

**Example:**
```
enable routing-circuit p_system2
```

subnet interface#
Enables the OSI protocol on the specified subnet (interface#).

**Example:**
```
enable subnet 0
```

**List**

Use the list command to display the current configuration of the OSI protocol.

**Syntax:**
```
list
```

`adjacencies`

Displays all statically configured ES adjacencies.

**Example:**
```
list adjacencies
```

<table>
<thead>
<tr>
<th>Ifc</th>
<th>Area Address</th>
<th>System ID</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0001-0203-0405</td>
<td>0001-0203-0405</td>
<td>0000-0000-0000</td>
</tr>
<tr>
<td>1</td>
<td>0002-4000-0000</td>
<td>0001-0203-0405</td>
<td>0000-0000-0000</td>
</tr>
</tbody>
</table>

**Ifc** Indicates the interface number that connects to the adjacency.

**Area Address** Indicates the area address of this ES adjacency.

**System ID** Indicates the portion of the NET that identifies the adjacency.

**MAC Address** Indicates the MAC address (SNPA) of the adjacency.
OSI/DECnet V Configuration Commands (Talk 6)

**algorithm**
Displays the routing algorithm that is configured in SRAM for the DNA V protocol. If you are running the OSI protocol only, this parameter is unsupported.

**Example:**
```
list algorithm
Level 1 algorithm  LINK_STATE
Level 2 algorithm  DISTANCE_VECTOR
```

**Level 1 Algorithm**
Indicates the current configuration of the routing algorithm for level 1, Link State (default) or Distance Vector.

**Level 2 Algorithm**
Indicates the current configuration of the routing algorithm for level 2, Link State or Distance Vector (default).

**Note:** Depending on whether DNA IV is enabled or disabled, the routing algorithm displayed here may be different from what is running on the router.

**alias**
Displays the configured aliases and their corresponding address segments.

**Example:**
```
list aliases
Alias   Segment Offset
joplin  AA0004000104  1
moon    0000931004F0  1
trane   000093E0107A  1
```

**filter**
Displays the defined filters for X.25 circuits.

**Example:**
```
list filters
Rout Cir Name Filter Name  DTE Addr Pri Call Data
routeCir2  filter1   25   5  81
```

**globals**
Displays the router’s current NET, area addresses, switch settings, global parameters, and timer configuration.

**Example:**
```
list globals
DNAV State: Enabled*  Network Entity Title: 4700050001:0000931004F0
Manual Area Addresses:
1. 4700050001 2. 7700050011

Switches:
ESIS Checksum = On ESIS Init Option = Off
Authentication = Off

Globals:
IS Type = L2 System ID Length = 6
L1 LSP Size = 1492 bytes L2 LSP Size = 1492 bytes
Max IS Adj = 50 Max ES Adj = 200
Max Areas = 50 Max Ext Prefix Adds = 100
Max Ifc Prefix Adds = 100 Max Synonymous Areas = 3
Max Link State Updates = 100

OSI State or DNAV State
Indicates if the OSI or DNA V protocol is running on the router.

Network Entity Title
Indicates the area address and system ID that make up the router’s NET.

Manual Area Addresses
Areas that the router operates within. The first area address reflects
the router’s configured NET area address. Additional area addresses were added with the **add area** command.

**Globals:**
Indicates the currently configured global parameters:

**IS Type**
The router’s designation in the OSI environment: L1 or L2.

**Domain ID Length**
The size (in bytes) of the system ID portion of the NET.

*Note:* All routers throughout the domain must agree on the length of the domain ID.

**L1 LSP Size/L2 LSP Size**
Displays the L1 and L2 maximum LSP buffer size.

**Max IS Adjacencies/Max ES Adjacencies**
Displays the maximum number of ES and IS adjacencies that are allowed for all circuits.

**Max Areas**
Displays the maximum number of areas in the routing domain.

**Max ESs per Area**
Displays the maximum number of ESs allowed in one area.

**Max Int Prefix Adds**
Displays the maximum number of internal prefix addresses.

**Max Ext Prefix Adds**
Displays the maximum number of external prefix addresses.

**Max Synonymous Areas**
Displays the maximum number of level 1 areas serviced by this router.

**password**
Displays the number of transmit and receive passwords configured for each OSI Domain and Area. You configure receive passwords using the **add receive-password** command. You configure transmit passwords using the **set transmit-password** command.

**Example:**
```
list password
Number of Passwords Configured:
  -- Domain --
    Transmit = 3
    Receive = 2
  -- Area --
    Transmit = 4
    Receive = 6
```

**phaseivpfx**
Displays the configured DNA phase IV address-prefix that the OSI protocol is using to route packets to a connected DNA IV network.

**Example:**
```
list phaseivpfx
   Local Phase IV Prefix: 49
```

**prefix-address**
Displays all the SNPAs for statically configured routes.

**Example:**
list prefix:-addresses
Ifc  Type  Metric  State  Address Prefix  Dest Phys Address
0  INT  20  On  470006  302198112233
1  EXT  50  OFF  470006  302198223344

Ifc Indicates the interface number where the address can be reached.
Type Indicates the type of metric, either internal (INT) or external (EXT).
Metric Indicates the cost of the reachable address.
Address prefix Indicates the destination NSAP prefix. This prefix may be 20 bytes long.
Dest Phys Address Indicates the destination DTE address if this interface is X.25 and the configured mapping is manual.

routing-circuits Displays a summary of all routing-circuits or details of each routing circuit.

Example:
list routing circuits
Summary or Detailed [Summary]? Summary
Ifc Name  Type  Enabled
0  routecir1  STATIC-OUT  YES
0  routecir2  STATIC-IN  YES
0  routecir3  DA  YES

Summary or Detailed [Summary]? Detailed
Routing Circuit Name [] routecir2
Interface #: 0
Enabled: YES
Type: STATIC
Direction: Incoming
Initial Minimum Timer: 55
Enable IS-IS: YES
L2 Only: NO
External Domain: NO
Metric: 20
IS-IS Hello Timer: 3
DECnetV Link Initialization: YES
Receive Verifier:
Transmit Verifier:
Explicit Receive Verification: TRUE

Interface # / Ifc The logical X.25 interface for this routing-circuit.
Name The alphanumeric name of this routing-circuit record.
Enabled Indicates the state of the routing-circuit: YES for enabled, NO for disabled.
Type Indicates whether the circuit is STATIC-IN, STATIC-OUT, or DA (dynamically allocated).
Direction Indicates how the router establishes a static routing circuit: by an incoming call request (IN) or an outgoing call request (OUT).

In either case, the SVC is initially established upon operator action, but the circuit is not fully enabled until both ends of the circuit have initialized successfully.

Initial Min Timer The amount of time (in seconds) that a static-out circuit waits for a link to be initialized (reception of either an ESH or an ISH) after the call request
has been accepted. If the initial min timer expires before the link is fully initialized, the SVC is cleared and an event is generated indicating initialization failure.

Enable IS-IS
Indicates whether the IS-IS protocol is enabled on this circuit.

L2 Only
Indicates whether this routing circuit is used for Level2 routing only.

External Domain
Indicates whether the router transmits and receives messages to and from a domain outside its IS-IS routing domain.

Metric
Gives the cost of this address.

ISIS Hello Timer
Gives the time interval between transmissions of ISIS hellos.

DECnetV Link Initialization
Indicates whether DEC-style link initialization for this circuit is enabled (YES) or disabled (NO).

Receive Verifier
Displays verification data to be checked against a received XID when verifying by circuit.

Transmit Verifier
Displays verification data to be included in XIDs when verifying by circuit.

Explicit Receive Verification
Indicates whether verification is done by the circuit or the system. TRUE indicates verification by the circuit, FALSE indicates verification by the system.

Subnet subnet.reprt intfc#
Displays subnet information.

- Subnet.reprt has two options, Summary and Detailed.
  - Summary displays information for all configured subnets.
  - Detailed displays information for LAN subnets only.
- intfc# is the interface that connects to the subnet.

Example:

<table>
<thead>
<tr>
<th>Ifc</th>
<th>State</th>
<th>Type</th>
<th>ESIS</th>
<th>ISIS</th>
<th>L2 Only</th>
<th>Ext Dom</th>
<th>Metric</th>
<th>EIH (sec)</th>
<th>IIH (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>On</td>
<td>LAN</td>
<td>Enb</td>
<td>Enb</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>On</td>
<td>X25</td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>On</td>
<td>Fr1</td>
<td></td>
<td></td>
<td>False</td>
<td>True</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ifc Indicates the interface number of the subnet.

State Indicates the state of the interface, ON or OFF.

Type Indicates the type of subnet: LAN, X25.

ESIS Indicates the state of the ES-IS protocol, enabled (Enb) or disabled (Dis).

ISIS Indicates the state of the IS-IS protocol, enabled (Enb) or disabled (Dis).

L2 Only Indicates if the router is operating at level 2 only, yes (true) or no (false).
OSI/DECnet V Configuration Commands (Talk 6)

**Ext Dom**
Indicates if the router is operating outside the IS-IS routing domain (external domain).

**Metric**
Indicates the cost of using this subnet.

**EIH**
Indicates the interval at which ES hello messages are sent out over the subnet.

**IIH**
Indicates the interval at which IS hello message are sent out over the subnet.

**Example:**
```
list subnet detailed
```

```
Interface Number [0]? 0

Detailed information for subnet 0:
   ISIS Level 1 Multicast: 018002B000014
   ISIS Level 2 Multicast: 018002B000015
   All ISs Multicast: 009002B000005
   All ESs Multicast: 009002B000004
   Level 1 Priority: 64
   Level 2 Priority: 64
```

**ISIS Level 1 Multicast**
Indicates the multicast address to use when transmitting and receiving L1 IS-IS PDUs.

**ISIS Level 2 Multicast**
Indicates the multicast address to use when transmitting and receiving L2 IS-IS PDUs.

**All ISs Multicast**
Indicates the multicast address to use when receiving ES hellos.

**All ESs Multicast**
Indicates the multicast address to use when transmitting IS hellos.

**Level 1 Priority/Level 2 Priority**
Indicates the router's priority for becoming the designated router on the LAN.

**templates**
Displays a list of templates defined on this router.

**Example:**
```
list template
```

```
Route Cir Name | Template Name | DTE Addr | Call UserData
--------------|--------------|----------|----------------
  routetest2   |  temptest2    |  25      |  81
```

**timers**
Displays the OSI/DNA V timer configuration (what is running on the router, OSI, or DNA V).

**Example:**
```
list timers
```

```
Timers:
  Complete SNP (sec) = 10  Partial SNP (sec) = 2
  Min LSP Gen (sec) = 30  Max LSP Gen (sec) = 900
  Min LSP Xmt (sec) = 30  Min Br LSP Xmt (msec) = 33
  Waiting Time (sec) = 60  DR ISIS Hello (sec) = 1
  ES Config Timer (sec) = 10
```

**Timers:**
Indicates the configuration of the OSI timers excluding any per circuit timers.

**Complete SNP**
The interval between generation of complete SNPs.
Partial SNP
The minimum interval between sending partial SNPs.

Min LSP Generation/Max LSP Generation
The minimum and maximum intervals between generations of LSPs.

Min LSP Transmission
The minimum interval between LSP retransmissions.

Min Broadcast LSP Transmission
The minimum interval between LSP retransmissions on a broadcast circuit.

Waiting Time
The time the update process must delay before entering the ON state.

DR ISIS Hello
The interval between generations of IS-IS hello PDUs if this router is a designated router.

ES Config Timer
The minimum interval between that an ES must send a hello packet each time an interface comes up.

virtual-circuits
Displays information about all X.25 virtual circuits.

Example: list virtual-circuits

Set

Use the set command to configure the router to run the OSI protocol.

Syntax:
set adjacency
set algorithm
set globals
set network-entity-title
set phaseivpfx
set subnet
set switches
set timers
set transmit-password (DEC configuration only)
set virtual-circuit (IBM 2210 configuration only)

adjacency
Adds or changes an ES adjacency. Add an ES adjacency for all LAN ESs that do not run the ES-IS protocol.

Example:
set adjacency
Interface Number [0]:
Area Address [ ]:
System ID [ ]:
MAC Address [ ]:
### Interface Number
Indicates the interface number that connects to the adjacency.

### Area Address
Indicates the area where the adjacency is located.

### System ID
Indicates system ID portion of the NET that is used to identify the adjacency.

### MAC Address
Indicates the MAC address (SNPA) of the adjacency.

### algorithm

**Note:** This is a DNA phase V command. This command will work only if the DNA phase V protocol is included in the software load. This enables you to select the type of routing algorithm that you are using for the DNA routing protocol, link state (DNA V) or distance vector (DNA IV).

**Example:**
```
set algorithm
Level 1 Algorithm [link_state]?
Level 2 Algorithm [distance_vector]?
```

**Level 1 Algorithm**
Selects the type of routing algorithm, link_state (for DNA V networks) or distance_vector (for DNA IV networks).

**Level 2 Algorithm**
Selects the type of routing algorithm, link_state (for DNA V networks) or distance_vector (for DNA IV networks).

### globals
Configures the global parameters required by the OSI protocol.

**Example:**
```
set globals
IS Type [L2]:
System ID Length [6 bytes]:
Max Synonymous Areas [3]:
L1 LSP Buffer Size [1492 bytes]:
L2 LSP Buffer Size [1492 bytes]:
Max IS Adjacencies [50]:
Max ES Adjacencies [200]:
Max Areas in Domain [50]:
Max ESs per Area [500]:
Max Internal Prefix Addresses [100]:
Max External Prefix Addresses [100]:
Max Link State Updates [100]:
```

**IS Type (L1 or L2)**
Selects the level of the router, level 1 or level 2.

**System ID Length**
Selects the length of the domain ID portion of the NET. This length must be the same for all routers in same domain.

**Max Synonymous Areas**
Selects the maximum number of level 1 areas that are serviced by this router.

**L1 LSP Buffer Size**
Selects the buffer size of the level 1 LSPs and SNPs originated by the router. Range is 512 to 1492. If the interface packet size is less than what you configured here, OSI will not run, and the router generates the ELS message ISIS.053.
L2 LSP Buffer
Selects the buffer size of the level 2 LSPs and SNPs originated by the router. Range is 512 to 1492. If the interface packet size is less than what you configured here, OSI will not run, and the router generates the ELS message ISIS.053.

Max IS Adjacencies
Selects the total number of IS adjacencies allowed for all circuits. This number is used to size the IS adjacency free pool.

Max ES Adjacencies
Selects the total number of ES adjacencies allowed for all circuits. This number is used to size the ES adjacency free pool.

Max Areas in Domain
Selects the total number of areas in the routing domain. This number is used to size the L2 routing table.

Max ESs per Area
Selects the total number ESs in any one area. This number is used to size the L1 routing table.

Max Internal Reachable Addresses
Selects the number you are using to size the internal metric routing table.

Max External Reachable Addresses
Selects the number you are using to size the external metric routing table.

Max Link State Updates
Selects the number you are using to size the link state database.

network-entity-title
Configures the router’s NET. The NET consists of the router’s system ID and area address.

Example:
```
set network-entity-title
Area-address [ ]
System-ID [ ]:
```

Area-address Indicates one of area address portion of the router’s NET. It is included as the first address in the router’s set of manual area addresses. Each area address may be a maximum of 19 bytes.

System-ID Defines the portion of the NSAP that identifies this specific router. The system ID can be a maximum of 19 bytes, but the length must agree with the domain ID length that you configured with the set globals command.

phaseivpfx
Configures the prefix-address to allow the OSI protocol to route packets to the attached DNA IV network. The default is 49 (hexadecimal).

Example:
```
set phaseivpfx
Local Phase IV prefix [49]?
```
Add or changes a subnet. This parameter prompts you for different information depending on the type of subnet that you are configuring: X.25, or LAN.

**Example:**

**X.25 subnet:**

```
set subnet
Interface number [0]:
Interface Type [X25]:
```

**LAN subnet:**

```
Interface number [0]:
Interface Type [LAN]:
Enable ES-IS [N]? 
Enable IS-IS [N]? 
Level 2 Only [N]? 
External Domain [N]? 
Default Metric [20]: 
ESIS IS Hello Timer [10 sec]: 
ISIS Hello Timer [3 sec]: 
Modify Transmit password [No]?  
Modify the set of receive passwords [No]? 
L1 Priority [64]: 
L2 Priority [64]: 
All ESs [0x000000000004]: 
All ISs [0x000000000005]: 
All L1 ISs [0x0180c2000014]: 
All L2 ISs [0x0180c2000015]: 
```

**Frame Relay subnet:**

```
Interface number [0]:
Interface Type [FRL]:
```

**Interface number**

Binds the subnet to the specified interface.

**Enable ES-IS**

Indicates whether the ES-IS protocol is going to run over the interface, yes (Y) or no (N).

**Enable IS-IS**

Indicates whether the IS-IS protocol is going to run over the interface, yes (Y) or no (N).

**Interface Type**

Indicates the type of subnet: LAN, X.25, and Frame Relay (FRL). LAN includes Ethernet and Token-Ring.

**Level 2 Only**

Indicates whether the subnet should run at level 2 only, yes (Y) or no (N). A no designation allows the router to route over that subnet at both level 1 and level 2.

**External Domain**

Indicates whether the circuit is operating outside the IS-IS routing domain.

**Default Metric**

Indicates the cost of the subnet. Cost range 20–63.

**IS Hello Timer**

Indicates the period between transmissions of IS hello PDUs.

**ISIS Hello Timer**

Indicates the period between transmissions of L1 and L2 IS-IS hello PDUs.
Modify Transmit password
Removes or changes a circuit transmit password. When you select yes, this option prompts you with the following:

Delete or change the transmit password [change]?

Modify the set of receive passwords
Removes all or adds one circuit receive-password. When you select yes, this option prompts you with the following:

Delete all or add 1 receive password [add]?

L1 Priority/L2 Priority
Indicates the router priority for becoming the designated router on the LAN.

All ESs
Indicates the multicast address to use when transmitting IS hellos. The default address reflects the ethernet/802.3 multicast address. If you are connecting to a 802.5 LAN, use C00000004000.

All ISs
Indicates the multicast address to use when receiving ES hellos. The default address reflects the ethernet/802.3 multicast address. If you are connecting to a 802.5 LAN, use C00000008000.

All L1 ISs
Indicates the multicast address to use when transmitting and receiving L1 IS-IS PDUs. The default address reflects the ethernet/802.3 multicast address. If you are connecting to a 802.5 LAN, use C00000008000.

All L2 ISs
Indicates the multicast address to use when transmitting and receiving L2 IS-IS PDUs. The default address reflects the ethernet/802.3 multicast address. If you are connecting to a 802.5 LAN, use C00000008000.

switches
Turns the OSI options on or off.

Example:

set switches
ES-IS Checksum Option [OFF]?
ES-IS Init Option [OFF]?
ISIS Authentication [OFF]?

IS-IS Checksum Option
When switched on, the router generates checksums for all sourced ES-IS packets.

ES-IS Init Option
When switched on, the router sends a directed IS Hello to a new ES neighbor.

IS-IS Authentication
If switched on, each IS-IS packet includes the transmit password configured for the domain, area, and circuits. Also, no checking against receive passwords is done.

timers
Configures the OSI timers, excluding any circuit timers.

Example:
OSI/DECnet V Configuration Commands (Talk 6)

```set timers
Complete SNP [10 sec]:
Partial SNP [2 sec]:
Minimum LSP Generation [30 sec]:
Maximum LSP Generation [900 sec]:
Minimum LSP Transmission [5 sec]:
Minimum Broadcast LSP Transmission [33 msec]:
Waiting Time [60 sec]:
Designated Router ISIS Hello [1 sec]:
Suggested ES Configuration Timer (sec) [10]:
```

**Complete SNP**
Selects the interval between the generation of complete sequence number PDUs (SNP) by the designated router on a broadcast circuit.

**Partial SNP**
Selects the minimum interval between sending partial sequence number PDUs (SNP).

**Minimum LSP Generation**
Selects the minimum interval between successive generations of Link State Packets (LSPs) with the same LSP ID generated by the router.

**Maximum LSP Generation**
Selects the maximum interval between LSPs generated by the router.

**Minimum LSP Transmission**
Selects the minimum interval between retransmissions of a LSP.

**Minimum Broadcast LSP Transmission**
Selects the minimum transmission, in milliseconds, between transmission of LSPs on a broadcast circuit.

**Waiting Time**
Selects the number of seconds the update process should delay in the waiting state before entering the ON state.

**Designated Router ISIS Hello**
Selects the interval between the generation of IS-IS hello PDUs by the router if the router is the designated router on a LAN.

**Suggested ES Configuration Timer**
Sets the option field of the IS hello message that instructs the ES to change the rate at which it sends ES hellos.

```transmit-password
Sets or changes a transmit password.
```

**Example:**
```
set transmit-password
Password type [Domain]:
Password [ ]:
Reenter password:
```

**Password type**
Selects the type of password: domain or area.
- Domain passwords are used with L2 LSPs and SNPs. Area passwords are used with L1 LSPs and SNPs.

**Password**
Indicates the character string that your using for authentication. Maximum allowable string can be 16 characters.
virtual-circuit

Configures an X.25 SVC or PVC, or a Frame Relay PVC.

Example:

```
set virtual-circuit
Interface Number [0]:
DTE Address []:
Enable ISIS (Y or N) [Y]?
L2 only (Y or N) [N]?
External Domain (Y or N) [N]?
Default Metric [20]:
ISIS Hello Timer [3 sec]?
Modify transmit password (y or n) [N]?
Modify the set of receive passwords [No]?
```

**Interface Number**

Indicates the X.25 or Frame Relay interface over which the virtual circuit is configured.

**DTE Address**

Indicates the destination DTE address for X.25 or the DLCI (Data Link Control Identifier) for Frame Relay. This address must be the same as the one defined for the virtual circuit in the X.25 configuration or the Frame Relay configuration.

**Default Metric**

Indicates the cost of the circuit.

**Enable IS-IS**

Indicates whether the IS-IS protocol is going to run over the interface, yes (Y) or no (N).

**L2 only**

Indicates whether the circuit should run at level 2 only, yes (Y) or no (N). A no designation allows the router to route at both level 1 and level 2.

**External Domain**

Indicates whether the circuit is operating outside the IS-IS routing domain.

---

**Accessing the OSI/DECnet V Monitoring Environment**

For information on how to access the OSI/DECnet V monitoring environment, refer to Getting Started (Introduction to the User Interface) in the Software User’s Guide

---

**OSI/DECnet V Monitoring Commands**

This section describes the OSI/DECnet V Monitoring commands. Use these commands to gather information from the database.

The monitoring commands either display or modify the volatile database.

**Table 108. OSI/DECnet V Monitoring Commands Summary**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See [Getting Help] on page xxviii.</td>
</tr>
<tr>
<td>Addresses</td>
<td>Displays the router’s NET and area addresses.</td>
</tr>
<tr>
<td>Change Metric</td>
<td>Modifies the cost of a circuit.</td>
</tr>
<tr>
<td>CLNP-Stats</td>
<td>Displays OSI CLNP statistics.</td>
</tr>
<tr>
<td>DNAV-info</td>
<td>Displays the DNAV Level1 and Level2 routing algorithm currently in effect.</td>
</tr>
</tbody>
</table>
### OSI/DECnet V Monitoring Commands (Talk 5)

#### Table 108. OSI/DECnet V Monitoring Commands Summary (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designated-router</td>
<td>Displays the designated router for the LAN.</td>
</tr>
<tr>
<td>ES-adjacencies</td>
<td>Displays all the ES adjacencies in the adjacency database.</td>
</tr>
<tr>
<td>ES-IS-Stats</td>
<td>Displays statistics associated with the ESIS protocol.</td>
</tr>
<tr>
<td>IS-adjacencies</td>
<td>Displays all the IS adjacencies in the adjacency database.</td>
</tr>
<tr>
<td>IS-IS-Stats</td>
<td>Displays statistics associated with the ISIS protocol.</td>
</tr>
<tr>
<td>L1-routes</td>
<td>Displays all the L1 routes in the Level 1 database.</td>
</tr>
<tr>
<td>L2-route</td>
<td>Displays all the L2 routes in the Level 2 database.</td>
</tr>
<tr>
<td>L1-summary</td>
<td>Displays a summary of the level 1 link state database.</td>
</tr>
<tr>
<td>L2-summary</td>
<td>Displays a summary of the level 2 link state database.</td>
</tr>
<tr>
<td>L1-update</td>
<td>Displays the information contained in L1 link state update packet.</td>
</tr>
<tr>
<td>L2-update</td>
<td>Displays the information contained in L2 link state update packet.</td>
</tr>
<tr>
<td>Ping-1139</td>
<td>Causes the router to send an echo request to a destination and wait for a reply.</td>
</tr>
<tr>
<td>Route</td>
<td>Displays the route a packet takes to a specified destination.</td>
</tr>
<tr>
<td>Send echo packet</td>
<td>Encodes an echo request message in the CLNP packet.</td>
</tr>
<tr>
<td>Show routing circuits</td>
<td>Displays the state of user-defined routing circuits for the specified interface. Applies when the router is configured as a DEC-style router.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Displays all user-defined subnets.</td>
</tr>
<tr>
<td>Toggle</td>
<td>Enables or disables the NSAP alias substitution function.</td>
</tr>
<tr>
<td>Traceroute</td>
<td>Displays the route a packet travels to its destination.</td>
</tr>
<tr>
<td>Virtual-circuits</td>
<td>Displays all user-defined virtual circuits. Applies when the router is configured as an IBM 2210-style router.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See <a href="#">Exiting a Lower Level Environment</a> on page xxviii.</td>
</tr>
</tbody>
</table>

### Addresses

Use the **addresses** command to list the router’s NET and the area addresses configured for this router.

**Syntax:**

```plaintext
addresses
```

**Example:**

```plaintext
addresses
Network Entity Title:
4700-0500-01 000-9310-04F0
Area Addresses:
4700-0500-01
4900-02
```

**Network Entity Title**

Identifies the router. The NET consists of an area address and a system ID.

**Area Address**

Indicates addresses within the routing domain. The router can have a maximum of three area addresses configured at any one time.

### Change Metric

Use the **change metric** command to modify the cost of a circuit.

**Syntax:**

```plaintext
change metric
```

**Example:**

```plaintext
change metric
```
OSI/DECnet V Monitoring Commands (Talk 5)

change metric
Circuit [0]?
New Cost [0]?

Circuit
Indicates the circuit number that you want to change.

New Cost
Indicates the new cost of the circuit. Range: 1 to 63.

CLNP-Stats

Use the `clnp-stats` command to display the OSI Connectionless Layer Network Protocol (CLNP) statistics.

**Syntax:**

`clnp-statistics`

**Example:**

```
clnp-statistics
```

```
Received incomplete packet 0
Received packet with bad NSAP length 0
Received packet with bad checksum 0
Received packet with bad version number 0
Received packet with bad type 0
Received packet with expired lifetime 0
Received packet with bad option 0
Received packet with unknown destination 0
Received packet with no segmentation permitted 0
Received data packet cannot be forwarded 0
CLNP input queue overflow 0
No buffer available to send error packet 0
No route to send error packet 0
Received OK CLNP packet 0
Cannot forward error packet 0
ISO unknown initial protocol ID 0
Received error packet 0
Received local data packet 0
Sent error packet 0
received echo packet - destination unknown 0
cannot send an echo packet, handler error 0
sent ECHO reply packet 0
sent ECHO request packet 0
received ECHO Request 0
received ECHO reply 0
Error PDU dropped - SP, MS or E/R flag set 0
```

**Received incomplete packet**
Indicates that a data packet fragment recognized as an ISO CLNP data packet was received.

**Received packet with bad NSAP length**
Indicates that an ISO CLNP data packet was received with an incorrect NSAP length.

**Received packet with bad checksum**
Indicates that an ISO CLNP data packet was received with a bad checksum.

**Received packet with bad version number**
Indicates that an ISO CLNP data packet was received with an incorrect or unsupported version number.

**Received packet with bad type**
Indicates that an ISO CLNP data packet was received with an incorrect or unsupported type field.
Received packet with expired lifetime
Indicates that an ISO CLNP data packet was received with an expired lifetime.

Received packet with bad option
Indicates that an ISO CLNP data packet was received with a bad optional parameter.

Received packet with unknown destination
Indicates that an ISO CLNP data packet was received but could not be routed. The routing table contains no entry for the destination.

Received packet with no segmentation permitted
Indicates that an ISO CLNP data packet was received that needed segmentation. The segmentation permitted flag was not set.

Received data packet cannot be forwarded
Indicates that an ISO CLNP data packet was received but could not be routed because of a handler error.

No buffer available to send error packet
An attempt to send an ISO CLNP error packet failed because of a lack of system I/O buffers.

No route to send error packet
An attempt to send an ISO CLNP error packet failed because it could not be routed.

Received OK CLNP packet
Indicates that an ISO CLNP data packet was received and passed error checking.

Cannot forward error packet
Indicates that an ISO CLNP error packet could not be routed because of a handler error.

ISO unknown initial protocol ID
Indicates that an ISO CLNP packet was received with an unknown or unsupported initial protocol identifier.

Received error packet
Indicates that an ISO CLNP error packet was received for this router.

Received local data packet
Indicates that an ISO CLNP data packet was received with the destination NSAP indicating one of the router’s NSAPs.

Sent error packet
Indicates that ISO CLNP error packet was sent on receipt of a bad packet.

Designated-router
Use the designated-router command to display the designated router for the LAN subnets that are physically attached to this router and actively running IS-IS.

Syntax:

designated-router

Example:
designated-router

Designated Router Information:

<table>
<thead>
<tr>
<th>Hdw</th>
<th>Int#</th>
<th>Circ</th>
<th>L1DR</th>
<th>L2DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth/1</td>
<td>1</td>
<td>2</td>
<td>0000931004F002</td>
<td>0000931004F002</td>
</tr>
<tr>
<td>TKR/0</td>
<td>0</td>
<td>1</td>
<td>Elvis-01</td>
<td>Elvis-01</td>
</tr>
</tbody>
</table>

**Hdw** Indicates the type and instance of LAN attached to this router.

**Int#** Indicates the interface number of this router that attaches to the LAN.

**Circ** Indicates the circuit number assigned by the router. This number is always one more than the interface number for LAN subnets.

**L1DR** Indicates the LAN ID of the designated router. If the use of an alias is enabled, this command displays the alias of the particular segment. The LAN ID is the designated router’s system ID concatenated with a 1-byte locally-assigned circuit ID.

**L2DR** Description is the same as L1DR described above.

**Note:** If the designated router has not been elected yet, “Not Elected” will be displayed instead of a LAN ID.

---

DNNAV-info

Use the **dnv-info** command to display the routing algorithm that is currently running on the router.

**Syntax:**

```
dnav-info
```

**Example:**

```
dnav-info
DNA V Level 1 Routing Algorithm: Distance-vector
DNA V Level 2 Routing algorithm: Distance-vector
```

**Note:** Depending on whether or not DNA IV is enabled or disabled, the routing algorithm displayed here may differ from what is configured in memory using the **set algorithm** command at the OSI/DECnet V config> prompt.

If DNA IV is enabled - the routing algorithm is the one configured in memory.

If DNA IV is disabled - the routing algorithm is set to link state and may differ from that set in memory.

---

ES-Adjacencies

Use the **es-adjacencies** command to display all the End System (ES) adjacencies that are either configured or learned through the ESIS protocol.

**Syntax:**

```
es-adjacencies
```

**Example:**

```
es-adjacencies
End System Adjacencies
System ID        MAC Address     Interface   Lifetime  Type
6666-6666-6666   1234-FEAA-041C  0           50         DNAIV
```

**System ID**

The system ID of the ES adjacency.
**OSI/DECnet V Monitoring Commands (Talk 5)**

**MAC Address**
Indicates the MAC address of the ES on the subnet.

**Interface**
Indicates the router’s interface number where the ES adjacency was learned.

**Lifetime**
Indicates the amount of time, in seconds, that the router has left before the information received in the last ES Hello message is discarded. In the case of static or a manually configured ES-Adjacency, this field reads **Static**.

**Type**
Indicates the type of ES adjacency, OSI, DNAIV, DNAIV’, and MANUAL for statically configured adjacencies.

**ES-IS-Stats**

Use the `es-is-stats` command to display the statistics for the ESIS protocol.

**Syntax:**

```
es-is-stats
```

**Example:**
```
es-is-stats
ESIS input queue overflow 0
Received incomplete packet 0
Received packet with bad checksum 0
Received packet with bad version 0
Received packet with bad type 0
No lob available to send hello 0
Cannot send hello due to packet handler error 0
Sent hello 3672
Received packet with bad header 0
Received hello with bad nsap 0
Received hello packet with bad option 0
Received hello 0
Received hello with unsupported domain source 0
No resources to install route 0
Received hello with conflicting route 0
Timed out route reactivated 0
No resources to send redirect 0
Redirect not sent - handler error 0
Sent redirect 0
Timed out route 0
Timed out route 0
Unacked HI message from remote system 0
Unacked full state update from remote 0
ESIS input queue overflow
ESIS hello PPDU dropped, no matching area address 0
dropped hello packet - manual ES adjacency exists 0

ESIS input queue overflow
The ESIS packet was dropped because of a task input queue has overflowed.

Received incomplete packet
A packet fragment recognized as an ESIS packet was received.

Received packet with bad checksum
An ESIS packet with a bad checksum was received.

Received packet with bad version
An ESIS packet with a bad or unsupported version was received.

Received packet with bad type
An ESIS packet with a bad or unsupported type field was received.
**No job available to send hello**
An attempt to send an ESIS hello failed because of a lack of system I/O buffers.

**Cannot send hello due to packet handler error**
An ESIS hello could not be sent because of a handler error.

**Sent hello**
An ESIS hello was sent out an interface.

**Received packet with bad header**
An ESIS hello packet with a bad holding time or received field was received.

**Received hello with nsap**
An ESIS hello packet with a bad NSAP or an NSAP that over ran the field was received.

**Received hello packet with bad option**
An ESIS CLNP data packet was received with a bad option parameter.

**Received hello**
An ESIS hello packet was received on the interface.

**Received hello with unsupported domain source**
An ESIS hello packet was received from an unspecified domain source.

**No resources to install route**
An ESIS hello packet was received, but there were no resources to install the route.

**Received hello with conflicting route**
An ESIS hello packet was received but could not be entered into the database. A previously-defined static or dynamic route in the database conflicts with the route in the hello.

**Timed out route reactivated**
An ESIS hello packet with a previously timed out route was received.

**No resources to send redirect**
An ESIS redirect packet could not sent because of a lack of resources.

**Redirect not sent handler error**
An ESIS redirect packet could not be sent because of a handler error.

**Sent redirect**
An ESIS redirect packet was sent out the interface.

**Timed out route**
An ESIS hello route has timed out.

**Unable to allocate resources for a new ES adjacency**
An ES-IS hello packet was received but the router had insufficient resources to establish an ES adjacency with the sending node.

**hello PDU dropped, received over point-to-point circ**
An ES-IS hello packet was dropped because the circuit involved is a point-to-point circuit.

**ESIS hello PPDU dropped, no matching area address**
An ES-IS hello packet was dropped because the area did not match the router’s area address. The ES-IS protocol applies to one area only.
dropped hello packet-manual ES adjacency exists.
An ES-IS hello packet was dropped because a static ES adjacency exists with the sending node.

IS-Adjacencies

Use the **IS-adjacencies** command to list all the IS adjacencies that are learned through the ISIS protocol.

**Syntax:**

```plaintext
is-adjacencies
```

**Example:**

```
is-adjacencies
Intermediate System Adjacencies
System ID      MAC Address     Int  Level  Usage  State  Life  Type
0000-0931D-04CB AA00-0400-EF04 0 L1   L1/L2  DOWN  OSI
0000-0931D-04CB AA00-0400-EF04 0 L2   L1/L2  DOWN  DNAIV
AA00-0400-0504 AA00-0400-0504 1 L2   L2     UP    5390 OSI
```

**System ID**
The system ID of the IS adjacency.

**MAC Address**
Indicates the MAC Address of the IS adjacency.

**Int**
Indicates the router’s interface number that connects to the IS adjacency.

**Level**
For LANs this indicates the neighbor system level from type of hello message, L1 or L2. For point-to-point this indicates the neighbor system type L1 only, otherwise L2.

**Usage**
Indicates from the hello packet circuit type, L1 only, L2 only, or L1 and L2.

**State**
Indicates the operational state of the IS adjacency, up or down.

**Life**
Indicates the amount of time, in seconds, before discarding the last IS Hello message.

**Type**
Indicates the routing protocol type of the IS adjacency, OSI or DNA IV.

IS-IS-Stats

Use the **is-is-stats** command to display information associated with the ISIS protocol.

**Syntax:**

```plaintext
is-is-stats
```

**Example:**

```
is-is-stats
Link State Database Information
no. of level 1 LSPs        1  no. of level 2 LSPs        0
no. of L1 Dijkstra runs    21  no. of L2 Dijkstra runs    0
no. of L1 LSPs deleted     0  no. of L2 LSPs deleted     0
no. of routing table entries allocated 6
Packet Information
level 1 lan hellos rcvd     0  level 1 lan hellos sent  10967
level 2 lan hellos rcvd     0  level 2 lan hellos sent  10967
pnt to pnt hellos rcvd      0  pnt to pnt hellos sent   0
level 1 LSPs rcvd           0  level 1 LSPs sent        40
level 2 LSPs rcvd           0  level 2 LSPs sent        0
level 1 CSNPs rcvd          0  level 1 CSNPs sent       0
```
OSI/DECnet V Monitoring Commands (Talk 5)

<table>
<thead>
<tr>
<th></th>
<th>Level 2 CSNPs rcvd</th>
<th>Level 2 CSNPs sent</th>
<th>Level 1 PSNPs rcvd</th>
<th>Level 1 PSNPs sent</th>
<th>Level 2 PSNPs rcvd</th>
<th>Level 2 PSNPs sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>no. of level 1/level 2 LSPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of L1 and L2 link state packets that are in the database.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>no. of L1/L2 Dijkstra runs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of times the router computed the L1 and L2 routing tables.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>no. of L1/L2 LSPs deleted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of L1 and L2 link state packets that were deleted from the database.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>no. of routing table entries allocated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of entries the routing able currently holds.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level 1/level 2 lan hellos rcvd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of LAN hellos the router has received.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level 1/level 2 hellos sent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of LAN hellos that router has sent.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pnt to pnt hellos rcvd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of point-to-point hellos that the router has received.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pnt to pnt hellos sent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of point-to-point hellos that the router has sent.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level 1/level 2 LSPs rcvd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of L1 and L2 link state packets (LSPs) that the router has received.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level 1/level 2 LSPs sent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of L1 and L2 LSPs that the router has sent.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level 1/level 2 CSNPs rcvd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of L1 and L2 complete sequence number PDUs (CSNPs) that the router has received.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level 1/level 2 CSNPs sent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of L1 and L2 CSNPs that the router has sent.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level 1/level 2 PSNPs rcvd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of L1 and L2 partial sequence number PDUs (PSNPs) that the router has received.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level 1/level 2 PSNPs sent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the number of L1 and L2 PSNPs that the router has sent.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**L1-Routes**

Use the `l1-routes` command to display all the level 1 routes that are in the L1 routing database.

**Syntax:**

`l1-routes`

**Example:**

```
11-routes
Level 1 Routes
Destination System ID  Cost  Source  Next Hop
```
OSI/DECnet V Monitoring Commands (Talk 5)

```
0000-9300-0047 0 LOCArea *
AA00-0400-080C 1 ESIS AA00-0400-0C04, Ifc 7
7777-7777-7777 0 ISIS 3455-6537-2215
```

**Destination System ID**
Indicates the system ID of the destination host.

**Cost**
Indicates the cost of this route.

**Source**
Indicates the one of three sources where the router learned of the route: LOCAREA, ESIS, or ISIS.

**Next Hop**
Indicates the next hop a packet would take on its route. An asterisk (*) designation refers to the router itself as the packet’s destination. An address with an interface number is either the MAC address of a directly connected ES, or the DTE address if the next hop is an X.25 switch, or a DLCI if the next hop is Frame Relay switch. A system ID (34555372215) refers to the next hop to destination.

**L2-Routes**
Use the `l2-routes` command to display all the level 2 routes in the L2 database.

**Syntax:**
```
l2-routes
```

**Example:**
```
l2-routes
```

```
<table>
<thead>
<tr>
<th>Destination</th>
<th>Cost</th>
<th>Type</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>4700-0500-01</td>
<td>0</td>
<td>LOC-AREA</td>
<td>*</td>
</tr>
<tr>
<td>4900-02</td>
<td>20</td>
<td>AREA</td>
<td>0000-9300-04C9</td>
</tr>
</tbody>
</table>
```

**Destination**
Indicates the system ID of the destination area or reachable address.

**Cost**
Indicates the cost of this route.

**Type**
Indicates the four types of routes: LOC-area (local), LOC-prefix, area, prefix/I, and prefix/E. LOC-area is a directly connected area; a LOC-prefix is a prefix that this router advertises; prefix/I and prefix/E are routes that require another hop to reach their destination.

**Next Hop**
Indicates the next hop a packet would take on its route. An * designation, or a direct designation, refers to a directly-connected host off the router. A system ID refers to the next router the packet must pass through to reach its destination.

**L1-Summary**
Use the `l1-summary` command to display a summary of the level 1 link state database.

**Syntax:**
```
l1-summary
```

**Example:**
## 11-summary

**Link State Database Summary - Level One**

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Lifetime</th>
<th>Sequence #</th>
<th>Checksum</th>
<th>Flags</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000-9300-40B0-0000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1024</td>
</tr>
<tr>
<td>0000-93E0-107A-0000</td>
<td>384</td>
<td>CE</td>
<td>3CC9</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>AA00-0400-0504-0000</td>
<td>298</td>
<td>8E</td>
<td>4BF1</td>
<td>8</td>
<td>20</td>
</tr>
<tr>
<td>AA00-0400-0504-0100</td>
<td>4</td>
<td>BB</td>
<td>A812</td>
<td>3</td>
<td>20</td>
</tr>
</tbody>
</table>

Total Checksum 25CC

**LSP ID**

This represents the system ID of the source of the link state PDU plus two additional bytes. The first additional byte designates the type of update. 00 represents a non-psuedonode update. 01–FF represents a pseudonode update for that circuit number. The second byte represents the LSP number. This number is attached to the packet when the data is contained in more than one packet.

**Lifetime**

Indicates the amount of time, in seconds, that router will maintain the LSP.

**Sequence #**

Indicates the sequence number of the LSP.

**Checksum**

Indicates the checksum value of the LSP.

**Flags**

Indicates a one-octet value that reflects the flag field of the LSP. The eight bits are broken down as follows:

- **Bit 8** Indicates the P flag. When set (1), the issuing IS supports the optional Partition Repair function.

- **Bits 7-4**
  - Indicate the ATT flag. When set (1), the issuing IS is attached to other areas using one of the following: the Default Metric (bit 4), the Delay Metric (bit 5), the Expense Metric (bit 6), or the Error Metric (bit 7).

- **Bit 3** Indicates the LSPDBOL flag. When set (1), an LSP database overload has occurred. An LSP with this bit set is not used by the decision process to calculate routes to another 1 through the originating system.

- **Bits 2-1**
  - Indicate the IS Type flag. When set to the following values, designates the type of IS router, level 1 or level 2.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Unused.</td>
</tr>
<tr>
<td>1</td>
<td>Bit 1 set. Level 1 IS.</td>
</tr>
<tr>
<td>2</td>
<td>Unused.</td>
</tr>
<tr>
<td>3</td>
<td>Bits 1 and 2 set. Level 2 IS.</td>
</tr>
</tbody>
</table>

**Cost**

Indicates the cost of routing to that neighbor.

## L2-Summary

Use the **l2-summary** command to display a summary of the level 2 link state database.

**Syntax:**

`l2-summary`
Example:

**l2-summary**

Link State Database Summary - Level Two

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Lifetime</th>
<th>Sequence #</th>
<th>Checksum</th>
<th>Flags</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000-9310-04F0-0000</td>
<td>33E</td>
<td>12</td>
<td>EF19</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>0000-5000-F806-0000</td>
<td>455</td>
<td>4</td>
<td>2BB1</td>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td>0000-5000-F806-0100</td>
<td>469</td>
<td>12</td>
<td>DE32</td>
<td>3</td>
<td>20</td>
</tr>
</tbody>
</table>

Total Checksum 0

The description of the L2-summary output is the same as the l1-summary command.

**L1-Update**

Use the **l1-update** command to display a link state update for the specified level 1 IS.

**Syntax:**

**l1-update**

**Example:**

```
l1-update
LSP ID [? 0000931004F0000
```

Link State Update For ID 0000931004F0000

Area Addresses

470005001

Intermediate System Neighbors | Metric | Two Way
--------------------------------|--------|----------
0000931004F002                 | 20     | N        
0000931004F001                 | 20     | Y        

End System Neighbors | Metric
---------------------|--------
0000931004F0000        | *      

**LSP ID**

Indicates the system ID of the source of the link state PDU plus two additional bytes. The first byte designates the type of update. 00 represents a non-pseudonode update. 01–FF represents a pseudonode update. The second byte represents the LSP number. This number is attached to the packet when the data is contained in more than one packet.

**Area Addresses**

Indicates the area addresses in which this router is configured to route packets.

**Intermediate System Neighbors**

Indicates adjacent neighbor ISs.

**Metric**

Indicates the cost to the neighbor IS.

**Two Way**

Indicates whether the router is receiving updates from its neighbor.

**End System Neighbors**

Indicates any directly connected ESs.
L2-Update

Use the l2-update command to display the link state update for the specified level 2 IS.

Syntax:
l2-update

Example:
l2-update
LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F0000

<table>
<thead>
<tr>
<th>Intermediate System Neighbors</th>
<th>Metric</th>
<th>Two Way</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000931004F001</td>
<td>20</td>
<td>N</td>
</tr>
<tr>
<td>55002000182000</td>
<td>20</td>
<td>N</td>
</tr>
</tbody>
</table>

Intermediate System Neighbors
Indicates other directly connected ISs.

Metric  Indicates the cost to the IS.

Two Way  Indicates whether the router is receiving updates from its neighbor.

Ping-1139

Causes the router to send an echo request to a destination and wait for a reply, as recommended in RFC 1139. RFC 1139 specifies this as an OSI function and not as a DECnet function. Ping-1139 supports short- and long-term echos. Short-term echos use regular CLNP data packets, which makes them transparent to intermediate systems that do not support RFC1139. Long-term echos use PING request/reply packets.

The default data length of the echo request packet is 16 bytes. You can set the data length up to 64 bytes.

Once you enter the ping-1139 command, echo requests are sent continually until you press any key. At that time, statistics are displayed showing the number of requests transmitted and the number of replies received.

Syntax:

ping-1139

Example:

ping-1139
Long-term/Short-term [LONG-TERM]?
Destination NSAP: []? AA0003000A14
Data Length [16]?

PINGing AA0003000A14

---- PING Statistics ----
8 requests transmitted, 8 replies received

Route

Use the route command to display the next hop a packet would take to a specified destination (destnsap).
OSI/DECnet V Monitoring Commands (Talk 5)

Syntax:

```
route dest-nsap
```

Example:

```
route 490002aa0004000e08
Destination System: 0000-9310-04C9
Destination MAC Address: AA00-0400-1408
Interface: 0
```

**Destination System**
Indicates the system ID of the next hop IS. For a directly connected ES, this will be blank.

**Destination MAC Address**
Indicates the MAC address of the next hop IS or the directly-connected ES.

**Interface**
Indicates the interface that a packet would go out over to reach the next hop IS or the directly-connected ES.

Send (Echo Packet)

Use the `send echo packet` command to encode an echo request message in the CLNP packet to the specified destination nsap. During this command, the system does not interact with the OSI monitoring. To verify that the echo request was sent and that an echo reply was received, check the ELS (Event Logging System).

**Note:** You cannot send an echo packet to yourself. If you try, you will receive an CLNP.004 ELS message.

Syntax:

```
send
```

Example:

```
send
Destination NSAP: []?
```

Subnets

Use the `subnets` command to display information on all operational subnets. Subnets that are down or disabled will not be listed.

Syntax:

```
subnets
```

Example:

```
subnets
Hdw Int # Circ Only ES-IS IS-IS L1DR L1Pri L2DR L2pri Cost Ext
PPP/2 2 3 N N Y Y 64 N 64 20 N
Eth/0 0 1 N Y Y 64 N 64 20 N
```

**Hdw**
The type and instance of the network that connects to the subnet.

**Int #**
The router’s interface number that connects to the subnet.

**Circ**
The circuit assigned ID for the ISIS protocol.

**L2 only**
Whether this router is a level 2 router only, Y (yes) or N (no).
OSI/DECnet V Monitoring Commands (Talk 5)

ES-IS  The ES-IS protocol is enabled on the subnet, Y or N.
IS-IS  The IS-IS protocol is enabled on the subnet, Y or N.
L1DR  This router is the level 1 designated router for this subnet, Y or N.
L1Pri  The subnet’s level 1 priority for becoming the designated router.
L2DR  This router is the level 2 designated router for this subnet, Y or N.
L2Pri  The LAN subnet’s level 2 priority for becoming the designated router.
Cost  The cost of the circuit.
Ext  Whether the subnet is operating outside the IS-IS routing domain (external).

Toggle (Alias/No Alias)

Use the toggle alias/no alias command to enable or disable the NSAP alias display function for the OSI protocol.

Syntax:

toggle

Example:

toggle
Alias substitution is ON

Traceroute

Use the traceroute command to track the path an OSI packet takes to a destination.

Note: You cannot do a traceroute to yourself or you will receive the following error message:
Sorry, can’t traceroute to this router.

Syntax:

traceroute address

Example:

traceroute 490002aa0004000e08
Successful trace:
TRACEROUTE 470007: 56 databytes
1 490002aa0004000e08 32ms 5ms 5ms
Destination unreachable response:
Destination unreachable
No response:
1 * * *
2 * * *

TRACEROUTE
Displays the destination area address and the size of the packet being sent to that address.

1  The first trace showing the destination’s NSAP and the amount of time it took the packet to arrive at the destination. The packet is traced three times.
OSI/DECnet V Monitoring Commands (Talk 5)

**Destination unreachable**
Indicates that no route to destination is available.

1 ***

2 *** Indicates that the router is expecting some form of response from the destination, but the destination is not responding. The router will wait 32 hops before timing out. Go to the ELS and turn on OSI CLNP messages to determine why the host is not responding.
Chapter 12. Using NHRP

This chapter describes how to use:

- Next Hop Resolution Protocol (NHRP) as specified in Internet Draft Version 13, which has been submitted for RFC status.

Next Hop Resolution Protocol (NHRP) Overview

The Next Hop Resolution Protocol (NHRP) defines a method for a source station to determine the Non-Broadcast Multi-Access (NBMA) address of the “next hop” towards a destination. The NBMA next hop may be the destination itself or the egress router from the NBMA network that is “nearest” to the destination station. This “next hop” information is called a “cut-through” route or VC in the NHRP specification; the router uses the term “shortcut” instead of “cut-through”. The source station can then establish an NBMA virtual circuit directly with the destination or the egress router and reduce the number of hops through the network.

The 2210 can use NHRP to establish shortcuts for IP traffic over the ATM NBMA network for both RFC 1483 and Emulated LAN (ELAN) interfaces. The Internet draft does not address the use of NHRP in an ELAN environment, but the 2210 includes enhancements to allow using LANs. These enhancements are currently implemented using the vendor-private extensions included in the NHRP protocol definition.

The NHRP draft describes the basic protocol flow as follows: NHRP clients register their protocol addresses and their NBMA addresses with one or more NHRP servers. The servers are typically routers on the routed path through the NBMA network to the clients. When a client wants to establish a shortcut to a destination, it sends a Next Hop Resolution Request packet along the routed path. The request...
includes the destination protocol address. The routers (that are also NHRP servers) along the routed path first check to see if the destination protocol address is an address that it can serve.

If the router can satisfy the request, the router returns a Next Hop Resolution Reply with the NBMA address of the destination station. The originator can then establish a direct virtual circuit with the destination. If it cannot satisfy the request, the router forwards the request to the next-hop router. This forwarding continues until the request can be satisfied, or it is determined that the destination cannot be reached.

To use client/server terminology, a device may be both a client and a server. The client is the device that originates Next Hop Resolution Requests, and the server is the one that provides Next Hop Resolution Replies with NBMA address information. The 2210 is such a device; the client conceptually “registers” with the server function in the same machine, although no Registration Requests actually flow. The server also supports NHRP Registrations from remote NHRP clients.

The information provided by clients to their server, and by servers to requestors, must be refreshed periodically and may be purged if conditions dictate. Clients and Servers maintain caches of resolution information that they have sent and received; holding times are used to age out the entries or force refreshes.

Benefits of NHRP and the IBM implementation

In general, use of NHRP shortcuts can:

• Improve end-to-end performance, by eliminating hops between routers when the source and destination are on the same NBMA network and can communicate directly
• Reduce the load on network routers, since they are bypassed for traffic that, without NHRP, would be handled by the router. This can reduce overall costs as fewer routers or less bandwidth may be needed.

The IBM implementation of NHRP provides these additional benefits:

• The NHRP draft does not address using the protocol in an Emulated LAN environment. However, the IBM implementation of NHRP includes considerations for such environments; NHRP packets can flow between routers over ELAN connections, and shortcut VCs can be established.
• One-hop Routing: ATM devices that do not support NHRP can be the destination of shortcut paths, eliminating another router hop for traffic, by expanding the definition of the devices that are “served” to include devices that share a protocol subnetwork with the server. For example, all IP addresses on a classical IP subnet that a server is part of, are “served” by that server. The NHRP function interfaces with classical IP 1577 and LAN Emulation components to use their existing ATM address resolution capabilities and apply them to NHRP requests. This enhancement can even be used for traffic to legacy LAN-attached devices that connect to ATM through LAN switches; the NHRP server in the router replies to the client with ATM addressing information for the LAN switch, allowing the client to shortcut directly to that switch. For examples of these “one-hop routing” cases, see Figure 26 on page 407 and Figure 27 on page 410

Note: A hop is an operation performed by a traditional router when forwarding packets from one subnet to another. In particular those operations are (1) doing a lookup on a Layer 3 subnet identifier (2) determining the outbound “next hop” for the packet (3) stripping and replacing the Layer 2 packet header, removing ingress link information and adding egress link
information. So, for “one-hop” routing this operation happens once during transfer of a packet from its source to its destination.

- The IBM implementation can operate in networks where some routers do not support NHRP. If the next-hop router is not capable of providing NHRP support, shortcut VCs can be established to the “last” server in the path. See Disallowed Router-to-Router Shortcuts on page 417 and Exclude Lists on page 416.

- The customer may configure the 2210 to establish shortcuts only when traffic to a destination exceeds a given data rate. This can eliminate the creation of VCs for low volume or one-time traffic (for example, SNMP traps). See “data-rate parameter” on page 428 and “attempt shortcuts? parameter” on page 427.

- The router provides solutions for the “domino” effect that is described in the NHRP draft. See “attempt shortcuts? parameter” on page 427.

- All ATM-attached routers on the routed path should support NHRP for the optimal benefit, although the 2210 can still operate and provide shortcuts in a mixed network.

Performance Characteristics

NHRP is used during initial contact from a source device to a destination. Once a shortcut VC has been established, NHRP is not involved in actual data transfer. Safeguards ensure that NHRP traffic is not retried for every packet. Also, the IBM implementation provides an option for NHRP shortcuts to be requested only when traffic to a certain destination exceeds a configurable data rate threshold. This can prevent, for example, the establishment of virtual circuits that would only be used for one SNMP trap frame that is generated by an IP host.

NHRP operation does not affect the performance of the router fastpath and will not significantly affect the slowpath. When shortcuts are available, the performance is improved by the elimination of extraneous hops over the ATM network. Also, the performance of intermediate routers that are bypassed by NHRP shortcuts should be improved, as they handle less traffic.

Note: If a configuration does not include a 1577 interface (that is, the router is configured only for ELANs), shortcut VCs can be established to the router only from clients that support the IBM extensions. This limitation can be avoided simply by defining a 1577 interface on the router.

Examples of NHRP Configurations

The following paragraphs give examples of NHRP configurations.

**NHRP in an RFC 1577 Classic IP Environment with All Devices NHRP-capable**

In this picture, the NHRP clients use RFC 1577 connections to communicate with the router. They use NHRP protocol to learn from the NHRP server about each other’s ATM addresses. Then they establish a direct virtual circuit between them for IP traffic.
Using NHRP

**NHRP in a Classic IP Environment with non-NHRP Device**

This example shows how NHRP can be used between two 1577 devices. When one of them does not support NHRP. Here, Device2 provides the NHRP client with the ATM address of the non-NHRP device and the client can establish a shortcut for traffic to the non-NHRP host. However, when traffic flows from the non-NHRP device, it flows on the routed path to Device2; then Device2 acts as an NHRP client and establishes a shortcut to the destination.

**Figure 27. NHRP in a Classic IP Environment**

**Figure 28. NHRP in a Classic IP Environment with non-NHRP Device**
NHRP in a Pure LAN Emulation Environment

In the LAN emulation case, routers use the IBM extensions to provide NBMA information for devices on their ELANs. When Device1 receives traffic from host A destined to host B, it originates a Next Hop Resolution Request and sends it on the routed path. Device2 replies to the request with NBMA information about host B, one of the stations that it serves because they are on the same ELAN. Device1 then can establish a data direct VCC to host B even though host B does not participate in or support the NHRP exchanges. Note that this VCC would be used only for traffic in the direction from A to B. Similarly when host B sends traffic to host A, Device2 generates a Next Hop Resolution Request, Device1 replies with addressing information about host A, and Device2 establishes a data direct VCC to A for traffic from B to A.

The LECs in this example are standard-compliant devices with no NHRP support. They must satisfy the LEC requirements described in “NHRP Implementation” on page 414.

Nothing special has to be configured in these devices or in the NHRP servers. The NHRP traffic flows over the ELAN subnet with no additional VCs.

NHRP in a LAN Emulation Environment with LAN Switches

In this example, the source and destination stations are attached to legacy LANs and do not connect to the ATM network. LAN switches operating as LAN Emulation Clients give ATM connectivity to the legacy LAN devices. The enhancements to NHRP and the IBM extensions allow the same kind of “one-hop routing” in this environment as described in the previous example. With the enhancements, the servers exchange the actual MAC addresses and routing information for the legacy-LAN devices. The 2210s can then establish data direct VCCs with the switches and pass the traffic directly. There is only one router “hop” in the path, although the traffic passes through two LAN switches.
Using NHRP

This example also illustrates that the ELAN environment can be token-ring or Ethernet or any mixture of LAN types.

NHRP in a Mixed Classical IP and ELAN Environment

The NHRP function in the router can operate with both Classic IP and ELAN interfaces in the same network. In this example, the NHRP client supports the IBM extensions and can shortcut directly to the LEC destination for traffic in that direction.
NHRP to an Egress Router

The source and/or destination stations of protocol traffic do not have to belong to subnets served by NHRP participants. They may access the ATM network via routers that communicate with the NHRP devices. In this case, the 2210 provides shortcuts through the ATM network to eliminate as many hops as possible.

Figure 31. NHRP in a Mixed Classical IP and ELAN Environment

NHRP to an Egress Router

Figure 32. NHRP to an Egress Router
NHRP interacts with the router function in the router. When the router function in the router is forwarding packets along the routed path and NHRP successfully obtains a shortcut VC, NHRP will update the router function to send the packet directly over the shortcut VC.

NHRP updates the routing function’s forwarding table after the VC is up. This allows the switch from routed path to the shortcut path to occur without any packet loss.

When an NHRP shortcut is used, the router transmits frames to a next hop address on a subnetwork that the router itself is not a part of. So the NET, or interface, that provides the outbound path for the traffic is called a “virtual” network interface.

**Virtual Network Interface (VNI)**

Normally, outbound packet flow from a router is constrained by the following:

- Inability to send packets directly to network addresses that are not defined on a network interface.
- Inability to send packets to network types (for example, token-ring ELAN) unless that network type is defined on a network interface.

The Virtual Network Interface (VNI) net-handler removes all of these constraints, which allows the router to forward packets directly to next hops obtained via NHRP (shortcut routes). It enables one-hop routing, where NHRP shortcut routes can be made directly to devices that do not support NHRP.

The VNI supports token-ring, Ethernet V2 and Ethernet DIX ELAN network interfaces and classic IP network interfaces. When the outbound path is to use a classic IP (1577) interface, the implementation actually uses the existing 1577 net-handler interface for the VNI. However, when the outbound path is to use a LANE shortcut, a unique interface is accessed. This is called the LANE Shortcut Interface (LSI). The LSI is different from a traditional LEC interface because it can provide more than one LAN encapsulation type; that is, one VC may be established using token-ring encapsulation while another uses Ethernet V2. Also the LSI provides connections to more than one Emulated LAN; a traditional LEC interface connects to only one ELAN.

When you enable NHRP, an LSI is created for each ATM adapter. The LSI is assigned the next available interface number, and will be listed when you invoke console functions that display information about the router interfaces.

**LANE Shortcut Interface (LSI)**

The LANE shortcuts provided by the IBM extensions to NHRP are not compatible with some LAN Emulation Client (LEC) and end-station protocol stack implementations. This section describes how these incompatibilities can arise and, in some cases, how they can be overcome using configuration options.

Paranoid LECs are devices that use the LAN Emulation Flush Protocol to verify that clients setting up Data Direct VCCs to it are actually members of its ELAN. These devices will not work with NHRP shortcuts generated by LSIs since the LSI is not part of the target ELAN.

**Note:** The “Exclude List” configuration option can be used to prevent shortcuts to Paranoid LECs as described in "Exclude Lists" on page 416.
By default, the LSI will use the MAC address burned into the associated ATM adapter as the source MAC address of frames transmitted over the LANE shortcut VCCs. It is possible, though unlikely, that this could confuse some end-station protocol stack implementations, since the MAC address will not match that of the router that the end-station uses as a gateway to transmit packets to the associated IP address.

For this to happen, the end-station would have to learn router MAC addresses from unicast IP frames which is not normal (IP-to-MAC address mappings are normally learned from ARP packets). If this were to happen, the end-station might use the learned MAC address as the destination MAC address of frames that it transmits to the associated IP destination instead of using the MAC address of the router. Such frames would either be dropped or forwarded over the LANE shortcut VCC. Forwarding would only occur if the LEC learns MAC-to-ATM address binding from received frames (which is an optional implementation choice).

In either case, these frames will not reach the destination since the LSI discards frames received over a LANE shortcut VCC. Furthermore, the LSI releases the LANE shortcut VCC and no further shortcuts will be established to the associated ATM address. Traffic for destinations associated with that ATM address will follow the routed path thereafter. Note that ELS messages and console display for LANE shortcuts aid in identifying these destinations.

The LSI can be configured not to use the universally administered MAC address as the source MAC address. With this option, you have two choices for the source MAC address:

1. You can use the MAC address of the last-hop router, provided in the NHRP resolution reply packet, as the source MAC address. Using the last-hop router’s MAC address as the source MAC address solves the problem of end-station protocol stack confusion but introduces another potential problem. It may confuse LECs that learn MAC-to-ATM address binding from received frames, and therefore should not be used with LECs that perform this type of learning. For example, the LEC in IBM’s 8281 ATM-LAN bridge performs this type of learning.

2. You can configure the source MAC address. The source MAC address can be configured to avoid the problem of duplicate MAC addresses seen on an ELAN because of inter-ELAN shortcuts. The MAC address should be configured for this LSI network when there are any disallowed LANE shortcut entries. See “LANE Shortcuts” on page 433 for details on displaying disallowed LANE shortcut entries.

These configuration options are provided to maximize flexibility in achieving compatibility with the largest possible set of destinations in a given installation. See “Configuring the LANE Shortcuts Interface (LSI)” on page 419 and “Change” on page 423 for a description of the change command.

Configuration Parameters

This section describes some of the NHRP related configuration parameters and their recommended usage. See “NHRP Configuration Commands” on page 421 for command syntax, command parameters, valid values and default values.
Using NHRP

NHRP Auto-Configuration
NHRP is enabled by default if IP is present in the box. It can be disabled by entering the disable NHRP command from the NHRP config> prompt. See [Accessing the NHRP Configuration Process](#) for additional information.

When using an existing configuration file, NHRP is enabled by default if it was not previously configured. The configuration file will be automatically updated at runtime to create NHRP shortcut interfaces. You need to save this updated configuration file and reboot in order for the NHRP client to use LANE shortcuts.

Exclude Lists
Configuration allows you to create a list of protocol addresses (and associated masks) that represent two types of devices:

- Next-hop routers that do not contain an NHRP server function
- Destination devices to which shortcut VCs should not be allowed

**Next-hop Routers:** The exclude list can be used to identify routers that are on the routed path but do not support NHRP server function.

The server responds to a Next Hop Resolution Request by providing the ATM address of the next-hop router when all of the following are true:

- The next-hop address is different from the destination address.
- The router interface to the next-hop router is either an ATM classical IP or an ELAN subnet.
- The next-hop address is in the exclude list.

In processing the request, the router does not forward the Resolution Request on to the next-hop address, but responds to the client with addressing information that allows the client to establish a shortcut VC to the next-hop router.

**Note:** If the next-hop router is one of the Disallowed R2R Shortcuts, the router sends a NAK to the Resolution Request instead of a positive reply.

In general, if the next-hop router is on the exclude list, the router does not send it any NHRP packets that would only be handled by an NHRP server.

**Destination Devices:** The exclude list can also be used to prevent shortcut VCs to a given protocol address (for example, a device on a CIP or ELAN subnet that can support only a small number of VCs).

When processing a Next Hop Resolution Request for a destination device, the server responds to the client with addressing information that allows the client to establish a shortcut VC to the router itself when all of the following are true:

- The next-hop address equals the destination address.
- The router interface to the destination is either an ATM classical IP or an ELAN subnet.
- The destination address is in the exclude list.

Extensions
The NHRP protocol includes Extensions. Extensions are appended to NHRP packets. Extensions are used to request additional functions from the NHRP participants. The use of the extensions parameter lets you determine if the router sends certain extensions:

- path information extensions
IBM vendor-private extensions

Path Information Extensions: Three extensions are defined in NHRP to provide path information. These extensions can be used to help monitor the request itself, to determine the path taken by the request, to determine who generated the reply, and the path taken by the reply. The path information extensions are:

- Forward Transmit - Each Next-Hop Server (NHS) that forwards the request along the way should append information about itself.
- Responder Address - The Next-Hop Server (NHS) that generates the reply should append information about itself.
- Reverse Transmit - Each Next-Hop Server (NHS) that forwards the reply along the way should append information about itself.

The router can be configured to send any or all of these extensions in Next Hop Resolution Request packets that it generates. The information received in the reply packets is displayed in the router’s NHRP ELS messages.

IBM Vendor-Private Extensions: To support NHRP in an Emulated LAN environment, the server adds vendor-unique extensions to NHRP packets. These extensions act as “queries”; the NHRP client places them in the Next Hop Resolution Request. If the server supports this function, it responds with three corresponding extensions containing ELAN address information (MAC address, ATM address and Routing information); these extensions are included in the Next Hop Resolution Reply.

The router can be configured so that it does not support the IBM-specific extensions. If the IBM specific extensions are not used, shortcuts directly to ELAN devices are not possible. Use the “Exclude List” option to disallow shortcuts selectively to certain ELAN devices.

Disallowed Router-to-Router Shortcuts
Operation of NHRP may result in establishing transit paths across NBMA network between routers. However, establishing an NHRP shortcut across a boundary where information used in route selection is lost may result in a routing loop. Such situations include the loss of BGP path vector information, and the interworking of multiple routing protocols with dissimilar metrics. Under such circumstances, NHRP shortcuts between routers should be disallowed. This situation can be avoided if there are no “back door” paths between the entry and egress router outside the NBMA network.

The server allows router-to-router (R2R) shortcuts by default. However, by configuring disallowed R2R shortcuts, you can create a list of destination or router addresses for which the router does not allow shortcuts.

To create a disallowed R2R shortcut, you must specify both a protocol address and a mask. The protocol address is either the destination or a router, and the mask allows for a range of addresses.

To illustrate how to specify disallowed R2R shortcuts using protocol addresses and masks, consider the following network diagram:
Using NHRP

Example 1: An entry with address=9.9.9.1 mask=255.255.255.255 would cause the NHS to send a NAK to the sender of a Next Hop Resolution Request with destination protocol address 9.9.9.1 (HOST1). Since 9.9.9.1 is not directly attached to one of the device subnets, but is reached by another router, the router checks the Disallowed R2R Shortcuts List.

Example 2: An entry with address=9.9.9.0 mask=255.255.255.0 would cause the router to send a NAK for any destination address 9.9.9.1 through 9.9.9.255. HOST1, HOST2, and ROUTER2 could not be reached using shortcuts to the router but devices on the other subnets serviced by ROUTER2 could be reached.

Example 3: An entry with address=1.1.1.5 mask=255.255.255.255 would cause the router to respond negatively for any destination whose next-hop router is 1.1.1.5, ROUTER1. The router would respond negatively for any address on subnet 9.9.9 and for any address on the other IP subnets reached via router 9.9.9.3 because next hop is 1.1.1.5.

Example 4: An entry with address=anything mask=0.0.0.0 would disable R2R shortcuts for all addresses.

Protocol Access Control Usage
This parameter determines if the protocol layer access controls will be checked and, if so, how these controls will be applied to NHRP packets.

If this configuration parameter is set to its default value of none, the protocol layer access controls are not checked.

With the value of source and destination, when the NHRP requester is not a router, the NHRP client’s IP address is assumed to be the source of all IP packets that will be transmitted by that client using the NHRP shortcut route. The router denies NHRP shortcut requests from a non-router NHRP client if any IP packets are being filtered for that IP destination/source address pair, where the source is the NHRP client’s address.

Selecting the destination only option causes the router to deny shortcut requests from any NHRP client if any IP packets are being filtered to the destination address. If NHRP clients should not be trusted, destination only should be selected.
destination only might be the best option when NHRP clients are non-routers with multiple IP addresses or non-router clients that transmit packet that originate from other sources.

NHRP clients that reside in the routers use the NHRP shortcut routes to forward packets from other sources: therefore, if source and destination is configured and the router receives a shortcut request from a router, the router applies the IP filters the same way as when destination only is selected.

**NHRP Access Controls**

NHRP access controls for denying shortcuts to certain IP addresses may be defined by adding those addresses to both the exclude list and disallowed-router-to-router shortcuts.

**ATM Network ID**

Since an server may have more than one ATM adapter, it may be connected to two different or unassociated networks. This must be considered when deciding when shortcut VCs should be allowed.

You can determine which interfaces should be treated as if they are connected to the same physical ATM network by assigning each ATM interface a Network-ID by using the set command at the ATM Interface Config> prompt as described in the “Using and Configuring ATM” chapter in Software User’s Guide.

ATM interfaces with the same Network-ID are considered to belong to the same network. By default, all ATM interfaces are assigned to Network-ID 0.

**Configuring the LANE Shortcuts Interface (LSI)**

The NHRP LANE Shortcut Interface (LSI) is automatically created for each ATM adapter when NHRP is enabled for the router. The LSI uses default values for the following parameters.

- ESI
- Selector
- Use Best Effort Service for Data VCCs
- Peak Cell Rate of outbound Data VCCs
- Sustained Cell Rate of outbound VCCs
- Use ATM adapter’s universally administered MAC address for source

The default values may be modified using the change command from the NHRP Advanced config> prompt. See [Change](#) on page 425.

**Configuring Devices in an ATM Network**

If you have a NHRP client/server and its configuration requires you to give the ATM address of the router NHRP server, you must select the proper ATM address. You must use an address associated with an “ATM interface” in the device, and an IP address must be assigned to this interface. The last two digits of the router ATM address, the selector, are assigned dynamically after the router is activated (and may change if the configuration of the router changes), unless you have configured a specific selector.

You can specify the ATM address, including selector, by entering prot arp at the talk 6 Config> prompt, followed by add atm, giving the desired IP address and then specifying a selector. This is the same procedure used to define an ATMARP client.
Using NHRP with LAN Emulation

If you want to use NHRP on the device, you must configure all LECs with a unique locally administered MAC address (LAA). If you do not configure the LECs with unique LAAs, the NHRP shortcut capability to the corresponding switch or device will not work because:

- Traffic sent over an NHRP LANE shortcut VCC will contain the router Universally Administered (universally administered) MAC address as the source MAC address.
- Some network devices learn the association between the MAC address and the VCC from traffic the device has received. These devices then use the NHRP VCC to transmit data.
- If the router detects incoming traffic on an NHRP VCC, it will assume that an error condition has occurred and will shut down that VCC, preventing any further shortcuts to that network device.

**Note:** By default, the router enables LAN Emulation Extensions on NHRP, so you must either disable the extensions or configure the unique locally administered MAC address for each LEC.
Chapter 13. Configuring and Monitoring NHRP

This chapter describes how to configure and monitor the Next Hop Resolution Protocol (NHRP). For a description of this protocol, refer to “Next Hop Resolution Protocol (NHRP) Overview” on page 407.

This chapter contains the following sections:
- “Accessing the NHRP Configuration Process”
- “NHRP Configuration Commands”
- “Accessing the NHRP Monitoring Process” on page 430
- “NHRP Monitoring Commands” on page 430
- “NHRP Packet Tracing” on page 436
- “NHRP Server Dynamic Reconfiguration Support” on page 436

Accessing the NHRP Configuration Process

To access the NHRP configuration:
1. At the operator monitoring prompt (*), type talk 6 and press enter.
2. At the config> prompt, type protocol nhrp and press enter.
3. The NHRP config> prompt is displayed.

NHRP Configuration Commands

This section explains all of the NHRP configuration commands as shown in Table 109. Enter the commands at the NHRP config> prompt.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page xxviii.</td>
</tr>
<tr>
<td>Enable NHRP</td>
<td>Turns on NHRP for all interfaces that are not explicitly defined.</td>
</tr>
<tr>
<td>Disable NHRP</td>
<td>Turns off NHRP for all interfaces that are not explicitly defined.</td>
</tr>
<tr>
<td>List</td>
<td>Displays the NHRP configuration.</td>
</tr>
<tr>
<td>Advanced config</td>
<td>Gets you to the NHRP Advanced config&gt; prompt, from which you can enter other commands as described in “NHRP Advanced Configuration Commands” on page 423.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxviii.</td>
</tr>
</tbody>
</table>

Enable NHRP

Use the enable command to enable NHRP on all interfaces not explicitly defined using an NHRP advanced config command. It is a simple way to get NHRP up and running with default parameters.

Syntax:

```
enable nhrp
```

Disable NHRP

Use the disable command to disable NHRP on all interfaces not explicitly defined using an NHRP advanced config command.

Syntax:
NHRP Configuration Commands (Talk 6)

Example:
NHRP config> disable
Disable NHRP for the router [No]:

Advanced Config
Use the advanced command to get to the NHRP advanced configuration prompt, NHRP Advanced config>. From this prompt, you can enter the commands described in "NHRP Advanced Configuration Commands" on page 423.

Syntax:
advanced nhrp

Example:
NHRP config> advanced
NHRP Advanced config>

Note: Most installations will not need to use this "advanced" command. The enable NHRP command is sufficient to enable NHRP with recommended default options.

List
Use the list command to list the NHRP configuration.

Syntax:
list

Example:
NHRP config> list
Box level NHRP enabled
    Explicit interface definitions override box level setting
Interfaces explicitly defined for NHRP
    --------------------------
    Interface 0: ATM
        NHRP enabled

NHRP LANE Shortcut Interface:
-------------------------------
Use Best Effort: no (Data)
Cell Rate(kbps): Peak: 155000 Sustained: 155000
ATM adapter's burned-in MAC address is used as source address

General Parameters
-------------------
Holding time: 20 minutes
Protocol Access Controls: Use source and destination address
When should NHC attempt shortcuts?: Based on datarate
Data-rate threshold: 10 packets/second
NHS allows shortcuts to ATMARP clients?: Yes

Cache Sizes
-----------
Resolution cache: 10000 entries
Server purge cache: 10000 entries
Server registrations cache: 10000 entries

Extension Usage
---------------
Use NHRP Forward transit NHS record client extension: No
Use NHRP Reverse transit NHS record client extension: No
NHRP Advanced Configuration Commands

This section explains all of the NHRP advanced configuration commands as shown in Table 110. Enter the commands from the NHRP Advanced config> prompt.

Table 110. NHRP Advanced Configuration Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxviii.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds an NHRP interface, exclude list, or disallowed R2R shortcuts.</td>
</tr>
<tr>
<td>Change</td>
<td>Changes an NHRP interface, or changes a LANE shortcut interface definition.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes an NHRP interface, exclude list, or disallowed R2R shortcuts.</td>
</tr>
<tr>
<td>List</td>
<td>Displays the NHRP configuration.</td>
</tr>
<tr>
<td>Set</td>
<td>Sets NHRP parameters.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxviii.</td>
</tr>
</tbody>
</table>

Add

Use the add command to add an explicit interface definition, an exclude list entry, or disallowed router-to-router shortcuts.

Syntax:

```
add <interface definition>
```

interface definition

```
adds an explicit interface definition to either enable or disable an NHRP interface. If NHRP is disabled on a particular network interface, NHRP packets are not forwarded to any routers that are reached via that interface. Also, incoming NHRP frames are discarded.

Note: Any explicit interface definitions override the "NHRP enabled/disabled" box-level setting.

Example: add int
```

```
Interface Number [0]?
Enable NHRP [Yes]:
```

exclude list

```
Adds an exclude list entry. Specify a protocol address which must be
```
NHRP Advanced Configuration Commands (Talk 6)

excluded from the NHRP network. This option adds an exclude list entry and prompts you to add the exclude list entry to the disallowed router-to-router shortcuts. See "NHRP Access Controls" on page 419 for more information.

Valid values: IP address and mask.
Default: Empty.

Example: add exc

```
IP Address [0.0.0.0]? 6.6.6.5
Address Mask [255.255.255.255]? 255.255.255.255
Deny Shortcuts[Yes]?
Record added to Disallowed Router-to-Router Shortcuts
Record added to Exclude List
```

disallowed router-to-router shortcuts

Adds a router protocol address to which shortcuts are not allowed.

See "Disallowed Router-to-Router Shortcuts" on page 417 for more information.

Example: add dis

```
IP ADDRESS [0.0.0.0]? 8.8.8.1
Address Mask [255.255.255.255]?
```

Valid values: IP address and mask.
Default: Empty.

Delete

Use the delete command to delete an interface definition for NHRP, an exclude list entry, or disallowed router-to-router shortcuts.

Syntax:

```
delete interface definition for NHRP
   exclude list
   disallowed router-to-router shortcuts
```

interface definition for NHRP

Deletes an explicit NHRP interface definition.

Example: del int

```
Interface Number [0]?
```

exclude list

Deletes an exclude list entry. This option deletes an exclude list entry and prompts you to delete the entry from the disallowed router-to-router shortcuts. See "NHRP Access Controls" on page 419 for more information.

You must specify an index which must be deleted. Use the list exclude command to determine the right index.

Example: del exc

```
Enter index of access control to be deleted [1]?
# Address        Mask
  1 6.6.6.5       255.255.255.255
Are you sure this the record you want to delete [Yes]?
Record deleted from Exclude List
Delete from Disallowed Router-to-Router Shortcuts [Yes]?
Record deleted from Disallowed Router-to-Router Shortcuts
```
disallowed router-to-router shortcuts

Deletes a disallowed router-to-router shortcuts entry. You must specify an index to be deleted. Use the list disallowed command to determine the right index.

Example: del dis

Disallowed shortcuts index [1]?

Change

Use the change command to modify NHRP interface definitions.

Syntax:

```
change interface definition
   nhrp lane shortcut interface
```

interface definition for NHRP

Change an explicit interface definition to either enable or disable an NHRP interface.

Example: ch int

```
Interface Number [0]?
Enable NHRP [Yes]:
```

NHRP LANE shortcut Interface

Change a LANE shortcut interface definition.

Example: ch nhrp

```
Interface Number of NHRP LANE Shortcut Interface [0]?
( 1) Use burned in ESI
Select ESI [1]?
Use internally assigned selector? [Yes]:
Use Best Effort Service for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Use ATM adapter's burned-in MAC address for source?
```

Interface Number of NHRP LANE Shortcut Interface

Use the interface number assigned to the LSI. The interface number can be determined by using the list interface command.

( 1) Use burned in ESI

Use universally administered ESI as part of the ATM address. You may be given other choices depending upon your configuration.

Select ESI

Specify the ESI.

Use internally assigned selector

Use internally assigned selector or assign a selector in the range 00 to FF.

Use Best Effort Service for Data VCCs

Specifies the type of traffic characteristics to be associated with Data VCCs. Bandwidth is not reserved for best effort traffic.

Peak Cell Rate of outbound Data VCCs (kbps)

Specifies the Peak Cell Rate (PCR) traffic parameter for the Data VCCs.
NHRP Advanced Configuration Commands (Talk 6)

Sustained Cell Rate of outbound Data VCCs (Kbps)
Specifies the Sustained Cell Rate (SCR) traffic parameter for the Data VCCs.

Use ATM adapter’s burned-in MAC address for source?
You can use as the source MAC address for LANE shortcuts:
1. The adapter’s universally administered MAC address
2. The MAC address supplied in the NHRP resolution reply
3. The MAC address you configured by specifying a MAC address using the change nhrp command.


Note: It is recommended that you use the default values until you have determined the specific processing options required by your environment.

List

Use the list command to display the NHRP configuration information.

Syntax:

list
   all
   exclude list
   disallowed router-to-router shortcuts
   interface definitions
   cache size

all Displays the entire NHRP configuration.
Example: li all
Output is the same as for the list command. See “List” on page 422.

exclude list
Displays the exclude list entries.
Example: li exc

List of NHRP IP exclude records
----------------------------------------
# Address      Mask
1 7.7.7.7 255.255.255.255

disallowed router-to-router shortcuts
Displays disallowed router-to-router shortcuts.
Example: li dis

Disallowed router-to-router shortcuts for IP
--------------------------------------------
1 8.8.8.1  255.255.255.255
2 6.6.6.1  255.255.255.255

interface definitions
Displays the NHRP interface definitions.
Example: li int

Interfaces explicitly defined for NHRP
---------------------------------------
None
NHRP Advanced Configuration Commands (Talk 6)

NHRP LANE Shortcut Interface:
--------------------------------------------------
Interface: 3 ESI: burned-in Sel: auto
Use Best Effort: yes (Data)
Cell Rate(kbps): Peak: 0/ 0 Sustained: 1000/538764944
MAC address supplied by NHS is used as source address

**cache size**
Displays cache sizes.

**Example:** `li ca`

```
Cache Sizes
----- -----
Resolution cache: 10000 entries
Server purge cache: 10000 entries
Server registrations cache: 10000 entries
```

**Set**

Use the `set` command for the following:

**Syntax:**

```
set protocol access control usage
  attempt shortcuts
  holding time
  data-rate threshold
  extensions ...
  cache size ...
  shortcuts to atmarp clients
```

**protocol access control usage**
Determines if the IP access controls will be checked and, if so, how these controls will be applied to NHRP packets. See ["Protocol Access Control Usage" on page 413](#) for more information.

**Example:** `set prot`

Use (Destination, Source & Destination, None) [None]?

**Valid Values:** None, Source and Destination, Destination

**Default Value:** None

**attempt shortcuts**
Determines how the NHRP client decides when to originate resolution requests.

**Valid values:** Y, N, Data-rate.

**Y** Yes. Always try to establish a shortcut VC by building a Next Hop Resolution Request and sending it to the next hop station.

**N** No. Never try to establish a shortcut. Using this option essentially disables the client function in the router. This setting might be used in an intermediate router (one that is not an entry point into the NBMA network for routed traffic) to eliminate the “domino effect”, where traffic following the routed path triggers NHRP Resolution Requests at each NHRP router along the path.
NHRP Advanced Configuration Commands (Talk 6)

**Data-rate**
Try to establish a shortcut only after the datarate threshold is reached.

**Note:** This setting can prevent the creation of VCCs for “one-time” traffic, such as SNMP traps that are sent to an SNMP manager.

**Default:** Data-rate.

**Example:** `set attempt`

Try shortcut VCs? (Yes, No, Data-rate) [Data-rate]?

**holding time**
Sets the holding time in minutes.

The holding time parameter is used for these functions:

- When the router responds to a Next Hop Resolution Request with information about itself (that is, the router is to become the next hop shortcut), the holding time is sent to the requestor as the length of time that the information can be considered valid.

- When the router responds to a Next Hop Resolution Request with information about another NBMA station that was not learned using NHRP (for example, the destination station is an ATM device with an IP address on one of the device subnets), the holding time is sent to the requestor as the length of time that the information can be considered valid.

**Valid values:** 1 - 60 minutes.

**Default:** 20 minutes.

**Example:** `set hold`

Holding time (in minutes) [20]?

**data-rate threshold**
Sets the data rate threshold in packets/second.

The datarate threshold is used when the **attempt shortcuts** parameter is set to **Data-rate**.

When traffic is destined for a particular station, but the rate is less than this threshold, then the router does not attempt to establish shortcuts. (In other words, it does not generate Next Hop Resolution Requests and send them to the next hop along the routed path.) Once the traffic rate exceeds the threshold, the router tries to establish a shortcut. If it can successfully create a shortcut path, the path is used even if the traffic drops below the threshold. The path continues to be used until the traffic stops for a period of time. This is done to avoid going back and forth from the routed path to the shortcut path if traffic is sporadic.

**Valid values:** Minimum 1 packet/second. Maximum is 5120 packets/second.

**Default:** 10 packets/second.

**Example:** `set data`

Data-rate threshold in packets/second [10]?
extensions
Sets the selected NHRP extension usage to yes or no.

- Forward transmit NHS (default: no)
- Reverse transmit NHS (default: no)
- Responder Address (default: no)
- Lane Shortcuts (default: yes)

Valid Values: yes or no

Example: set ext lane

Use LANE shortcuts extension [Yes]?

cache size resolution OR registration OR server purge
Sets the selected cache's maximum entries.

Cache sizes can be selected for any of the following:

resolution cache
This parameter lets you determine the number of entries in the cache for client functions. Each cache entry contains the protocol address-to-NBMA address mapping that can be used to create shortcut VCs. Entries are in the cache when the router has:

- Successfully resolved a protocol address to an NBMA address by sending Next Hop Resolution Requests.
- Attempted to resolve a protocol request to an NBMA address but has either not received a reply, or has received a negative reply, and the associated timer has not expired. These entries are kept in the cache to prevent the device from generating additional Next Hop Resolution Requests for some period of time.
- Received a registration request from a client and the holding time indicated in that request has not yet expired.

When the cache size is exceeded, no new attempts are made to resolve protocol addresses to NBMA addresses (in other words, no new Next Hop Resolution Requests are sent) until existing entries are purged, either because the holding time has expired or a specific purge request has been received from the originator of the information. Also, when cache size is exceeded, Registration Requests from new clients are rejected.

Valid values: 256 - 65535 entries.

Default: 10000 entries.

Example: set cache res

Number of cache entries [10000]?

registration cache
Sets a limit on the number of registration entries in the resolution cache. When the server receives a registration request, it checks to see if the number of NHRP client registrations is below this limit before adding a registration entry in the resolution cache.

Valid values: 256 - 16384 entries.

Default: 10000 entries.

Example: set cache reg
server purge cache

This parameter lets you determine the number of entries in the server purge cache. An entry in this cache represents a destination protocol address and a client to which the server has provided Authoritative NBMA information for that destination.

The destination address may represent the server itself, devices on subnetworks to which the server is attached, NHRP clients that have registered with the server, or routers for which a R2R shortcut has been advertised. The router uses the information in these cache entries to notify clients to purge address information that becomes invalid before the holding time expires.

When the server purge cache size is exceeded, the server rejects Authoritative Next Hop Resolution Requests.

Valid values: 256 - 65535 entries.

Default: 10000 entries.

Example: set cache serv

shortcuts to ATMARP clients

Allows or disallows shortcuts to ATMARP clients.

This parameter can be used to allow or disallow the server from giving out shortcuts to native ATMARP clients that do not support NHRP. This may be required if these clients are not capable of supporting large number of VCs. Use the “Exclude List” option if shortcuts need to be disallowed selectively to certain clients or subnets.

Example: set shortcut

Accessing the NHRP Monitoring Process

To access the NHRP monitoring prompt:
1. At the operator monitoring prompt (*), type talk 5 and press enter.
2. At the +>prompt, type protocol nhrp and press enter.
3. The NHRP> prompt is displayed.

NHRP Monitoring Commands

This section explains all of the NHRP monitoring commands as shown in Table 111. Enter the commands from the NHRP> prompt.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxvii.</td>
</tr>
<tr>
<td>Box Status</td>
<td>Displays NHRP enable/disable status.</td>
</tr>
<tr>
<td>Interface Status</td>
<td>Displays NHRP interface status.</td>
</tr>
<tr>
<td>Statistics</td>
<td>Displays NHRP interface statistics.</td>
</tr>
<tr>
<td>Cache</td>
<td>Displays NHRP resolution cache entries.</td>
</tr>
<tr>
<td>Server_purge_cache</td>
<td>Displays NHRP server_purge_cache entries.</td>
</tr>
</tbody>
</table>
### Box Status

Use the **box status** command to display NHRP status as configured for the box (for example, all interfaces not explicitly defined).

**Syntax:**

```
box-status
```

**Example:**

```
box status
Box level NHRP is ON by config
```

### Interface Status

Use the **interface status** command to display NHRP status on interfaces.

**Syntax:**

```
interface-status
```

**Example:**

```
interface status
Interface 0: UP (NHRP enabled)
Interface 1: UP (NHRP disabled)
Interface 2: DOWN
Interface 3: UP (NHRP LANE Shortcut Interface)
```

### Statistics

Use the **statistics** command to display NHRP statistics for all interfaces or for a specific interface.

**Syntax:**

```
statistics all
```

```
statistics interface
```

**Example:**

```
statistics all
```

Output is the same as that for the **statistics interface** command as shown in the following example.

```
interface
```

Lists NHRP statistics on a specified interface.

**Example:**

```
statistics interface
```
NHRP Monitoring Commands (Talk 5)

Interface number [0]? 0

Statistics for Interface 0
---------------------------------
Field Description | Value
----------------- -----
Inbound Requests | 5
Outbound Requests | 3
Inbound Replies | 3
Outbound Replies | 5
Inbound Registers | 0
Outbound Registers | 0
Inbound Error Packets | 0
Outbound Error Packets | 0
Inbound Error Indication Packets | 0
Outbound Error Indication Packets | 0
Reply Forwards | 0
Unrecognized Options | 0
Registration Overflows | 0
ProtocolErrors | 0
Negative Outbound Replies | 0
Inbound Packets on NHRP disabled interface | 0
'Send to me' Outbound Replies | 0
Inbound Purges | 0
Outbound Purges | 2

Cache

Use the cache command to display all NHRP resolution cache entries or a specific cache entry identified by a destination address.

Syntax:
```
cache
   list
```
```
cache entry
```

Examples:
```
cache list
Total Client Cache Entries = 3

NHRP Client Cache Entries
--------------------------
Dest Address | NextHop Address | State | Htime | MTU | Net
------------|-----------------|-------|-------|-----|---
5.5.5.1     | 5.5.5.1         | Act   | 1121  | 4490| 1
5.5.5.2     | 5.5.5.2         | Inact | 1185  | 4490| 1
6.6.6.1     | 6.6.6.1         | Act   | 602   | 9180| 0

```
cache entry
```
Enter destination address [0.0.0.0]? 6.6.6.1
Destination: 6.6.6.1
NextHop: 6.6.6.1
ATM Address: 39840F00000000000000041005A00DEADCA
State: Act
Net: 0
HoldingTime: 433 seconds
MTU size: 9180
Flags: 0x00420000

Server_purge_cache

Use the server_purge_cache command to list all NHRP server purge cache entries.

Syntax:
```
server_purge_cache
```
MIB

Use the MIB command to display NHRP MIB related information.

**Syntax:**

```plaintext
mib
  - list ...
  - entry ...
```

- **list** Lists NHRP mib entries for:
  - Server table
  - Client table
  - Next-Hop Server (NHS) statistics table
  - Next-Hop Client (NHC) statistics table
  - Resolution cache table

**Example:** `mib list server table`

```
<table>
<thead>
<tr>
<th>Index</th>
<th>Server Address</th>
<th>State</th>
<th>ATM Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>6.6.6.2</td>
<td>UP</td>
<td>39840F00...</td>
</tr>
</tbody>
</table>
```

- **entry** Lists a specific NHRP mib entry in either:
  - Server table
  - Client table
  - Next-Hop Server (NHS) statistics table
  - Next-Hop Client (NHC) statistics table
  - Resolution cache table

**Example:** `mib entry serv`

```
Index [0]? 0
Index : 0
Protocol : 1x0800
Protocol Address: 6.6.6.2
ATM Address type: 0x0 (NSAP)
ATM Address : 39840F00000000000000000210005A00DEADC8
SubnetworkId : 0
Authentication : 1
Current Clients : 0
Max Clients : 512
State : 1
Net : 1
```

LANE Shortcuts

Use the lane shortcuts command to display all or specific entries using LANE shortcuts. You can also display any ATM addresses for which LANE shortcuts are disallowed due to operational problems.

**Syntax:**

```plaintext
lane-shortcuts
  - all
  - entry
  - disallowed
```

- **all** Displays all LANE shortcuts.

**Example:** `lane all`

```
LANE Shortcut Interface #: 1, ATM Network Interface #: 0
================================================================
Next Hop Prot @ Dest Mac @ VPI/VCI
---------------- ----------------- --------
```

Chapter 13. Configuring and Monitoring NHRP
entry
Displays a LANE shortcut entry.

Example: lane entry

LANE Shortcut Interface number [0]? 1
Enter IP address of next hop [0.0.0.0]? 5.5.5.1
Next Hop Addr: 5.5.5.1
Dest Mac Addr: 04-AA-AA-AA-AA-01
ATM Address: 39840F0000000000000000000310005A00DEAD02
Media type: Token Ring
VPI/VCI: 0/34
Holding Time: 20 minutes
MTU size: 4490
RI Field: 064001020203

disallowed
Displays all disallowed LANE shortcut entries.

Any ATM address listed in this display means that the NHRP LANE Shortcut Interface received data from that ATM address. This is not allowed since all NHRP LANE Shortcut Interface VCCs will be used only to transmit data to a LEC at the other end. If the LEC attempts to send data over a VCC set up by an NHRP LANE Shortcut Interface, then the VCC will be brought down and no further LANE shortcuts will be set up to that LEC.

Once the condition which caused the NHRP LANE Shortcut Interface to receive data has been corrected, then the device must be restarted in order to allow that ATM address to be again used for NHRP LANE shortcuts.

Example: lan dis

LAN Shortcut Interface #: 2, ATM Network Interface #: 0
Atm Address
39840F0000000000000000000310005A00DEAD02

CONFIG Parameters

Use the config parameters command to access the command menus for display, change, or reset NHRP configuration parameters.

Table 112. NHRP Config Parameter Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See <a href="#">Getting Help on page xxvii</a>.</td>
</tr>
<tr>
<td>Display</td>
<td>Displays the current NHRP and Route-switching configuration parameters.</td>
</tr>
<tr>
<td>Change</td>
<td>Allows NHRP configuration parameters to be dynamically changed without affecting the static configuration.</td>
</tr>
<tr>
<td>Reset</td>
<td>Reads the configuration parameter from the static configuration and uses it during the router's runtime.</td>
</tr>
</tbody>
</table>

Display

Use the display command to display the current NHRP and Route-Switching configuration parameters.

Syntax:

display nhrp

nhrp Displays NHRP configuration parameters, including general parameters, cache sizes, extensions usage, exclude list, and disallowed router-to-router shortcuts.
Change

Use the **change** command to change the current NHRP configuration parameters. See [Set" on page 427 for a description of these configuration parameters.

**Syntax:**

```
change
  protocol_access_control_usage
  attempt_shortcuts
  holding_time
  data-rate_threshold
  cache_size
  extensions
  shortcuts_to_atmarp_clients
```

Reset

Use the **reset** command to reset the dynamic configuration parameter value to the value in the static configuration. See [Set" on page 427 for a description of these configuration parameters.

**Syntax:**

```
reset
  protocol_access_control_usage
  attempt_shortcuts
  holding_time
  data-rate_threshold
  cache_size
  extensions
  shortcuts_to_atmarp_clients
  exclude_list
  disallowed_router-to-router
```

Reset

Use the **reset** command to dynamically reconfigure NHRP protocol or an interface. A reset causes the applicable static configuration values to be used.

**Syntax:**

```
reset
  interface
    nhrp
```

**nhrp** Resets NHRP statistics, interfaces, and configuration parameters to the static configuration values. This is equivalent to a cold-start of NHRP.

**interface** De-activates the NHRP interface and then activates the interface with new interface static configuration values.
NHRP Packet Tracing

NHRP packet traces can be activated from the Event Logging System (ELS) which is an integral part of the router operating system. See "Using and Configuring the Event Logging System" and "Monitoring the Event Logging System" in Software User's Guide.

The NHRP packet tracing mechanism supports the "set trace decode on" option. This option enables the NHRP packet trace output to be interpreted for viewing. The control frames over the LSI can also be traced apart from the NHRP protocol packets. For details on using the trace facility see the description of the trace command in "Monitoring the Event Logging System" in Software User's Guide.

The NHRP protocol packets are identified by event 19 and the LSI control packets are identified by event 113.

Sample trace output #1:

Dir:OUTGOING Time:0.0.48.88 Trap:6035 Comp:NHRP Type:UNKNOWN Port:1 Circuit:0x000000 Size:160
** NHRP/MPOA Frame **
AddressFamily:ATM_NSAP ProtocolType:IPv4 HopCount:64 PacketSize:160
Checksum:0x03F4 ExtensionOffset:0x000B Version:1 PktType:ResolutionRequest
SrcAddrTL:20 SrcSubAddrTL:0 SrcProtoLen:4 DstProtoLen:4
Src NBMA:39840F0000000000000000000610005A019600C9
Src Protocol Addr: 6.6.6.1 Dest Protocol Addr: 3.3.3.2
0038: 00 08 00 1C 08 00 5A 00 00 01 00 0A 00 00 00 00 | ......Z......... |
0048: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................ |
0058: 00 08 00 34 08 00 5A 00 00 01 00 0C 00 00 00 00 | ...4..Z......... |
0068: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................ |
0078: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................ |
0088: 00 00 00 00 00 00 00 00 00 08 00 08 00 08 00 5A 00 | ................ |
0098: 00 01 00 06 80 00 00 00

Sample trace output #2:

Dir:INCOMING Time:0.0.50.69 Trap:6035 Comp:NHRP Type:UNKNOWN Port:1 Circuit:0x000000 Size:202
** NHRP/MPOA Frame **
AddressFamily:ATM_NSAP ProtocolType:IPv4 HopCount:63 PacketSize:202
Checksum:0xEC88 ExtensionOffset:0x005C Version:1 PktType:ResolutionReply
SrcAddrTL:20 SrcSubAddrTL:0 SrcProtoLen:4 DstProtoLen:4
Src NBMA:39840F0000000000000000000310005A01950103
Src Protocol Addr: 3.3.3.1 Dest Protocol Addr: 3.3.3.2
1483 VCC Shortcut Information (CIE) follows:
   CIE NBMA:39840F0000000000000000000310005A01950103
   CIE Protocol Addr: 3.3.3.1
005C: 00 08 00 1C 08 00 5A 00 00 01 00 0B 00 00 00 01 | ......Z......... |
006C: 00 08 00 34 08 00 5A 00 00 01 00 0C 00 00 00 00 | ...4..Z......... |
007C: 00 08 00 34 08 00 5A 00 00 01 00 0C 00 00 00 00 | ...4..Z......... |
008C: 00 08 00 34 08 00 5A 00 00 01 00 0C 00 00 00 00 | ...4..Z......... |
009C: 00 08 00 34 08 00 5A 00 00 01 00 0C 00 00 00 00 | ...4..Z......... |

NHRP Server Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.
**CONFIG (Talk 6) Delete Interface**

NHRP Server supports the CONFIG (Talk 6) `delete interface` command with the following consideration:

- The NHRP LANE Shortcut Interface cannot be deleted with the `delete interface` command. Use the `disable nhrp` config option to delete NHRP LANE Shortcut Interface.

**GWCON (Talk 5) Activate Interface**

NHRP Server supports the GWCON (Talk 5) `activate interface` command with the following consideration:

- The NHRP LSI (LANE Shortcut Interface) associated with each ATM physical interface is activated automatically after the associated ATM physical interface is activated.

All NHRP Server interface-specific commands are supported by the GWCON (Talk 5) `activate interface` command.

**GWCON (Talk 5) Reset Interface**

NHRP Server supports the GWCON (Talk 5) `reset interface` command with the following consideration:

- Cannot reset the interface type NHRP LANE Shortcut Interface without restart.

All NHRP Server interface-specific commands are supported by the GWCON (Talk 5) `reset interface` command.
NHRP Packet Tracing
Chapter 14. Using IP Version 6 (IPv6)

This chapter describes how to use IPv6.

IPv6 Overview

IP Version 6 (IPv6) is a new version of the Internet Protocol. It is designed as a successor to IP Version 4 (IPv4). The following list identifies some of the advantages provided by IPv6:

- Large address space
  IPv6 uses a 128-bit address.
- Routing
  Using the large address size, IPv6 provides an hierarchical address scheme which allows you to create a flexible routing hierarchy.
- Ease of configuration
  NDP provides host autoconfiguration.
- Security
  IPv6 makes IP Security mandatory.
- Support for multimedia traffic
  The IPv6 header has priority and flow label fields to accommodate integrated Quality of Service.
- Simplification
  The IPv6 header is fixed and simplified. The router is no longer required to perform fragmentation, simplifying packet processing. In addition, options type data is implemented in extension headers that are only processed by the destination node.

IPv6 Comparison with IPv4

IPv6 includes many changes from IPv4. The most significant changes are:

- Address
- Header format
- Minimum MTU
- Mandatory Path MTU discovery
- Mandatory IP security
- Neighbor Discovery Protocol (NDP)

IPv6 Addressing

IPv6 addressing increases the address from 32 bits to 128 bits. This increase allows more degrees of hierarchy than the basic layers of network, subnet and host.

IPv6 addresses belong to one of three categories:

- Unicast. A packet is delivered to the interface identified by the address.
- Multicast. A packet is sent to all members of the multicast group identified by the address.
- Anycast. A packet is sent to only the nearest member of the group identified by the address.

Broadcast addressing has been replaced by multicast addressing in IPv6.
Using IPv6

IPv6 Address Format

The IPv6 address is composed of 128 bits. These bits are written as eight 16-bit integers separated by colons.

Example:


You can use the following simplifying rules:

- Skip leading zeroes.
  
  Example:
  
  ABCD:1234:0:1234:0:FFEE:7777:123

- Inside an address, a set of consecutive, null 16-bit numbers can be replaced by two colons.
  
  Example:
  
  ABCD:1234::1234:5555:FFEE:7777:123
  
  1234::7899

The double colon can be used only once inside the address.

- When dealing with a mixed environment of IPv4 and IPv6 nodes, you can use the form x:x:x:x:x:d.d.d
  
  , where the x’s are hexadecimal values of the six high-order 16-bit pieces of the address, and the d’s are the decimal values of the four low-order 8-bit pieces of the address in standard IPv4 representation.
  
  Example:
  
  ABCD:1234::1234:5555:FFEE:1.2.3.4
  
  ::1.2.3.4

Text Representation of Address Prefixes

An IPv6 address prefix is represented by the notation:

IPv6-address/prefix-length

The IPv6 address can use any of the notations listed in IPv6 Address Format and the prefix length is a decimal value specifying how many of the leftmost contiguous bits of the address comprise the prefix.

Example:

ABCD:1234::1234:5555:FFEE:1.2.3.4/64

IPv6 Header Format

The IPv6 header has a total of 8 fields, eliminating some IPv4 fields such as checksum and fragmentation.

IPv6 Minimum MTU

The minimum MTU for IPv6 is 1280 bytes. You cannot enable IPv6 on an interface with an MTU less than 1280 bytes.
IPv6 Mandatory Path MTU Discovery

IPv6 Mandatory Path MTU Discovery is a protocol that allows a host to determine the maximum size packet that will successfully traverse a path to a destination without fragmentation. As packets are generated and sent from the host, the MTU of the particular output interface that the packet will be transmitted to is available.

If the packet will fit on the output interface, either as a whole or in fragments, it is transmitted. If a router in the path needs to forward that packet onto a net with a smaller MTU than the packet size, the packet will be dropped and an ICMP message will be sent to the originator of the packet indicating the packet size that is necessary to fit onto the output net of the intermediate router. The host receiving this message will adjust the size of subsequent packets forwarded on the path. This process may occur multiple times before the packet reaches its final destination. Once the packet reaches its destination, subsequent packets should not be dropped because their packet size being too large.

Because the route can change dynamically, the path MTU may increase and will need adjustment in the host node. Learned path MTUs are aged and the Path MTU Discovery process re-occurs. This allows the transmitted packet size to react to the dynamic nature of routes through the network.

Path MTU Discovery is mandatory because fragmentation is not allowed on transit routers.

If the device is acting as a transit router, it will not forward packets that are larger than the output net's MTU. It will generate an ICMP Packet Too Big message back to the source of the packet.

The `enable path-mtu-discovery` command at the IPv6 Config> prompt can be used to enable or disable path MTU discovery. Path MTU discovery is enabled by default.

Use the `set path-mtu-aging-timer` command at the IPv6 Config> prompt to specify the aging time for path MTUs that have been determined.

IPv6 Mandatory Security

An IPv6 node must support IP security. IP security can be enabled or disabled. See ["Using IP Security"] and ["Configuring and Monitoring IP Security"] in the [Using and Configuring Features] for additional information about IP security.

1. Use the `add packet` command at the IPv6 Config> prompt to add a packet filter.
2. Use the `update packet` command at the IPv6 Config> prompt to update the packet filter.
3. Use the `add access` command at the Packet-filter 'filter_name' Config> prompt to add access controls.
4. Use the `set acc on` command at the IPv6 Config> prompt to enable access control.
IPv6 Neighbor Discovery Protocol (NDP)

IPv6 uses NDP to perform autoconfiguration. NDP allows IPv6 nodes on the same link to discover each other’s presence, to determine each other’s link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors.

Router and Prefix Discovery

Hosts use Router Discovery to discover routers that reside on an attached link. Each router periodically multicasts a Router Advertisement packet, if configured, announcing its availability. Router advertisements contain a list of prefixes used for on-link determination and autonomous address configuration. Hosts can use the advertised on-link prefixes to determine when a packet’s destination is on the link or beyond a router.

Address Autoconfiguration

Router advertisements allow routers to inform host how to perform address autoconfiguration. Routers can specify whether hosts use stateful or autonomous (stateless) address configuration.

Address Resolution

Routers accomplish address resolution by multicasting a neighbor solicitation message that asks the target node to return its link-layer address. The link-layer address is returned in a unicast neighbor advertisement. By including its link-layer address in the neighbor solicitation message, a single request-response pair of messages, the message initiator and the target can determine each other’s link-layer addresses.

Neighbor Unreachability Detection

NDP can detect the failure of a neighbor or the failure of the forward path to the neighbor. When no positive confirmation has been received from a neighbor for a time interval, the node actively probes the neighbor using unicast neighbor solicitation messages to verify that the forward path is still working.

Redirect

If the source address of the packet and the next hop are on the same network, a router may send a redirect message informing the sender that the next hop is a neighbor.

Use the `p ndp` command at the `Config>` prompt to configure NDP parameters.

IPv6 over IPv4 Tunneling

IPv6 over IPv4 tunneling allows you to migrate from IPv4 networks to IPv6 networks without the need to simultaneously upgrade all equipment to IPv6 support. IPv6 over IPv4 tunneling allows IPv6 frames to cross an IPv4 network and reach an IPv6 destination. The IPv6 frame is encapsulated in an IPv4 frame and this encapsulated frame is forwarded through the IPv4 network to a specific IPv4 destination, called the endpoint of the tunnel. At this endpoint, the packet is decapsulated and forwarded to the final IPv6 destination.
Adding a configured tunnel causes a virtual interface to be added. That virtual interface is then treated as a normal interface by IPv6 and may be used by RIP for route establishment.

Use the `add tunnel` command at the IPv6 Config> prompt to add an IPv6 over IPv4 tunnel.

---

**Protocol Independent Multicast (PIM)**

See "Using PIM" on page 483 for usage information about the PIM protocol.
Chapter 15. Configuring and Monitoring IPv6

This chapter describes how to use the IPv6 configuration and operating commands and includes the following sections:

- "Accessing the IPv6 Configuration Environment"
- "IPv6 Configuration Commands"
- "Accessing the IPv6 Monitoring Environment" on page 463
- "IPv6 Monitoring Commands" on page 463
- "IPv6 Dynamic Reconfiguration Support" on page 469

Accessing the IPv6 Configuration Environment

Use the following procedure to access the IPv6 configuration process.

1. At the OPCON prompt, enter talk 6. (For more detail on this command, refer to The OPCON Process and Commands in the Software User’s Guide.) For example:
   ```
   * talk 6
   Config>
   ```
   After you enter the talk 6 command, the CONFIG prompt (Config>) displays on the terminal. If the prompt does not appear when you first enter configuration, press Return again.

2. At the CONFIG prompt, enter the p ipv6 command to get to the IPv6 Config> prompt.

IPv6 Configuration Commands

To configure IPv6, enter the commands at the IPv6 Config> prompt.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See <a href="#">Getting Help</a> on page xxi.</td>
</tr>
<tr>
<td>add</td>
<td>Adds an address, leaked-routes, packet-filter, route, or tunnel.</td>
</tr>
<tr>
<td>change</td>
<td>Changes an address, leaked routes, packet-filter, route, or tunnel.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes an address, leaked routes, packet filter, route, or tunnel.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables icmp redirects, packet filter, or path MTU discovery.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables ICMP redirects, packet filters, or path MTU discovery.</td>
</tr>
<tr>
<td>list</td>
<td>Lists the configuration.</td>
</tr>
<tr>
<td>move</td>
<td>Moves access control.</td>
</tr>
<tr>
<td>set</td>
<td>Sets configuration values associated with automatic tunnels, fast forwarding path cache buffer size, default gateway, MLD, path MTU aging timer, packet reassembly buffer size, routing table size, router id, and router time to live.</td>
</tr>
<tr>
<td>update</td>
<td>Updates the packet filter.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See <a href="#">Exiting a Lower Level Environment</a> on page xxviii.</td>
</tr>
</tbody>
</table>

Add

Use the add command to add an IPv6 address, leaked routes, packet filters, routes, or IPv6 over IPv4 tunnels.

```bash
add access-control
address net address prefix
leaked-routes destination
```
IPv6 Configuration Commands (Talk 6)

Example:
IPv6 config>add address
Which net is this address for [0]? 5
New address []? 1::2
Prefix length must between 8 and 128 [128]?

IPv6 config>add leaked
IPV4 destination []? 1.2.3.4
Address mask [255.0.0.0]? 255.255.255.255

IPv6 config>add packet-filter
Packet-filter name []? pktf01
Filter incoming or outgoing traffic [IN]
Which interface is this filter for [0]? 3

IPv6 config>add route
IPv6 destination []? 8::9
Prefix length must between 8 and 128 [8]? 128
Via gateway 1 at []? 1::2
Cost [1]?
Via gateway 2 at []? 2::3
Cost [1]? 1000
Via gateway 3 at []? 3::4
Cost [1]? 10000
Via gateway 4 at []? 4::5
Cost [1]? 10
IPv6 config>add tunnel
Add a static route through this tunnel? [Yes[:
IPv6 destination network []? 3::4
Prefix length must between 0 and 128 [64]? 128
IPv4 tunnel remote address []? 1.2.3.4
IPv4 tunnel local address []? 2.3.40.0
Cost [1]?
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):

access-control
Adds access control.

access control type
Indicates what is done with packets that match the access control rule parameters.

E Exclusive; matching packets are discarded.
I Inclusive; matching packets are processed further by the router.

Internet source
Source Internet address.

Valid Values: Any valid Internet address
Default Values: None

Source Prefix length
Specifies the prefix length for the Internet source address.

Valid Values: 0 - 128
Default Values: 128
**Internet destination**
Destination Internet address.

**Valid Values:** Any valid Internet address

**Default Value:** None

**Destination Prefix length**
Specifies the prefix length for the Internet destination address.

**Valid Values:** 0 - 128

**Default Values:** 128

**Starting protocol number**
Specifies the starting protocol number for a range of protocol numbers. Enter a value of 0 to select all protocols.

Some common protocol numbers are:
1 for ICMP
6 for TCP
17 for UDP
89 for OSPF
50 for ESP-Encryption
51 for AH-Encryption

**Valid Values:** 0 to 255

**Default Values:** 0

**Ending protocol number**
Specifies the ending protocol number for a range of protocol numbers. Enter a value of 0 to select all protocols.

Some common protocol numbers are:
1 for ICMP
6 for TCP
17 for UDP
89 for OSPF
50 for ESP-Encryption
51 for AH-Encryption

**Valid Values:** 0 to 255

**Default Values:** the value specified as the starting protocol number

**Starting destination port number**
Specifies the starting port number for a range of TCP/UDP destination port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17.

Some commonly used port numbers are:
21 for FTP
23 for Telnet
25 for SMTP
513 for rlogin
520 for RIP for IPv4
521 for RIP6 for IPv6

**Valid Values:** 0 - 65535
Default Value: 0

**Ending destination port number**
Specifies the ending port number for a range of TCP/UDP destination port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17.

Some commonly used port numbers are:
- 21 for FTP
- 23 for Telnet
- 25 for SMTP
- 513 for rlogin
- 520 for RIP for IPv4
- 521 for RIP6 for IPv6

**Valid Values:** 0 - 65535

Default Value: the value specified as the **starting destination port number**

**Starting source port number**
Specifies the starting port number for a range of TCP/UDP source port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17. See the description of **starting destination port number** for a list of commonly used TCP/UDP port numbers.

**Valid Values:** 0 - 65535

Default Value: 0

**Ending source port number**
Specifies the ending port number for a range of TCP/UDP source port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17. See the description of **starting destination port number** for a list of commonly used TCP/UDP port numbers.

**Valid Values:** 0 - 65535

Default Value: the value specified as the **starting source port number**

**address**
Adds an IPv6 address.

**Which net is this address for**
Specifies the net to which the IPv6 address is to be added.

**Valid Values:** A numeric value identifying a network interface

Default Value: 0

**New address**
Specifies the new IPv6 address to be added.

**Valid Values:** Any valid IPv6 address

Default Value: None
IPv6 Configuration Commands (Talk 6)

Prefix length
Decimal value specifying how many of the leftmost contiguous bits of the address comprise the prefix.

Valid Values: 8 - 128
Default Value: 128

leaked-routes
Adds a leaked route.

IPV4 destination
Specifies the IPv6 address of the destination for the leaked route.

Valid Values: Any valid IPv6 address
Default Value: None

packet-filter
Adds a packet-filter.

packet-filter name
Specifies an alphanumeric name used to identify the packet filter.

Valid Values: Any alphanumeric character string up to 16 characters in length
Default Value: None

Filter incoming or outgoing traffic?
Specifies whether you want to filter incoming or outgoing traffic.

Valid Values: OUT or IN
Default Value: IN

which interface is this filter for
Specifies the network interface number to which the packet filter is to be added.

Valid Values: A numeric value identifying any interface for which IPv6 is a valid protocol, or “a”, which specifies that this filter is for the automatic tunnel.
Default Value: 0

route
Adds a route.

IPv6 destination
Specifies the IPv6 address of the target for the route.

Valid Values: Any valid IPv6 address
Default Value: None

Prefix length
Specifies the mask to be applied to the destination address.

Valid Values: 8 - 128 (0 is allowed if the IPv6 destination is 0::0)
Default Value: 8

Via gateway 1
Specifies the IPv6 address of the gateway 1.

Valid Values: Any valid IPv6 address
Default Value: None
IPv6 Configuration Commands (Talk 6)

**Cost**
Specifies the cost of this route.

*Valid Values:* A numeric value

*Default Value:* 1

**Via gateway 2**
Specifies the IPv6 address of the gateway 2.

*Valid Values:* Any valid IPv6 address

*Default Value:* None

**Cost**
Specifies the cost of this route.

*Valid Values:* A numeric value

*Default Value:* 1

**Via gateway 3**
Specifies the IPv6 address of the gateway 3.

*Valid Values:* Any valid IPv6 address

*Default Value:* None

**Cost**
Specifies the cost of this route.

*Valid Values:* A numeric value

*Default Value:* 1

**Via gateway 4**
Specifies the IPv6 address of the gateway 4.

*Valid Values:* Any valid IPv6 address

*Default Value:* None

**Cost**
Specifies the cost of this route.

*Valid Values:* A numeric value

*Default Value:* 1

**tunnel**
Adds a tunnel.

**Add a static route through this tunnel?**
Specifies whether or not the tunnel will have a static route defined.

*Valid Values:* Yes or No

*Default Value:* Yes

**IPv6 destination network**
Specifies the IPv6 address of the destination network that will be reached by the tunnel.

*Valid Values:* Any valid IPv6 address

*Default Value:* None

**Prefix length**
Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.

*Valid Values:* 8 - 128

*Default Value:* 64
IPv6 Configuration Commands (Talk 6)

IPv4 tunnel remote address
Specifies the IPv4 address for the IPv6 frames passed through the tunnel.

Valid Values: Any valid IP (32-bit) address
Default Value: None

IPv4 tunnel local address
Specifies the IPv4 source address for the IPv6 frames passed through the tunnel.

Valid Values: Any valid IP (32-bit) address
Default Value: None

Cost
Specifies the cost associated with the tunnel which will be used during route lookups to find the best route to the destination.

Valid Values: 1 - 255
Default Value: 1

TTL value
Specifies the time-to-live value used in frames encapsulated for this tunnel

Valid Values: Any numeric value in the range of 1 - 255
Default Value: 64

Allow fragmentation in the tunnel?
Specifies whether the fragmentation in the tunnel will be allowed.
Specifying yes allows fragmentation in the tunnel in case the IPv4 network that the tunnel is using does not provide enough information to allow the device to return a “Packet Too Big” message to the IPv6 host.

Valid Values: yes or no
Default Value: no

Change

Use the change command to add an access control record, IPv6 address, leaked routes, packet filters, routes, or tunnels.

Syntax:
```
change
  access-control index
  address net address prefix
  leaked-routes destination
  packet-filter name interface
  route destination mask gateway cost ...
  tunnel destination prefix raddress locaddress cost ttl
  fragmentation
```

access-control
Changes access control configuration.

address
Changes an address.

leaked-routes
Changes a leaked route configuration.
IPv6 Configuration Commands (Talk 6)

packet-filter
    Changes a packet filter configuration.

route
    Changes a route configuration.

tunnel
    Changes a tunnel configuration.

See "Add" on page 445 for a description of the parameters associated with the change command.

Delete

Use the delete command to remove an access control record, address, leaked-routes, packet filter, route or tunnel.

Syntax:
```
delete
    access-control index
    address address
    leaked-routes destination
    packet-filter name
    route destination mask gateway
    tunnel tunnel#
```

Disable

Use the disable command to disable ICMP redirect, packet filters, and path MTU discovery.

Syntax:
```
disable
    icmp-redirect address
    packet-filter packet-filter-name
    path-mtu-discovery
```

icmp-redirect
    Disables ICMP redirects.

packet-filter
    Disables a packet-filter.

    packet-filter name
        Specifies the name of the packet filter to be disabled.

        Valid Values: Any configured packet filter

        Default Value: None

path-mtu-discovery
    Disables Path MTU Discovery.

Enable

Use the enable command to enable ICMP redirects, packet filters, or path MTU discovery.

Syntax:
```
enable
    icmp-redirect address
    packet-filter packet-filter-name
    path-mtu-discovery
```

icmp-redirect
    Enables ICMP redirects.
interface address
   Specifies the interface address.
   **Valid Values:** Any valid IPv6 address
   **Default Value:** Null (specifies all addresses)

packet-filter
   Enables a packet-filter.

**packet-filter name**
   Specifies the name of the packet-filter to be enabled. This name is configured using the `add packet-filter` command.
   **Valid Values:** Any valid IPv6 address
   **Default Value:** None

path-mtu-discovery
   Enables Path MTU Discovery, a protocol that allows a host node to determine the maximum size packet that will traverse a path to a destination without fragmentation.

**List**

Use the `list` command to display the IPv6 configuration.

**Syntax:**

```
list [all | access-control | addresses | icmp-redirect | leaked-routes | mld | packet-filter | routes | sizes | tunnels]
```

**Example:**

```
IPv6 config>list all
Interface addresses
IPv6 addresses for each interface:
   intf 0 IP disabled on this interface
   intf 1 IP disabled on this interface
   intf 2 IP disabled on this interface
   intf 3 IP disabled on this interface
   intf 4 IP disabled on this interface
   intf 5 1234:1234:1234:1234:5234:6234:7234:8234/128
          1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8

Routing
route to: 1234::1223/128
   via: 1234:0:9::8 cost: 100
   via: 1234:0:9::8:7:6:8 cost: 232
   via: 1:2:3:4:5:6:7:8 cost: 1
   via: 8:7:6:5:4:3:2:1 cost: 1
route to: ::/0
   via: 1::8 cost: 100
route to: 2::8:9/8
   via: 1::8 cost: 1
```
IPv6 Configuration Commands (Talk 6)

Path MTU Discovery: disabled
Path MTU Aging Timer: 10 minutes

Access Control is: enabled

IPv6 config>list addresses
IPv6 addresses for each interface:
  intf 0 IP disabled on this interface
  intf 1 IP disabled on this interface
  intf 2 IP disabled on this interface
  intf 3 IP disabled on this interface
  intf 4 IP disabled on this interface
  intf 5 1234:1234:1234:1234:5234:6234:7234:8234/128
        1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8
IPv6 config>list icmp-redirect
ICMP Redirect generation for IP interface:
  intf 0 IP disabled on this interface
  intf 1 IP disabled on this interface
  intf 2 IP disabled on this interface
  intf 3 IP disabled on this interface
  intf 4 IP disabled on this interface
  intf 5 1234:1234:1234:1234:5234:6234:7234:8234/128 ICMP Redirect enabled
        1223::7:1234/8 ICMP Redirect enabled
  intf 6 IP disabled on this interface
  intf 7 IP disabled on this interface

IPv6 config>list leaked-routes
# IPv4 Address Mask
IPv6 config>list mld
Net Query Interval Response Interval Leave Query Interval
  (secs) (secs) (secs)
--- -------------- ----------------- --------------------
  5 125 10 1

IPv6 config>list packet-filter
List of packet-filter records:

Name Interface State
packet01 0 On
pack01 5 On

Access Control is: enabled
IPv6 config>list routes
route to: 1234::1223/128
  via: 1234:0:9::8 cost: 100
  via: 1:2:3:4:5:6:7:8 cost: 1
  via: 8:7:6:5:4:3:2:1 cost: 1
route to: ::/0
  via: 1::8 cost: 100
route to: 2::8:9/8
  via: 1::8 cost: 1

IPv6 config>list sizes
Routing table size: 768 nets (79872 bytes)
Reassembly buffer size: 12000 bytes
Routing cache size: 64 entries
IPv6 Configuration Commands (Talk 6)

Time to live: 64
Path MTU aging timer: 10

IPv6 config> list tunnel
Tun# Remote Endpoint Local Endpoint Frag Allowed TTL Cost Net# IPv6 Address/Prefix
1 1.2.3.4 2.3.4.5 No 100 100 7 1:2:3:4:5:6:7:8/128
IPv6 config>

Move

Use the move command to change the order of configured access control records.

Syntax:
move

Index of control to move
Select the index number of the access control record you want to move.

Move record AFTER record number
Select the index number of the access control record you want this record to follow.

Are you sure that this is what you want to do
Allows you to confirm that the move instruction is correct.

Set

Use the set command to set configuration parameters.

Syntax:
set

Example:
IPv6 config> set au
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):
IPv6 config> set ca
number of cache entries [64]?
IPv6 config> set mld query-interval
Network interface [0]? 5
New Query Interval (in secs) [125]?
IPv6 config> set mld response-interval
Network interface [0]? 5
New Response Interval (in secs) [10]?
IPv6 config> set mld robust
Network interface [0]? 5
New Robustness Variable [2]?
IPv6 Configuration Commands (Talk 6)

IPv6 config>
set mld leave
Network interface [0]?
New Leave Interval (in secs) [1]?
IPv6 config>?

access-control
  Specifies whether access control is enabled or disabled.
  
  **Valid Values:** on or off
  
  **Default Value:** off

automatic-tunnel-parameters
  Specifies the tunnel parameter values for automatic tunnels that flow through the router.
  
  **ttl value**
  Specifies the time-to-live value for the frames encapsulated for the tunnel.
  
  **Valid Values:**
  
  **Default Value:** 64

allow fragmentation in tunnel?
  Specifies whether the fragmentation in the tunnel will be allowed.
  Specifying yes allows fragmentation in the tunnel in case the IPv4 network that the tunnel is using does not provide enough information to allow the device to return a “Packet Too Big” message to the IPv6 host.
  
  **Valid Values:** yes or no
  
  **Default Value:** no

hop count
  Specifies the hop count to be used on automatically tunnelled packets.
  
  **Valid Values:** 1 - 255
  
  **Default Value:** 64

**cache-size**
  Specifies the buffer size for the fast forwarding path cache.

  **number of cache entries**
  Specifies the number of entries in the fast forwarding path cache.
  
  **Valid Values:** 64 - 10 000
  
  **Default Value:** 64

default network-gateway
  
  **default gateway**
  
  **Valid Values:** Any valid IPv6 address
  
  **Default Value:** none

  **gateway’s cost**
  Specifies the cost associated with this gateway.
  
  **Valid Values:** 1 - 255
  
  **Default Value:** 1

default subnet-gateway
for which subnetted network
  Valid Values: Any valid IPv6 address
  Default Value: none

default gateway
  Valid Values: Any valid IPv6 address
  Default Value: none

gateway's cost
  Specifies the cost associated with this gateway.
  Valid Values: 1 - 255
  Default Value: 1

internal-ip-address
  Valid Values: Any valid IPv6 address
  Default Value: None

mld

query-interval
  network interface
    Valid Values: Any valid network interface number
    Default Value: 0
  new query interval (in secs)
    Valid Values: 1 - 3600
    Default Value: 125

response-interval
  network interface
    Valid Values: Any valid network interface number
    Default Value: 0
  new response interval (in secs)
    Valid Values: 1 - 60
    Default Value: 10

robustness-variable
  network interface
    Valid Values: Any valid network interface number
    Default Value: 0
  new robustness variable
    Valid Values: 2 - 10
    Default Value: 2

leave-interval
  network interface
    Valid Values: Any valid network interface number
IPv6 Configuration Commands (Talk 6)

Default Value: 0
new leave interval (in secs)
Valid Values: 1 - 60
Default Value: 1

path-mtu-aging-timer
Specifies the aging time in minutes for path MTUs that have been
determined using path MTU discovery.
Valid Values: 10 - 60 minutes, where 0 = disable
Default Value: 10

reassembly-size
Specifies the size of the reassembly buffers used for processing the
fragment header.
Valid Values: 2048 - 65536
Default Value: 12000

router-id
Specifies the IPv6 address of the router.
Valid Values: Any valid IPv6 address
Default Value: None

routing table-size
number of nets
Valid Values: 64 - 65 535
Default Value: 768

ttl
Specifies the IPv6 time-to-live value.
Valid Values:
Default Value: 64

Update
Use the **update** command to update the packet filter

**Syntax:**
update packet-filter

**packet-filter**
Use this command to access the Packet-filter 'xx' Config> command
prompt from which you can configure packet-filters.

Update Packet-filter Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See <a href="#">Getting Help</a> on page xxvili.</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Adds access control.</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Changes access control.</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes access control.</td>
<td></td>
</tr>
</tbody>
</table>
Table 114. Update Packet-Filter Configuration Command Summary (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move</td>
<td>Reorders the access control list applied to the packet filter.</td>
</tr>
<tr>
<td>List</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxviii.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxviii.</td>
</tr>
</tbody>
</table>

**Add**

Use the `update packet-filter add` command to add an access control list.

**Syntax:**

```
add access-control type sourceaddr sourceprefix destaddr destprefix
```

- `access-control`: Adds an access-control item to the access control list.
- `type`: Specifies whether the access control is inclusive or exclusive.
  - **Valid Values:** I or E
  - **Default Value:** I
- `sourceaddr`: Specifies the IPv6 address of the packet source.
  - **Valid Values:** Any valid IPv6 address
  - **Default Value:** None
- `sourceprefix`: Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.
  - **Valid Values:** 0 - 128
  - **Default Value:** 128
- `destaddr`: Specifies the IPv6 address of the packet destination.
  - **Valid Values:** Any valid IPv6 address
  - **Default Value:** None
- `destprefix`: Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.
  - **Valid Values:** 0 - 128
  - **Default Value:** 128

**Starting protocol number**

Specifies the starting protocol number for a range of protocol numbers. Enter a value of 0 to select all protocols.

Some common protocol numbers are:

- 1 for ICMP
- 6 for TCP
- 17 for UDP
- 89 for OSPF
- 50 for ESP-Encryption
- 51 for AH-Encryption

- **Valid Values:** 0 to 255
IPv6 Configuration Commands (Talk 6)

**Default Values:** 0

**Ending protocol number**
Specifies the ending protocol number for a range of protocol numbers. Enter a value of 0 to select all protocols.

Some common protocol numbers are:
- 1 for ICMP
- 6 for TCP
- 17 for UDP
- 89 for OSPF
- 50 for ESP-Encryption
- 51 for AH-Encryption

**Valid Values:** 0 to 255

**Default Values:** the value specified as the **starting protocol number**

**Starting destination port number**
Specifies the starting port number for a range of TCP/UDP destination port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17.

Some commonly used port numbers are:
- 21 for FTP
- 23 for Telnet
- 25 for SMTP
- 513 for rlogin
- 520 for RIP

**Valid Values:** 0 - 65535

**Default Value:** 0

**Ending destination port number**
Specifies the ending port number for a range of TCP/UDP destination port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17.

Some commonly used port numbers are:
- 21 for FTP
- 23 for Telnet
- 25 for SMTP
- 513 for rlogin
- 520 for RIP

**Valid Values:** 0 - 65535

**Default Value:** the value specified as the **starting destination port number**

**Starting source port number**
Specifies the starting port number for a range of TCP/UDP source port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is
not 6 or 17. See the description of starting destination port number for a list of commonly used TCP/UDP port numbers.

Valid Values: 0 - 65535

Default Value: 0

Ending source port number
Specifies the ending port number for a range of TCP/UDP source port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17. See the description of starting destination port number for a list of commonly used TCP/UDP port numbers.

Valid Values: 0 - 65535

Default Value: the value specified as the starting source port number

Change
Use the update packet-filter change command to change access control.

Syntax:
change access-control type sourceaddr sourceprefix destaddr destprefix

access-control
Changes an access-control item.

Type
Specifies whether the access control item is inclusive or used to identify packets to be secured.

Valid Values: I or S

Default Value: I

Internet source
Specifies the IPv6 address of the packet source.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length
Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.

Valid Values: 0- 128

Default Value: 128

Internet destination
Specifies the IPv6 address of the packet destination.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length
Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.

Valid Values: 0- 128

Default Value: 128
IPv6 Configuration Commands (Talk 6)

Delete
Use the `update packet-filter delete` command to remove an access control item from the access control list.

Syntax:
```
del **e**te _**a**ccess-control index#
```

- **access-control**
  Deletes access-control.

  - **index of access control to be deleted**
    Specifies the index of the access control configuration to be removed.
    
    - **Valid Values**: 1 to the number of access control records defined for this packet filter
    
    - **Default Value**: 1

Move
Use the `update packet-filter move` command to re-order the access control list applied to the packet-filter.

Syntax:
```
move _**a**ccess-control index# after#
```

- **access-control**
  
  - **index of control to move**
    
    - **Valid Values**: 1 to the number of access control records defined for this packet filter
    
    - **Default Value**: 1

  - **Move record after record number**
    Specifies target location in the access-control list. You will be asked to verify that this is the action you want to configure.
    
    - **Valid Values**: 1 to the number of access control records defined for this packet filter
    
    - **Default Value**: 0

List
Use the `update packet-filter list` command to display the access control list configuration.

Syntax:
```
list _**a**ccess-controls
```

Example:
```
Packet-filter 'x' Config> li acc
Access control is : enabled
List of access control records:

1 Type=IS Source=2001:1::6101/128
   Dest= 2001:1::86/128
   Tid=3

2 Type=I Source::/0
```
Accessing the IPv6 Monitoring Environment

Use the following procedure to access the IPv6 monitoring commands. This process gives you access to the IPv6 monitoring process.

1. At the OPCON prompt, enter talk 5. (For more detail on this command, refer to the chapter entitled “The OPCON Process and Commands” in the Software User’s Guide.) For example:

```
+ talk 5
```

After you enter the talk 5 command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press Return again.

2. At the + prompt, enter the p ipv6 command to get you to the ipv6> prompt.

Example:
```
+ p ipv6
ipv6>
```

IPv6 Monitoring Commands

This section describes the IPv6 monitoring commands.

Table 115. IPv6 Monitoring Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See <a href="#">Getting Help on page xxvii</a>.</td>
</tr>
<tr>
<td>access-control</td>
<td>Displays access control records.</td>
</tr>
<tr>
<td>cache</td>
<td>Displays cache entries.</td>
</tr>
<tr>
<td>counters</td>
<td>Display counters</td>
</tr>
<tr>
<td>dump routing</td>
<td>Dumps the configured routing tables.</td>
</tr>
<tr>
<td>tables</td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>Displays the addresses defined on the interface.</td>
</tr>
<tr>
<td>addresses</td>
<td></td>
</tr>
<tr>
<td>internal</td>
<td>Displays the specified internal address.</td>
</tr>
<tr>
<td>address</td>
<td></td>
</tr>
<tr>
<td>mcast</td>
<td>Displays a list of registered multicast addresses.</td>
</tr>
<tr>
<td>mld</td>
<td>Displays MLD counters or parameters.</td>
</tr>
<tr>
<td>reset</td>
<td>Resets the IPv6 interface.</td>
</tr>
<tr>
<td>route</td>
<td></td>
</tr>
<tr>
<td>sizes</td>
<td>Displays buffer sizes.</td>
</tr>
<tr>
<td>sniffer</td>
<td>Sets various trace options.</td>
</tr>
<tr>
<td>static routes</td>
<td>Displays static routes.</td>
</tr>
<tr>
<td>packet-filter</td>
<td>Displays configured packet filters.</td>
</tr>
<tr>
<td>path-mtu</td>
<td></td>
</tr>
<tr>
<td>ping6</td>
<td>Activates Ping.</td>
</tr>
<tr>
<td>traceroute6</td>
<td>Dynamically traces a route.</td>
</tr>
<tr>
<td>tunnels</td>
<td>Displays configured tunnels.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level.</td>
</tr>
</tbody>
</table>

Chapter 15. Configuring and Monitoring IPv6
IPv6 Monitoring Commands (Talk 5)

Access-control

Use the `access-control` command to monitor configured access control records.

Syntax:
```
access-control
```

Cache

Use the `cache` command to display

Syntax:
```
cache
```

Example:
```
IPv6> cache
```

Counters

Use the `counters` command to display the status of counters.

Syntax:
```
counters
```

Example:
```
IPv6> counters
Routing errors
Count Type
  0  Routing table overflow
  0  Net unreachable
  0  Bad subnet number
  0  Bad net number
  0  Unhandled broadcast
  0  Unhandled anycast
  0  Unhandled directed broadcast
  0  Attempted forward of LL broadcast
  0  None

Packets discarded through filter  0
IP multicasts accepted:  0

IP input packet overflows
Net  Count
  ATM/0  0
  NHRPL/0  0
  TKR/0  0
  TKR/1  0
  FR/0  0
  PPP/0  0
  IP64/0  0
```

Dump routing tables

Use the `dump` command to display the configured routing tables.

Syntax:
```
dump
```

Example:
IPv6 Monitoring Commands (Talk 5)

IPv6>dump
Type Dest net/Prefix Cost Age Next hop(s)
Stat* 1:2:3:4:5:6:7:8/128 100 30 IP64/0

IPv6 Routing table size: 768 nets (79872 bytes), 1 nets known
0 nets hidden, 0 nets deleted, 0 nets inactive
0 routes used internally, 767 routes free

Interface addresses

Use the interface command to display addresses configured on the interface.

Syntax:
interface

Example:
IPv6>interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Net:Status</th>
<th>State</th>
<th>MTU</th>
<th>redir</th>
<th>Address/Prefixlen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth/0</td>
<td>0: DWN</td>
<td>DWN</td>
<td>1500</td>
<td>Enabled</td>
<td>2003:6:14:1::610/64</td>
</tr>
<tr>
<td>Eth/1</td>
<td>1: DWN</td>
<td>DWN</td>
<td>1500</td>
<td>Enabled</td>
<td>2003:7:6:1::610/64</td>
</tr>
<tr>
<td>IP64/0</td>
<td>3: UP</td>
<td>UP</td>
<td>2048</td>
<td>Enabled</td>
<td>FE80::14FF:FE80:3/64</td>
</tr>
</tbody>
</table>

Internal address

Use the internal command to display the specified internal address.

Syntax:
internal

Mcast

Use the mcast command to display configured multicast addresses.

Syntax:
mcast

Example:
IPv6>mcast
List of IPV6 registered multicast addresses

Interface: Eth/0:

<table>
<thead>
<tr>
<th>Address/Ref_Cnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF02::1/1</td>
</tr>
<tr>
<td>FF02::2/1</td>
</tr>
<tr>
<td>FF02::1:FF00:610/1</td>
</tr>
<tr>
<td>FF02::1:FF02:6200/1</td>
</tr>
<tr>
<td>FF02::9/1</td>
</tr>
</tbody>
</table>

Mld

Use the mld command to display configured.

Syntax:
mld counters
IPv6 Monitoring Commands (Talk 5)

Example:

IPv6>mld counters
Net Querier Polls Sent Polls Rcvd Reports Rcvd
--- ------- ---------- ---------- ------------

IPv6>mld parameters
Net Robustness Query Interval Response Interval Leave Query Interval
Variable (secs) (secs) (secs)
--- ---------- -------------- ----------------- -------------------

IPv6>

Reset

Use the reset command to dynamically reset the IPv6 interface.

Syntax:
reset

Example:
IPv6>reset ipv6

Route

Use the route command to show the route to the IPv6 address.

Syntax:
route

Example:
IPv6>route 6::9
IPv6>

Sizes

Use the sizes command to display configured buffer sizes.

Syntax:
sizes

Example:
IPv6>sizes
Routing table size: 768
Table entries used: 3
Reassembly buffer size: 12000
Largest reassembled pkt: 0
Size of routing cache: 64
# cache entries in use: 0

IPv6>

Sniffer

Use the sniffer command to set various trace options.

Syntax:

Example:
Choose the trace command from this list:

1. List current traces
2. Trace source address
3. Trace destination address
4. Trace protocol
5. Trace TCP source port
6. Trace TCP destination port
7. Trace UDP source port
8. Trace UDP destination port
9. Clear trace
10. Exit

Static routes

Use the static command to display configured static routes.

Syntax:
static

Example:
IPv6> static
Net/Mask_len Cost Next hop
1234::1223/128 100 1234:0:9::8 PPP/0
232 1234:0:9:8:7:6:8 PPP/0
8::9 128 N/A filter
IPv6>

Packet-filter

Use the packet-filter command to display a summary of configured packet filters.

Syntax:
packet-filter

Example:
IPv6> pac
Name Dir Intf State #Access-Controls
packet01 Out 0 On 0
pack01 Out 5 On 2
IPv6>

Path-mtu

Use the path-mtu command to show the paths that have been identified as having an MTU that is less than the size of a packet sent along that path.

Syntax:
path-mtu

Example:
IPv6 Monitoring Commands (Talk 5)

Ping6

Use the ping6 command to ping an IPv6 address.

**Syntax:**

```
ping6
```

**Example:**

IPv6>ping
Destination IPv6 address [:]: 8::9
Source IPv6 Address [1::8]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
PING6 1::8 -> 8::9: 56 data bytes, ttl=64, every 1 sec.

```
----8::9 PING6 Statistics----
36 packets transmitted, 36 packets received
```

**Destination IPv6 address**

- **Valid Values:** Any valid IPv6 address
- **Default Value:** None

**Source IPv6 address**

- **Valid Values:** Any valid IPv6 address
- **Default Value:** None

**Ping data size in bytes**

- **Valid Values:** 0 to size of global buffer
- **Default Value:** 56

**Ping ttl**

Specifies the time-to-live for the ping.

- **Valid Values:** 1 - 255
- **Default Value:** 64

**Ping rate in seconds**

Specifies the ping frequency.

- **Valid Values:** 1 - 60
- **Default Value:** 1

Traceroute6

Use the traceroute6 command to dynamically trace a route.

**Syntax:**

```
traceroute6 ...
```

**Example:**

IPv6>traceroute6
Destination IPv6 address [:]: 7::8
Source IPv6 address [:]: 6::9
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
TRACEROUTE 6 7::8: 56 data bytes
1 * * * *
IPv6>

**Destination IPv6 address**
- **Valid Values:** Any valid IPv6 address
- **Default Value:** None

**Source IPv6 address**
- **Valid Values:** Any valid IPv6 address
- **Default Value:** None

**Data size in bytes**
- **Valid Values:** 0 to size of global buffer
- **Default Value:** 56

**Number of probes per hop**
- **Valid Values:** 1 - 10
- **Default Value:** 3

**Wait time between retries in seconds**
- **Valid Values:** 1 - 60
- **Default Value:** 3

**Maximum ttl**
- **Valid Values:** 1 - 255
- **Default Value:** 32

---

**Tunnels**

Use the **tunnels** command to display configured tunnels.

**Syntax:**

```
tunnels
```

**Example:**

```
IPv6>tunnels
Configured Tunnels
Tun# Remote Endpoint Local Endpoint Frag Allowed TTL MTU Net# IPv6 Address/PREFIX
1  1.2.3.4  2.3.4.5 No 100 2048 7 1:2:3:4:5:6:7:8/128

Automatic Tunnels
Tun# Remote Endpoint Frag Allowed TTL MTU
IPv6>
```
**GWCON (Talk 5) Activate Interface**

IPv6 supports the GWCON (Talk 5) **activate interface** command with the following consideration:

- If IPv6 was not configured before, you need to reboot.

All IPv6 interface-specific commands are supported by the GWCON (Talk 5) **activate interface** command.

**GWCON (Talk 5) Reset Interface**

IPv6 supports the GWCON (Talk 5) **reset interface** command with the following considerations:

- If IPv6 was not configured before, you need to reboot.
- If memory allocation fails, you need to reboot.

All IPv6 interface-specific commands are supported by the GWCON (Talk 5) **reset interface** command.

**GWCON (Talk 5) Component Reset Commands**

IPv6 supports the following IPv6-specific GWCON (Talk 5) **reset** commands:

**GWCON, Protocol IPv6, Reset IPv6 Command**

**Description:**
Rereads the SRAM and reinitializes IPv6. Also resets RIP6, NDP6, and PIM6.

**Network Effect:**
None.

**Limitations:**
None.

All IPv6 configuration changes are automatically activated except the following:

<table>
<thead>
<tr>
<th>Commands whose changes are not activated by the GWCON, protocol ipv6, reset ipv6 command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG, protocol ipv6, set routing table-size</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, set reassembly-size</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, set cache-size</td>
</tr>
</tbody>
</table>

**CONFIG (Talk 6) Immediate Change Commands**

IPv6 supports the following CONFIG commands that immediately change the operational state of the device. These changes are saved and are preserved if the device is reloaded, restarted, or you execute a dynamically reconfigurable command.

<table>
<thead>
<tr>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG, protocol ipv6, add route</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, delete route</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, change route</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, enable icmp-redirect</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, disable icmp-redirect</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, set access-control</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, set ttl</td>
</tr>
<tr>
<td>CONFIG, protocol ipv6, set path-mtu-aging-timer</td>
</tr>
</tbody>
</table>
IPv6 Monitoring Commands (Talk 5)
Chapter 16. Configuring and Monitoring Neighbor Discovery Protocol (NDP)

Configuration for NDP is done for each interface. This chapter describes how to use the NDP configuration and operating commands and includes the following sections:

- "Accessing the NDP Configuration Environment"
- "NDP Configuration Commands"
- "Accessing the NDP Monitoring Environment" on page 478
- "NDP Monitoring Commands" on page 479
- "NDP6 Dynamic Reconfiguration Support" on page 480

Accessing the NDP Configuration Environment

Use the following procedure to access the NDP configuration process.

1. At the OPCON prompt, enter `talk 6`. (For more detail on this command, refer to *The OPCON Process and Commands* in the Software User’s Guide.) For example:
   ```
   * talk 6
   Config>
   ```
   After you enter the `talk 6` command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press `Return` again.

2. At the CONFIG prompt, enter the `p ndp` command to get to the NDP6 Config> prompt.

NDP Configuration Commands

To configure NDP, enter the commands at the NDP6 Config> prompt.

Table 116. NDP Configuration Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See <a href="#">Getting Help on page xxvii</a>.</td>
</tr>
<tr>
<td>add</td>
<td>Adds a router advertisement or parameters.</td>
</tr>
<tr>
<td>change</td>
<td>Changes a router advertisement or parameters.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a router advertisement or parameters.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables router advertisement.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables router advertisement.</td>
</tr>
<tr>
<td>list</td>
<td>Lists the configuration.</td>
</tr>
<tr>
<td>set</td>
<td>Sets the DHCP Hop Count.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See <a href="#">Exiting a Lower Level Environment on page xxviii</a>.</td>
</tr>
</tbody>
</table>

Add

Use the `add` command to add a router advertisement.

```
add
   ra ...
   - dhcp-server
   ra  Adds a router advertisement.
```
NDP Configuration Commands (Talk 6)

add router advertisement on which interface
  Specifies the interface to which the router advertisement is to be added.
  
  **Valid Values**: A numeric value identifying a network interface
  **Default Value**: 0

Managed address configuration (stateful)
  Specifies whether hosts use the administered protocol for address autoconfiguration in addition to addresses autoconfigured using stateless autoconfiguration.
  
  **Valid Values**: yes or no
  **Default Value**: n
  
  If you specify yes, the DHCPv6 relay agent allows hosts to use local link addresses at address configuration time, even though the DHCPv6 server is not on the same link.

Other stateful configuration
  Specifies whether hosts use the administered protocol for autoconfiguration of other (non-address) information.
  
  **Valid Values**: yes or no
  **Default Value**: no

Include link layer address with router advertisement
  Specifies whether to include the link layer address in the router advertisement. A router may omit the link layer address in the router advertisement in order to enable inbound load sharing across multiple link layer addresses.
  
  **Valid Values**: yes or no
  **Default Value**: yes

Hop limit
  Specifies the default value to be placed in the hop limit field in the router advertisement messages sent by the router. This value is used in the hop count field of the IP header for outgoing IP packets.
  
  **Valid Values**: 0 - 255, where 0 means unspecified by this router
  **Default Value**: 0

Maximum router advertisement interval
  Specifies the maximum time, in seconds, allowed between sending unsolicited multicast router advertisements from the interface.
  
  **Valid Values**: 4 - 1800 seconds
  **Default Value**: 600

Minimum router advertisement interval
  Specifies the minimum time, in seconds, allowed between sending unsolicited multicast router advertisements from the interface.
  
  **Valid Values**: 3 - (.75 * Maximum router advertisement interval)
  **Default Value**: Maximum router advertisement interval/3

Router lifetime
  Specifies the time, in seconds, that the router is to be used as a default router.
Valid Values: 0 or 4 - 9000 seconds, where 0 indicates that the router is not being used as a default router

Default Value: (3 * Maximum router advertisement interval)

Reachable Time
Specifies the time, in seconds, that a node assumes a neighbor is reachable after having received a reachability confirmation.

Valid Values: 0 - 3 600 seconds, where 0 indicates unspecified by this router

Default Value: 0

Retransmit timer
Specifies the time, in seconds, between retransmitted neighbor solicitation messages.

Valid Values: 0 - 3 600 seconds, where 0 indicates unspecified by this router

Default Value: 0

link-mtu
Specifies the value to be placed in the MTU options sent by the router. This value should be sent on links that have a variable MTU and may be sent on other links.

Valid Values: A 32-bit unsigned integer, where 0 indicates that no MTU options are sent

Default Value: 0

dhcp-server
Adds a DHCP server.

server addresses
Specifies a list of unicast IPv6 server addresses to be used to forward the initial DHCPv6 solicitation message. If no addresses are specified, the DHCPv6 relay agent sends the packet to the DHCP servers multicast address.

Note: If you use the multicast servers address, you must enable multicast routing in the box by enabling and configuring Protocol Independent Multicast (PIM). See [Chapter 17. Configuring and Monitoring Protocol Independent Multicast Routing Protocol (PIM)] on page 483 for information.

Valid Values: Any valid IPv6 address

Default Value: None

Change

Use the change command to change a route advertisement or prefix.

Syntax:
change ...prefix ...

prefix Changes a configured prefix. Prefixes are added or deleted as you modify the IPv6 address configuration. See [Add on page 445] for more information about adding IPv6 addresses.
NDP Configuration Commands (Talk 6)

To add a prefix:

```bash
Config> p IPv6
IPv6 user configuration
IPv6 config> add addr
Which net is this address for [0]? 5
New address []? 2002:9::6204
Prefix length must be between 8 and 128 [128]? 64
IPv6 config> exit
```

To change a prefix:

```bash
Config> p ndp6
Neighbor Discovery for IPv6 user configuration
NDP6 Config> change prefix
Change Prefix Information option for which Prefix address []? 2002:2::
Use this prefix for on-link determination? [Yes]: n
Valid lifetime for Prefix [2592000]? fffffffff
Decrement the Valid Lifetime in real time? [No]:
Preferred Lifetime for Prefix [604800]? ffffffff
Decrement the Preferred Lifetime in real time? [No]:
```

Change prefix information options for which prefix address?

Specifies the IPv6 address prefix to be placed in the prefix information option in router advertisements sent from the interface.

**Valid Values:** Any valid IPv6 address

**Default Value:** None

Use this prefix for on-link determination?

Specifies the value to be placed in the on-link flag in the prefix information option. When set to yes, the prefix can be used for on-link determination. When set to no, the advertisement will make no statement about on-link or off-link properties of the prefix.

**Valid Values:** yes or no

**Default Value:** yes

Use this prefix for autonomous address configuration?

Specifies the value to be placed in the autonomous address configuration flag in the prefix information option. When set to yes, the prefix can be used for autonomous address configuration.

**Valid Values:** yes or no

**Default Value:** yes

**Valid Lifetime for Prefix?**

Specifies the amount of time, in seconds, to be placed in the valid lifetime in the prefix information option. This value represents the length of time, relative to the time that the packet is sent, that the prefix is valid for the purpose of on-link determination.

**Valid Values:** A 32-bit unsigned integer, where X'FFFFFFF' represents unlimited lifetime

**Default Value:** 259200 (which is 30 days)

Decrement the Valid Lifetime in real time?

Specifies whether the Valid Lifetime decrements in real time, resulting in a lifetime of zero at the specified time in the future OR is fixed (stays the same in consecutive router advertisements).

**Valid Values:** yes or no
Preferred lifetime for prefix
Specifies the amount of time, in seconds, to be placed in the preferred lifetime in the prefix information option. This value represents the length of time, relative to the time that the packet is sent, that addresses generated from the prefix via stateless address autoconfiguration remain preferred.

Valid Values: A 32–bit unsigned integer, where X'FFFFFFFF' represents unlimited lifetime

Default Value: 604800

Decrement the Preferred Lifetime in real time?
Specifies whether the Preferred Lifetime decrements in real time, resulting in a lifetime of zero at the specified time in the future, or is fixed (stays the same in consecutive router advertisements).

Valid Values: yes or no

Default Value: no

ra Changes a configured route advertisement. See “Add” on page 473 for a description of the parameters associated with the change ra command.

Delete
Use the delete command to remove a configured route advertisement.

Syntax:
delete dhcp-server ra

Disable
Use the disable command to disable route advertisement.

Syntax:
disable dhcp-relay ra
dhcp-relay
Disables the DHCPv6 relay agent.
ra Disables route advertisement.

Enable
Use the enable command to enable route advertisement.

Syntax:
  enable dhcp-relay ra
dhcp-relay
Enables DHCPv6 relay agent.
ra Enables route advertisement.
NDP Configuration Commands (Talk 6)

List

Use the list command to display the NDP configuration.

Syntax:
```
list dhcp
list ndp6 configuration
list prefix
list ra
```

Example:
```
NDP> list dhcp
DHCPv6 Relay Agent
----------------------
State       Hopcount
DISABLED    4
NDP>
NDP config> list ndp6

NDP config> list ra

NDP config> list prefix
NDP config>
```

Set

Use the set command to set the DHCP hop count.

Syntax:
```
set dhcp-hopcount
```

dhcp-hopcount
Specifies the number of hops to be used in relaying DHCPv6 packets.

Valid Values:

Default Value: 4

Example:
```
NDP6 Config> set dhcp-hopcount
Hop Count [4]? 4
NDP6 Config>
```

Accessing the NDP Monitoring Environment

Use the following procedure to access the NDP monitoring commands. This process gives you access to the NDP monitoring process.

1. At the OPCON prompt, enter talk 5. (For more detail on this command, refer to The OPCON Process and Commands in Software User’s Guide.) For example:
```
* talk 5
+
```

After you enter the talk 5 command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press Return again.

2. At the + prompt, enter the p ndp command to get you to the NDP> prompt.
NDP Monitoring Commands

This section describes the NDP monitoring commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the</td>
</tr>
<tr>
<td></td>
<td>options for specific commands (if available). See &quot;Getting Help&quot; on page</td>
</tr>
<tr>
<td></td>
<td>xxviii</td>
</tr>
<tr>
<td>dhcpv6-relay</td>
<td>Sets DHCPv6-relay counters and parameters.</td>
</tr>
<tr>
<td>dump</td>
<td>Displays routing tables.</td>
</tr>
<tr>
<td>list</td>
<td>Displays the configuration.</td>
</tr>
<tr>
<td>ping6</td>
<td>Dynamically pings an IPv6 address.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level</td>
</tr>
<tr>
<td></td>
<td>Environment&quot; on page xxviii</td>
</tr>
</tbody>
</table>

**DHCPv6-Relay**

Use the `dhcpv6-relay` command to set DHCPv6-Relay counters and parameters.

**Syntax:**
```
dhcpv6-relay counters parameters
```

**Example:**
```
NDP>
```

**Dump**

See "Dump routing tables" on page 489 for information about the `dump` command.

**List**

Use the `list` command to display the configuration. Only interfaces with RA configured are displayed even though a prefix may exist in the prefix list on other interfaces as a result of IPv6 address configuration.

**Syntax:**
```
list dhcpv6-relay dump routing tables ndp6 parameters ping6
```

**Example:**
```
NDP>list dhcp
```

**DHCPv6 Relay Agent**

State: DISABLED
Hopcount: 4

NDP>
NDP Monitoring Commands (Talk 5)

Router Advertisement for Interface 0 (PPP/0):

<table>
<thead>
<tr>
<th>Hop RA Interval</th>
<th>Rtr</th>
<th>Reach</th>
<th>Retrans</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>M</td>
<td>O</td>
<td>LLA</td>
</tr>
<tr>
<td>Limit</td>
<td>N</td>
<td>Y</td>
<td>0</td>
</tr>
<tr>
<td>Min</td>
<td>0</td>
<td>Max</td>
<td>200</td>
</tr>
<tr>
<td>Max</td>
<td>600</td>
<td>Life-</td>
<td>1800</td>
</tr>
<tr>
<td>Time</td>
<td>0</td>
<td>Timer</td>
<td>0</td>
</tr>
<tr>
<td>MTU</td>
<td>0</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Advertised Prefixes:

Prefix/Length On-Link Auto Valid/Preferred Life

Ping6

See [Ping6 on page 468](#) for details about the ping6 command.

NDP6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Neighbor Discovery Protocol for IPv6 (NDP6) supports the CONFIG (Talk 6) delete interface command with no restrictions.

GWCON (Talk 5) Activate Interface

NDP6 supports the GWCON (Talk 5) activate interface command with no restrictions.

The following table summarizes the NDP6 configuration changes that are activated when the GWCON (Talk 5) activate interface command is invoked:

<table>
<thead>
<tr>
<th>Commands whose changes are activated by the GWCON (Talk 5) activate interface command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG, protocol NDP6, add ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, change prefix</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, change ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, delete ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, disable ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, enable ra</td>
</tr>
</tbody>
</table>

GWCON (Talk 5) Reset Interface

NDP6 supports the GWCON (Talk 5) reset interface command with no restrictions.

The following table summarizes the NDP6 configuration changes that are activated when the GWCON (Talk 5) reset interface command is invoked:

<table>
<thead>
<tr>
<th>Commands whose changes are activated by the GWCON (Talk 5) reset interface command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG, protocol NDP6, add ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, change prefix</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, change ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, delete ra</td>
</tr>
</tbody>
</table>
GWCON (Talk 5) Component Reset Commands

NDP6 supports the following NDP6-specific GWCON (Talk 5) reset commands:

GWCON, Protocol IPV6, Reset IPV6 Command

Description:
Dynamically resets all of the NDP6 configuration parameters. See the command description under IPv6 for complete details of this command.

Network Effect:
No network disruption for NDP6.

Limitations:
None.

The following table summarizes the NDP6 configuration changes that are activated when the GWCON, protocol ipv6, reset ipv6 command is invoked:

<table>
<thead>
<tr>
<th>Commands whose changes are activated by the GWCON, protocol ipv6, reset ipv6 command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG, protocol NDP6, add ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, change prefix</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, change ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, delete ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, disable ra</td>
</tr>
<tr>
<td>CONFIG, protocol NDP6, enable ra</td>
</tr>
</tbody>
</table>
NDP Monitoring Commands (Talk 5)

Configuration for PIM is done for each interface. This chapter describes how to use the PIM configuration and operating commands and includes the following sections:

- “Using PIM”
- “Accessing the PIM Configuration Environment” on page 484
- “PIM Configuration Commands” on page 484
- “Accessing the PIM Monitoring Environment” on page 488
- “PIM Monitoring Commands” on page 489
- “PIM Dynamic Reconfiguration Support” on page 496
- “PIM for IPv6 Dynamic Reconfiguration Support” on page 497
- “Multicast Forwarding Cache Dynamic Reconfiguration Support” on page 498
- “Multicast Forwarding Cache V6 Dynamic Reconfiguration Support” on page 498

Using PIM

Protocol Independent Multicast dense mode (PIM-DM) is a broadcast and prune multicast protocol used by IP. It supports both IPv4 and IPv6 and the commands and syntax are identical for both versions. It works well in campus networks, where bandwidth is plentiful and users are closely grouped, not dispersed over a wide area of networks. PIM uses a broadcast and prune approach for the multicast forwarding of datagrams and is used when multicast groups are densely distributed across the Internet. It assumes that all downstream systems want to receive multicast datagrams and prunes back branches from those systems which do not.

PIM-DM is a soft state protocol. This means that the prune states, if not removed by some other activity (such as grafting or joining), are removed after a period of time (configurable) and the multicast data is once again broadcasted to all downstream systems where pruning once again occurs.

PIM-DM establishes adjacency to neighboring PIM routers by exchanging Hello messages with all neighbors. It keeps the adjacency active until it is timed out. As long as the neighboring routers are active and running, new Hello messages are sent to refresh the Hello state and prevent the adjacency from timing out. You can configure how often Hello messages are sent.

PIM-DM uses the unicast routing table, regardless which unicast protocol owns an entry, to perform the reverse path forwarding calculation on a received multicast datagram. Reverse path forwarding (RPF) is used to validate whether the received multicast datagram arrived on an interface that would be valid for forwarding to the source address contained in the multicast datagram. If this is an incorrect interface, the datagram is discarded, or else a new multicast entry is built and the multicast datagram is forwarded on all other interfaces (those with PIM-DM active, local host members, and any additional interfaces added by other multicast protocols). The use of unicast routes to perform RPF for input interface validation requires unicast routing to be symmetrical.

Grafting is also supported to allow hosts to dynamically join a group. This grafts a branch to an already existing multicast tree, removing all prune states where required, to ensure that the joined hosts receive the requested group multicast datagrams.
Because of the independent nature of PIM with respect to unicast routing protocols and the broadcast nature of PIM-DM, parallel paths from the source may occur and duplicate multicast data may be forwarded. PIM-DM uses an Assert procedure to choose the appropriate forwarding router when this occurs. Preferences may be configured on routers that run different unicast routing protocols to resolve which router is desired to have precedence. When unicast routing is the same, unicast metric costs to the source are used to determine the best route. And when all else is equal, the router with the largest IP interface address is chosen as the appropriate forwarder.

Use the `p pim` command at the Config> prompt to configure PIM parameters.

### Accessing the PIM Configuration Environment

Use the following procedure to access the PIM configuration process.

1. At the OPCON prompt, enter `talk 6`. (For more detail on this command, refer to “The OPCON Process and Commands” in Software User’s Guide.) For example:
   
   ```
   * talk 6
   Config>
   ```

   After you enter the `talk 6` command, the CONFG prompt (Config>) displays on the terminal. If the prompt does not appear when you first enter configuration, press Return again.

2. For IPv4, at the CONFIG prompt, enter the `p pim` command to get to the PIM Config> prompt. For IPv6, enter the `p pim6` command to get to the PIM6 Config> prompt.

### PIM Configuration Commands

To configure PIM for IPv4, enter the commands at the PIM Config> prompt. For IPv6, enter the commands at the PIM6 Config> prompt.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page xxvii.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a PIM interface.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables PIM on the device.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables PIM on the device and sets global PIM default configuration values.</td>
</tr>
<tr>
<td>list</td>
<td>Lists the configuration.</td>
</tr>
<tr>
<td>set</td>
<td>Sets PIM configuration parameter values.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxvii.</td>
</tr>
</tbody>
</table>

### Delete

Use the `delete` command to remove a configured PIM interface.

**Syntax:**

```
delete interfaceaddr
```

**Interface address**

**Example:**
Use the **disable** command to disable PIM on the device.

**Syntax:**
```
disable
```

Use the **enable** command to enable PIM on the device and set global PIM default configuration values.

**Syntax:**
```
enable
```

Use the **list** command to display the PIM configuration.

**Syntax:**
```
list [all | interface | preference | variables]
```

- **all**: Displays all PIM configuration information.
- **interface**: Displays PIM configuration information about the currently configured interfaces.
- **preference**: Displays configuration information about global PIM variables.
- **variables**: Displays configuration information about global PIM variables.

**Example:**
```
PIM Config> list i
```

<table>
<thead>
<tr>
<th>Type</th>
<th>IP Address</th>
<th>Hello Interval</th>
<th>State Holdtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>9.37.2.1</td>
<td>30</td>
<td>210</td>
</tr>
</tbody>
</table>

- **Type**: Identifies the type of interface that is configured.
- **IP address**: Identifies the IP address assigned to this interface.
- **Hello Interval**: Identifies the interval between hello messages, in seconds, sent on this interface.
- **State Holdtime**: Identifies the number of seconds to tell other devices upstream to hold PIM state for this device. For PIM, this is the amount of time for upstream devices to keep prunes alive.

**Example:**
```
PIM Config> list v
```

PIM Global Configuration Values

```
PIM: on
```
PIM Configuration Commands (Talk 6)

Graft Timeout: 3 seconds  
Assert Timeout: 210 seconds

PIM Config>
PIM: on/off  
Identifies whether PIM is currently enabled or disabled.

Graft timeout  
Identifies the number of seconds that grafts are retransmitted if no graft acknowledgement has been received.

Assert timeout  
Identifies the number of seconds that assert information learned by upstream devices is retained before reverting back to local routing information.

preference  
Displays current configured routing type metric preferences.

Example: (IPv4 only)
PIM Config> list p  
PIM Config> list p  
Direct 0  
Static 1  
OSPF 110  
RIP 120  
BGP 200

PIM Config>

Route type  
Identifies the route type supported and lists a hexadecimal value displaying the currently configured metric preference.

Set

Use the set command to change PIM configuration parameter values. You can use this command to add a new physical interface.

Syntax:
set   interface interfaceaddress helloperiod  
joinpruneholdtime  
preference routetype preferencevalue  
variables

interface

Example:
PIM Config> set interface  
Interface address []?  
Hello period [30]?
Join Prune Hold Time [210]?

Interface address

Valid Values: Any valid IP address

Default Value: None

Hello period

Specifies the number of seconds between Hello messages. On point-to-point interfaces, this value is ignored. Once the 2210 establishes adjacency, Hello messages are silenced.

Valid Values: 1 - 65535
Join prune hold time
Controls messages to inform the receiving device on how long (in seconds) to hold the state activated by the message. Prunes sent to the device remain active for this number of seconds.

Valid Values: 1 - 65535
Default Value: 210

preference routetype
This is a configured metric preference to be used in the assert process. It allows the user to selectively select which unicast route types in the unicast forwarding tables has precedence over other route types. It is of local significance only, meaning it is used for this device and all its attached PIM activated interfaces. This can be used if several unicast routing protocols are in use by this router, adjacent routers are running different routing protocols, or route types, such as default routes, are desired over learned routes.

Routetype can specify the following route types:
- direct
- static
- ospf (IPv4 only)
- rip (IPv4 only)
- bgp

Example:
PIM Config> set preference rip
RIP Metric Preference [120]?

Metric Preference
This value is sent to other routers in the assert process during duplicate multicast forwarding detection and is used with route metric costs to determine which router should be the forwarding router. All metric preferences are initially set to 0.

Range: 0 - 65535
Default Values:
- direct 0
- static 1
- ospf 110
- rip 120
- bgp 200

variables cache_life
Example:
PIM Config> set v cache_life
Mcfwd cache Holdtime [60]

Mcfwd cache holdtime
Specifies the amount of time in seconds that a multicast forwarding entry which has not been used to forward any multicast datagrams will be allowed to exist in the multicast forwarding cache before it is removed.
PIM Configuration Commands (Talk 6)

Valid Values: A numeric value greater than 0
Default Value: 60

variables assert_tout

Example:

PIM Config> set v assert_tout
PIM Assert Time Out [210]

Assert time out
The amount of time in seconds that downstream routers will save assert information received from two or more asserting upstream routers. Assert information is used to ensure the downstream routers understand who the correct upstream router is, or forwarding router, so that PIM messages may be sent to the correct router. If no further asserts are received before the assert time has expired, the assert information is discarded and the router uses local information in the unicast routing tables to determine the correct upstream forwarding router.

Valid Values: 1 - 65535
Default Value: 210

variables graft_tout

Example:

PIM Config> set v graft_tout
PIM Graft Time Out [3]

Graft time out
Specifies the number of seconds that the device that has sent a graft message, but has received no acknowledgement, will wait before sending another message.

Valid Values: 1 - 65535
Default Value: 3

Accessing the PIM Monitoring Environment

Use the following procedure to access the PIM monitoring commands. This process gives you access to the PIM monitoring process.

1. At the OPCON prompt, enter talk 5. (For more detail on this command, refer to The OPCON Process and Commands in the Software User’s Guide.) For example:

   + talk 5
   +

   After you enter the talk 5 command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press Return again.

2. For IPv4, at the + prompt, enter the p pim command to get to the PIM> prompt.
   For IPv6, at the + prompt, enter the p pim6 command to get to the PIM6> prompt.

   Example:

   + p pim
   PIM>
PIM Monitoring Commands

This section describes the PIM monitoring commands.

Table 119. PIM Monitoring Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxviii.</td>
</tr>
<tr>
<td>dump</td>
<td>Displays routing tables.</td>
</tr>
<tr>
<td>clear</td>
<td>Clears the multicast forwarding table.</td>
</tr>
<tr>
<td>interface</td>
<td>Displays the status of the interface.</td>
</tr>
<tr>
<td>join</td>
<td>Joins a multicast group.</td>
</tr>
<tr>
<td>leave</td>
<td>Leaves a multicast group.</td>
</tr>
<tr>
<td>mcache</td>
<td>Displays currently active multicast forwarding table cache entries.</td>
</tr>
<tr>
<td>mgroups</td>
<td>Displays group membership of the device’s attached interfaces.</td>
</tr>
<tr>
<td>mstats</td>
<td>Displays various multicast routing statistics.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Displays information about current adjacencies.</td>
</tr>
<tr>
<td>pim</td>
<td>Displays the PIM state database.</td>
</tr>
<tr>
<td>summary pim</td>
<td>Displays a summary of the PIM state database.</td>
</tr>
<tr>
<td>ping</td>
<td>Dynamically pings an IPv6 address.</td>
</tr>
<tr>
<td>reset</td>
<td>Dynamically resets PIM.</td>
</tr>
<tr>
<td>traceroute</td>
<td>Dynamically traces a route.</td>
</tr>
<tr>
<td>variables</td>
<td>Displays the configuration values for PIM variables.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxviii.</td>
</tr>
</tbody>
</table>

Dump routing tables

Use the dump command to display the configured routing tables.

**Syntax:**

```
dump
```

For an example of the output of this command, see the description of the dump routing table command at PIM Monitoring Commands in Protocol Configuration and Monitoring Reference Volume 1.

Clear

Use the clear command to reset the cache.

**Syntax:**

```
clear
```

**Example:**

```
PIM>clear

Mfwd Cache has been cleared!
PIM>
```

Interface

Use the interface command to display a summary of the statistics and parameters related to the interface.
PIM Monitoring Commands (Talk 5)

Syntax:
interface

Example:
PIM> interface
PIM Interface Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hello Interval</th>
<th>State Holdtime</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.32.45.1</td>
<td>30</td>
<td>210</td>
<td>up</td>
<td>TKR/0</td>
</tr>
<tr>
<td>9.10.32,23</td>
<td>30</td>
<td>210</td>
<td>up</td>
<td>TKR/1</td>
</tr>
</tbody>
</table>

IP address
Specifies the IP address of the interface.

Hello interval
Specifies the number of seconds between hello messages on this interface.

State holdtime
Specifies the number of seconds upstream devices are informed to hold state information before discarding. For PIM, this is the number of seconds a prune is active upstream.

Status
Specifies the current status of the interface.

- up The interface is up and fully operational, but does not generate the mld queries.
- disabled The interface is operational but is disabled and PIM is not active.
- down The interface is not operational.

Join

Use the `join` command to join a multicast group.

Syntax:
join

Example:
PIM> join 224.12.2.2

Leave

Use the `leave` command to leave a multicast group. This prevents the device from responding to pings and SNMP queries sent to the group address.

Syntax:
leave

Example:
PIM> leave 224.12.2.2

Mcache

Use the `mcache` command to display a list of currently active multicast cache entries. Multicast cache entries are built on demand, wherever the first matching
multicast datagram is received. There is a separate cache entry (and therefore a separate route) for each datagram source network and destination group combination.

**Syntax:**

```
mcache
```

**Example:**

```
PIM> mcache

0: TKR/0 1: TKR/1 2: TKR/2 3: IPPN/0 4: BDG/0 5: Internal

+ Prot Count Upstr Downstream +
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Owner</th>
<th>Count</th>
<th>Upstr</th>
<th>Downstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10.12.3</td>
<td>224.12.2.2</td>
<td>PIM 124</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.23.55.2</td>
<td>224.32.4.5</td>
<td>PIM 3</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
```

**Prot** Specifies the owning protocol of the multicast forwarding table entry.

**Count** Displays the number of multicast packets received for this multicast forwarding table entry.

**Upstr** Displays the neighboring network or router from which the datagram must be received in order to be forwarded.

**Downstream** Displays the total number of downstream interfaces or neighbors to which the datagram will be forwarded.

### Mgroups

Use the `mgroups` command to display the group membership of the device’s attached interfaces. Only the group membership for those interfaces on which the router is either designated router or backup designated router are displayed.

**Syntax:**

```
mgroups
```

**Example:**

```
PIM>mgroups

Local Group Database

Group Interface Lifetime (secs)

224.12.2.2 9.32.4.5 (TKR/0) 176
224.5.5.5 Internal 1
```

**Group** Displays the group address as it has been reported (through MLD) on a particular interface.

**Interface** Displays the interface address to which the group address has been reported (through MLD). The router’s internal group membership is indicated by a value of `internal`. For these entries, the lifetime field (see following description) indicates the number of applications that have requested membership in the particular group.
PIM Monitoring Commands (Talk 5)

**Lifetime**
Displays the number of seconds that the entry will persist if Membership Reports cease to be heard on the interface for the given group.

**Mstats**
Use the `mstats` command to display various multicast routing statistics. The command indicates whether multicast routing is enabled and whether the router is an inter-area and/or inter-AS multicast forwarder.

**Syntax:**
mstats

**Example:**
PIM> mstats

MOSPF forwarding: Disabled
Inter-area forwarding: Disabled
DVMRP forwarding: Enabled
PIM forwarding: Disabled

Datagrams received: 10143 Datagrams fwd (multicast): 10219
Datagrams fwd (unicast): 0 Locally delivered: 0
Unreachable source: 0 Unallocated cache entries: 0
Off multicast tree: 0 Unexpected DL multicast: 0
Buffer alloc failure: 0 TTL scoping: 0
Administrative filtering: 235

# DVMRP routing entries: 5 # DVMRP entries freed: 0
# fwd cache alloc: 1 # fwd cache freed: 0
# fwd cache GC: 0 # local group DB alloc: 0
# local group DB free: 0

PIM>

**Datagrams received**
Displays the number of multicast datagrams received by the router.

**Datagrams fwd (multicast)**
Displays the number of datagrams that have been forwarded as data-link multicasts (this includes packet replications, when necessary, so this count could very well be greater than the number received).

**Datagrams fwd (unicast)**
Displays the number of datagrams that have been forwarded as data-link unicasts.

**Locally delivered**
Displays the number of datagrams that have been forwarded to internal applications.

**Unreachable source**
Displays a count of those datagrams whose source address was unreachable.

**Unallocated cache entries**
Displays a count of those datagrams whose cache entries could not be created due to resource shortages.

**Off multicast tree**
Displays a count of those datagrams that were not forwarded either because there was no upstream neighbor or no downstream interfaces/neighbors in the matching cache entry.
PIM Monitoring Commands (Talk 5)

Unexpected DL multicast
Displays a count of those datagrams that were received as data-link multicasts on those interfaces that have been configured for data-link unicast.

Buffer alloc failure
Displays a count of those datagrams that could not be replicated because of buffer shortages.

TTL scoping
Indicates those datagrams that were not forwarded because their TTL indicated that they could never reach a group member.

Administrative filtering
Displays the number of datagrams discarded because of outbound filtering.

#fwd cache alloc
Indicates the number of cache entries allocated. The current forwarding cache size is the number of entries allocated (# fwd cache alloc) minus the number of cache entries freed (# fwd cache freed).

#fwd cache freed
Indicates the number of cache entries freed. The current forwarding cache size is the number of entries allocated (# fwd cache alloc) minus the number of cache entries freed (# fwd cache freed).

#fwd cache GC
Indicates the number of cache entries were cleared because they were not recently used and the cache overflowed.

#local group DB alloc
Indicates the number of local group database entries allocated. The number allocated (# local group DB alloc) minus the number freed (# local group DB free) equals the current size of the local group database.

#local group DB free
Indicates the number of local group database entries freed. The number allocated (# local group DB alloc) minus the number freed (# local group DB free) equals the current size of the local group database.

Neighbor

Use the neighbor command to display information about neighbor PIM devices and their adjacency status.

Syntax:
neighbor

Example:
PIM>neighbor
PIM Neighbor Listing

<table>
<thead>
<tr>
<th>Neighbor Addr</th>
<th>DR</th>
<th>Last Heard</th>
<th>First Heard</th>
<th>Ifc</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.12.2.2</td>
<td>NO</td>
<td>21</td>
<td>6139</td>
<td>TKR/0</td>
</tr>
<tr>
<td>9.25.3.111</td>
<td>YES</td>
<td>29</td>
<td>6204</td>
<td>TKR/1</td>
</tr>
</tbody>
</table>

PIM>

Neighbor Addr
Identifies if this router has identified the neighbor as the designated router.

DR
Identifies if this router has identified the neighbor as the designated router.
PIM Monitoring Commands (Talk 5)

**Last Heard**
The number of seconds since last heard from the neighbor.

**First Heard**
The total number of seconds since the adjacency was first established to this neighbor.

**Ifc**
The interface that the neighbor was discovered on.

**PIM**
Use the `pim` command to display the PIM state database.

**Syntax:**
```
pim
```

**Example:**
```
PIM>pim
  PIM State Database
  -------------------
  Interface Group Source Lifetime (sec)
  1 PRUNE 224.12.2.2 9.32.4.128 205
  1 PRUNE 224.23.121.4 9.124.23.1 155
PIM>
```

**Group**
The destination group address associated with the entry.

**Source**
The source address of the originator of the multicast datagram.

**Interface**
The PIM interface number and the type of PIM state in the database.

**Lifetime**
The total lifetime, in seconds, of the state received, obtained from the PIM control message that set up the state.

**Summary PIM**
Use the `summary pim` command to display summary information about the PIM state database.

**Syntax:**
```
summary pim
```

**Example:**
```
PIM>s
  Summary PIM State Database
  --------------------------
  0) Group: 224.0.1.42
  0) Source: 9.37.179.1
  0) States: 1-P 2-P
PIM>
```

**Group**
The destination group address associated with the entry.

**Source**
The source address of the originator of the multicast datagram.

**States**
Displays the interfaces and states associated to the source group pair. P identifies a prune state.
Ping

Use the **ping** command to dynamically ping another destination IPv6 address.

**Syntax:**

```
ping
```

For an example of the output of this command see the description of the **ping** command at [P Monitoring Commands](#) in Protocol Configuration and Monitoring Reference Volume 1.

See [*Ping6*](#) on page 468 for a description of the parameters.

Reset

Use the **reset** command to reset PIM and reload the configuration.

**Syntax:**

```
reset
```

Example:

```
PIM> reset
```

Traceroute

Use the **traceroute** command to dynamically trace a route.

**Syntax:**

```
traceroute
```

For an example of the output of this command see the description of the **traceroute** command at [P Monitoring Commands](#) in Protocol Configuration and Monitoring Reference Volume 1. See [*Traceroute6*](#) on page 468 for a description of the parameters.

Variables

Use the **variables** command to display information about the PIM configuration variables.

**Syntax:**

```
variables
```

Example:

```
PIM> variables

PIM: on
      Graft Timeout: 3 seconds
      Assert Timeout: 210 seconds

PIM Unicast Metric Preferences
  Direct       0
  Static       1
  OSPF         110
  RIP          120
  BGP          200

PIM>
```
PIM Monitoring Commands (Talk 5)

**PIM: on/off**
This indicates whether PIM-DM is currently enabled or disabled.

**Graft Timeout**
The number of seconds that grafts are retransmitted if no graft acknowledgement has been received.

**Assert Timeout**
The number of seconds that assert information learned by upstream routers is retained before reverting back to local routing information.

**PIM Unicast Metric Preferences**
Displays current configured routing type metric preferences. Each route type supported is listed with a decimal value displaying the currently configured metric preference.

---

**PIM Dynamic Reconfiguration Support**
This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

**CONFIG (Talk 6) Delete Interface**
Protocol Independent Multicast (PIM) supports the CONFIG (Talk 6) delete interface command with no restrictions.

**GWCON (Talk 5) Activate Interface**
PIM supports the GWCON (Talk 5) activate interface command with the following consideration:

- PIM must be globally enabled before PIM can be activated on a network interface.

All PIM interface-specific commands are supported by the GWCON (Talk 5) activate interface command.

**GWCON (Talk 5) Reset Interface**
PIM supports the GWCON (Talk 5) reset interface command with the following consideration:

- PIM must be globally enabled before PIM can be activated on a network interface.

All PIM interface-specific commands are supported by the GWCON (Talk 5) reset interface command.

**GWCON (Talk 5) Component Reset Commands**
PIM supports the following PIM-specific GWCON (Talk 5) reset commands:

**GWCON, Protocol PIM, Reset Command**

**Description:**
Dynamically resets PIM variable values and interfaces.

**Network Effect:**
Loss of PIM neighbor adjacency on all interfaces running PIM. This may impact IP multicast forwarding, though information is corrected after a period of time during which neighbor adjacency is once again established.
PIM for IPv6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Protocol Independent Multicast for IPv6 (PIM6) supports the CONFIG (Talk 6) delete interface command with no restrictions.

GWCON (Talk 5) Activate Interface

PIM6 supports the GWCON (Talk 5) activate interface command with the following consideration:

PIM6 must be globally enabled before PIM6 can be activated on a network interface.

All PIM6 interface-specific commands are supported by the GWCON (Talk 5) activate interface command.

GWCON (Talk 5) Reset Interface

PIM6 supports the GWCON (Talk 5) reset interface command with the following consideration:

PIM6 must be globally enabled before PIM6 can be activated on a network interface.

All PIM6 interface-specific commands are supported by the GWCON (Talk 5) reset interface command.

GWCON (Talk 5) Component Reset Commands

PIM6 supports the following PIM6-specific GWCON (Talk 5) reset commands:

GWCON, Protocol PIM, Reset Command

Description:
Dynamically resets PIM6 variable values and interfaces.

Network Effect:
Loss of PIM6 neighbor adjacency on all interfaces running PIM6. This may impact IPv6 multicast forwarding, though information is corrected after a period of time during which neighbor adjacency is once again established.

Limitations:
None.

All PIM6 commands are supported by the GWCON, protocol pim, reset command.
Multicast Forwarding Cache Dynamic Reconfiguration Support

**Note:** The following commands are common among MOSPF, DVMRP, and PIM and are considered MFC commands for IPv4:
- join
- leave
- mcache
- mgroups
- mstats

Refer to [Configuring and Monitoring OSPF](#) for more information about MOSPF and [Configuring and Monitoring DVMRP](#) for more information about DVMRP. Both chapters are in [Protocol Configuration and Monitoring Reference Volume 1](#).

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

**CONFIG (Talk 6) Delete Interface**
Multicast Forwarding Cache (MFC) supports the CONFIG (Talk 6) delete interface command with the following consideration:
- IP must notify MFC of address update.

**GWCON (Talk 5) Activate Interface**
MFC supports the GWCON (Talk 5) activate interface command with the following consideration:
- IP must notify MFC of address update.

All MFC interface-specific commands are supported by the GWCON (Talk 5) activate interface command.

**GWCON (Talk 5) Reset Interface**
MFC supports the GWCON (Talk 5) reset interface command with the following consideration:
- IP must notify MFC of address update.

All MFC interface-specific commands are supported by the GWCON (Talk 5) reset interface command.

**Non-Dynamically Reconfigurable Commands**
All MFC configuration parameters can be changed dynamically.

Multicast Forwarding Cache V6 Dynamic Reconfiguration Support

**Note:** The following PIM commands are considered Multicast Forwarding Cache (MFC6) commands for IPv6:
- join
- leave
- mcache
- mgroups
- mstats
This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

**CONFIG (Talk 6) Delete Interface**
Multicast Forwarding Cache V6 (MFC6) supports the CONFIG (Talk 6) delete interface command with the following consideration:
IPv6 must notify MFC6 of address update.

**GWCON (Talk 5) Activate Interface**
Multicast Forwarding Cache V6 (MFC6) supports the GWCON (Talk 5) activate interface command with the following consideration:
IPv6 must notify MFC6 of address update.

All Multicast Forwarding Cache V6 (MFC6) interface-specific commands are supported by the GWCON (Talk 5) activate interface command.

**GWCON (Talk 5) Reset Interface**
Multicast Forwarding Cache V6 (MFC6) supports the GWCON (Talk 5) reset interface command with the following consideration:
IPv6 must notify MFC6 of address update.

All Multicast Forwarding Cache V6 (MFC6) interface-specific commands are supported by the GWCON (Talk 5) reset interface command.

**Non-Dynamically Reconfigurable Commands**
All Multicast Forwarding Cache V6 (MFC6) configuration parameters can be changed dynamically.
Chapter 18. Configuring and Monitoring Routing Information Protocol (RIP6)

RIP6 is a distance vector routing protocol. Configuration for RIP6 is done for each interface. This chapter describes how to use the RIP6 configuration and operating commands and includes the following sections:

- "Accessing the RIP6 Configuration Environment"
- "RIP6 Configuration Commands"
- "Accessing the RIP6 Monitoring Environment" on page 510
- "RIP6 Monitoring Commands" on page 510
- "RIP6 Dynamic Reconfiguration Support" on page 511

Accessing the RIP6 Configuration Environment

Use the following procedure to access the RIP6 configuration process.

1. At the OPCON prompt, enter talk 6. (For more detail on this command, refer to "The OPCON Process and Commands" in Software User’s Guide.) For example:
   
   talk 6
   Config>

   After you enter the talk 6 command, the CONFIG prompt (Config>) displays on the terminal. If the prompt does not appear when you first enter configuration, press Return again.

2. At the CONFIG prompt, enter the p rip6 command to get to the RIP6 Config> prompt.

RIP6 Configuration Commands

To configure RIP6, enter the commands at the RIP6 Config> prompt.

Table 120. RIP6 Configuration Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See Getting Help on page xxvii.</td>
</tr>
<tr>
<td>add</td>
<td>Adds RIP6 on an interface.</td>
</tr>
<tr>
<td>change</td>
<td>Changes RIP6 metric configuration values or the originating default.</td>
</tr>
<tr>
<td>delete</td>
<td>Removes RIP6 from an interface.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables RIP6 on an interface.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables RIP6 on an interface.</td>
</tr>
<tr>
<td>list</td>
<td>Lists the configuration.</td>
</tr>
<tr>
<td>set</td>
<td>Sets RIP6 metric values.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See Exiting a Lower Level Environment on page xxviii.</td>
</tr>
</tbody>
</table>

Add

Use the add command to add RIP6 on an interface.

Syntax: 
add

interface#

Specifies the interface to which RIP6 protocol is to be added.
RIP6 Configuration Commands (Talk 6)

**Note:** This interface must have an IPv6 address configured or be the virtual interface of an IPv6 over IPv4 tunnel.

**Valid Values:** Any valid interface number

**Default Value:** None

**Change**

Use the `change` command to change a RIP6 metric.

**Syntax:**
```
change originating-default rip6-in-metric rip6-out-metric
```

**originating-default**

This following configuration parameters allow you to change the originating default router.

**Always originate default route**

Enabling this parameter allows RIP6 to advertise the router as a default router (called “originating the default route”). The default router performs routing for other routers on the Internet that have packets for an unknown network destination.

**Valid Values:** Yes or No

**Default Value:** No

**Originate default dependent on BGP route availability**

This field allows user to enable or disable a router running EGP/BGP to advertise itself as a default router via its IGP (RIP6 in this case.)

**Valid Values:** Yes or No

**Default Value:** No

**From AS number**

If you are configuring RIP6 to originate a default route when EGP routes are available, you can also configure it to originate the default only if EGP routes are received from a particular AS. For example, if you want a default route generated only if an EGP route is received from AS number 12, you would set this parameter to 12. Setting the AS number to 0 means “from any AS.”

**Valid Values:** 0 - 65535

**Default Value:** None

**Destination prefix (or network number)**

If you are originating a default route when EGP routes are available, you can also choose to originate the default only if a particular route is received through the EGP. For example, if you want a default route generated only if a route to network N is received, you would set this parameter to N. Setting the network number to :: (zero) means “any route received.”

**Valid Values:** Any IPv6 unicast address, no multicast address, no loopback address, no linklocal address, no site local address, no IPv4 mapped address
Prefix length
The length of the prefix. This parameter must be configured if originate default if BGP routes available is yes.

Valid Values: 8 - 128

Default Value:

Originated default cost
This parameter specifies the cost that RIP will advertise with the default route that it originates. The cost is used to determine the shortest path for the default route to its neighbor router.

Valid Values: 1 - 16

Default Value: 1

Example:
RIP6 config> set originating
Always originate default route? [No]: Yes
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>

Example:
RIP6 config> set originating
Always originate default route? [Yes]: no
Originated default dependent on BGP6 route availability? [No]: yes
From AS number [0]? 10
Dest. prefix (or network number) [:][:] 1234::0
Prefix length must between 8 and 128 [64]? 64
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>

RIP6 in-metric
Changes the value of the RIP6 metric for the incoming RIP6 updates.

Change RIPng metric on which interface?
Specifies the interface number on which RIP6 input metric is to be changed.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

RIP6 input Metric
Changes the value of the RIP6 metric on incoming RIP6 updates.

Valid Values: 1 - 15
RIP6 Configuration Commands (Talk 6)

Default Value: 1

rip6-out-metric
Changes the RIP6 metric on the outgoing RIP6 updates.

Change RIPng metric on which interface?
Specifies the interface number on which RIP6 output metric is to be changed.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

RIP6 output Metric
Specifies the value of the RIP6 metric on outgoing RIP6 updates.

Valid Values: 0 - 15

Default Value: 0

Delete

Use the delete command to remove RIP6 from the specified interface.

Syntax:

delete

interface#

Specifies the interface from which RIP6 protocol is to be removed.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: None

Disable

Use the disable command to disable RIP6.

Syntax:

disable

override ...

rip6

sending ...

override ...

static-routes

Overrrides RIP6 static routes on an interface.

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be disabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0
Overrides RIP6 default routes on an interface.

**Modify RIP6 flags on which interface?**
Specifies the interface number on which RIP6 is to be disabled.

**Note:** The interface must have RIP6 configured.

**Valid Values:** Any valid interface number

**Default Value:** 0

Disables RIP6 on the specified interface.

**Valid Values:** Yes or No

**Default Value:** Yes

**Modify RIP6 flags on which interface?**
Specifies the interface number on which RIP6 is to be disabled.

**Note:** The interface must have RIP6 configured.

**Valid Values:** Any valid interface number

**Default Value:** 0

Disables advertisement of all RIP6 routes on an interface.

**Valid Values:** Yes or No

**Default Value:** Yes

Disables advertisement of RIP6 default routes on an interface.

**Valid Values:** Yes or No

**Default Value:** Yes

Disables advertisement of RIP6 static routes on an interface.

**Valid Values:** Yes or No

**Default Value:** Yes

Disables poison reverse in sending RIP6 updates on an interface.

**Valid Values:** Yes or No
RIP6 Configuration Commands (Talk 6)

Default Value: Yes

Enable

Use the `enable` command to enable RIP6.

**Syntax:**

```
enable                              override ...
   rip6                              Sending ...
override ...
```

**static-routes**

Overrides RIP6 static routes on an interface.

**Modify RIP6 flags on which interface?**

Specifies the interface number on which RIP6 is to be enabled.

**Note:** The interface must have RIP6 configured.

**Valid Values:** Any valid interface number

**Default Value:** 0

**default**

Overrides RIP6 default routes on an interface.

**Modify RIP6 flags on which interface?**

Specifies the interface number on which RIP6 is to be enabled.

**Note:** The interface must have RIP6 configured.

**Valid Values:** Any valid interface number

**Default Value:** 0

**rip6**

Enables RIP6 on the specified interface.

**Valid Values:** Yes or No

**Default Value:** Yes

**Modify RIP6 flags on which interface?**

Specifies the interface number on which RIP6 is to be enabled.

**Note:** The interface must have RIP6 configured.

**Valid Values:** Any valid interface number

**Default Value:** 0

**sending ...**

**Modify RIP6 flags on which interface?**

Specifies the interface number on which RIP6 is to be enabled.

**Note:** The interface must have RIP6 configured.

**Valid Values:** Any valid interface number
RIP6 Configuration Commands (Talk 6)

Default Value: 0

**all-routes**

Enables advertisement of all RIP6 routes on an interface.

**Valid Values**: Yes or No

**Default Value**: Yes

**default-routes**

Enables advertisement of RIP6 default routes on an interface.

**Valid Values**: Yes or No

**Default Value**: Yes

**static-routes**

Enables advertisement of RIP6 static routes on an interface.

**Valid Values**: Yes or No

**Default Value**: Yes

**poisoned-reverse-routes**

Enables poison reverse in sending RIP6 updates on an interface.

**Valid Values**: Yes or No

**Default Value**: Yes

**List**

Use the `list` command to display the RIP6 configuration.

**Syntax:**

```
list
```

**Example:**

```
RIP6>list all
RIP6
Nets: - 0 RIP6: ENABLED
Send: static routes
    Poison reverse enabled.
Receive: Not override default and static routes
    RIP interface input metric: 1
    RIP interface output metric: 0

RIP6 default origination: BGP6(AS=10, net/prefix_len=1234::/64), cost = 1
Import BGP6 routes: enabled - AUTOTAG: enabled
```

**Set**

Use the `set` command to set RIP6 configuration parameters.

**Syntax:**

```
set
```

```
import bgp6 routes
originating default
rip6-in-metric
rip6-out-metric
```

**Example:**

```
import bgp6 routes
```

This parameter specifies that routes learned by BGP6 will be imported into
the RIP6 routing network. Only routes that appear in the BGP6 input exchange tables will be imported. All routes are imported with their cost equal to their routing table cost.

Valid Values: Yes or No

Default Value: Yes

If the routes learned by BGP6 are imported into the RIP6 routing network, the following parameter can be configured:

Enable autotag
This parameter allows RIP6 to automatically generate tags for BGP6 routes. The tag value is the AS number from which the route is learned.

Valid Values: Yes or No

Default Value: Yes

Example:
RIP6 config> set import
Import BGP6 routes?? [Yes]:
Enable AUTOTAG? [Yes]:
AUTOTAG is updated dynamically

originating default
This following configuration parameters allow you to set RIP6 to advertise the router as a default router.

Always originate default route
Enabling this parameter allows RIP6 to advertise the router as a default router (called originating the default route). The default router performs routing for other routers on the Internet that have packets for an unknown network destination.

Valid Values: Yes or No

Default Value: No

Originate default dependent on BGP route availability
This field allows user to enable or disable a router running EGP/BGP to advertise itself as a default router via its IGP (RIP6 in this case.)

Valid Values: Yes or No

Default Value: No

From AS number
If you are configuring RIP6 to originate a default route when EGP routes are available, you can also configure it to originate the default only if EGP routes are received from a particular AS. For example, if you want a default route generated only if an EGP route is received from AS number 12, you would set this parameter to 12. Setting the AS number to 0 means “from any AS”.

Valid Values: 0 - 65535

Default Value: None

Destination prefix (or network number)
If you are originating a default route when EGP routes are available, you can also choose to originate the default only if a particular route is received through the EGP. For example, if you
want a default route generated only if a route to network N is received, you would set this parameter to N. Setting the network number to :: (zero) means “any route received”.

Valid Values: Any IPv6 unicast address, no multicast address, no loopback address, no linklocal address, no site local address, no IPv4-mapped address

Default Value: None

Prefix length
The length of the prefix. This parameter must be configured if originate default if BGP routes available is yes.

Valid Values: 8 - 128

Default Value:

Originated default cost
This parameter specifies the cost that RIP will advertise with the default route that it originates. The cost is used to determine the shortest path for the default route to its neighbor router.

Valid Values: 1 - 16

Default Value: 1

Example:
RIP6 config>set originating
Always originate default route? [No]: Yes
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>

Example:
RIP6 config>set originating
Always originate default route? [Yes]: no
Originate default dependent on BGP6 route availability? [No]: yes
From AS number [0]? 10
Dest. prefix (or network number) [::]? 1234::0
Prefix length must between 8 and 128 [64]? 64
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>

rip6-in-metric
Sets the RIP6 metric on incoming RIP6 updates.

Change RIPng metric on which interface?
Specifies the interface number on which RIP6 input metric is to be set.

Valid Values: Any valid interface number

Default Value: 0
RIP6 Configuration Commands (Talk 6)

**RIP6 input Metric**
Specifies the value of the RIP6 metric used on incoming RIP6 updates.

Valid Values: 1 - 15
Default Value: 1

**rip6-out-metric**
Sets the RIP6 metric used on outgoing RIP6 updates.

Change RIPng metric on which interface?
Specifies the interface number on which RIP6 output metric is to be set.

Valid Values: Any valid interface number
Default Value: 0

**RIP6 output Metric**
Specifies the value of the metric used on outgoing RIP6 updates.

Valid Values: 0 - 15
Default Value: 0

----

Accessing the RIP6 Monitoring Environment

Use the following procedure to access the RIP6 monitoring commands. This process gives you access to the RIP6 monitoring process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to [The OPCON Process](#) in Software User’s Guide.) For example:

```
talk 5
```

After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press Return again.

2. At the + prompt, enter the **p rip6** command to get you to the RIP6> prompt.

Example:

```
+ p rip6
RIP6>
```

RIP6 Monitoring Commands

This section describes the RIP6 monitoring commands.

Table 121. RIP6 Monitoring Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See <a href="#">Getting Help</a> on page xxvii.</td>
</tr>
<tr>
<td>dump</td>
<td>Displays routing tables.</td>
</tr>
<tr>
<td>list</td>
<td>Displays the configuration.</td>
</tr>
<tr>
<td>ping6</td>
<td>Dynamically pings an IPv6 address.</td>
</tr>
<tr>
<td>reset</td>
<td>Dynamically resets RIP6.</td>
</tr>
<tr>
<td>traceroute6</td>
<td>Dynamically traces a route.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See <a href="#">Exiting a Lower Level Environment</a> on page xxvii.</td>
</tr>
</tbody>
</table>
RIP6 Monitoring Commands (Talk 5)

Dump

See [Dump routing tables" on page 489 for information about the dump command.

List

Use the list command to display the configuration.

Syntax:
list

Example:
RIP6>list

RIP6
Intf State Metric Metric Send-Flags Receive-Flags
0 Enabled /UP 1 0 St,P

Send Flags: St=Static D=Default P=PoisonReverse
Recv Flags: OSt=Override-Static OD=Override-Default

RIP originates default with cost 1 under these conditions:
BGP6 or OSPF6 External route 1234::/64 from AS 10 available
Default origination conditions not satisfied
Import BGP6 routes: enabled - AUTOTAG: enabled

Ping6

See [Ping6" on page 468 for details about the ping6 command.

Reset

Syntax:
reset

Example:
RIP6>reset

Traceroute6

See [Traceroute6" on page 468 for details about the traceroute6 command.

RIP6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Routing Information Protocol for IPV6 (RIP6) supports the CONFIG (Talk 6) delete interface command with the following consideration:
All RIP6 configurations configured for this interface are deleted, too.

GWCON (Talk 5) Activate Interface

RIP6 supports the GWCON (Talk 5) activate interface command with the following consideration:
IPv6 must be configured for this interface
All RIP6 interface-specific commands are supported by the GWCON (Talk 5) activate interface command.
RIP6 Monitoring Commands (Talk 5)

**GWCON (Talk 5) Reset Interface**

RIP6 supports the GWCON (Talk 5) `reset interface` command with the following consideration:

All RIP6 configurations for an interface change dynamically if there is an IPv6 address configured for this interface.

All RIP6 interface-specific commands are supported by the GWCON (Talk 5) `reset interface` command.

**GWCON (Talk 5) Component Reset Commands**

Routing Information Protocol for IPv6 (RIP6) supports the following RIP6-specific GWCON (Talk 5) `reset` commands:

**GWCON, Protocol RIP6 Reset Interface (or All Interfaces) Command**

**Description:**
Dynamically changes the policies or parameters of an RIP6 interface (all RIP6 interfaces.)

**Network Effect:**
Depending on the configuration changes, it will alter the sending or receiving policies of RIP6 routes on an interface.

**Limitations:**
None.

All RIP6 commands are supported by the GWCON, protocol RIP6 reset interface (or all interfaces) command.

**CONFIG (Talk 6) Immediate Change Commands**

RIP6 supports the following CONFIG commands that immediately change the operational state of the device. These changes are saved and are preserved if the device is reloaded, restarted, or you execute a dynamically reconfigurable command.

All RIP6 Talk 6 commands are dynamic.

**Non-Dynamically Reconfigurable Commands**

All RIP6 configuration parameters can be changed dynamically.
Chapter 19. Configuring and Monitoring BGP6


This chapter describes the BGP6 configuring and monitoring commands and includes the following sections:

- "BGP6 Configuration Commands"
- "Accessing the BGP6 Configuration Environment"
- "Accessing the BGP6 Monitoring Environment" on page 528
- "BGP6 Monitoring Commands" on page 528
- "BGP6 Dynamic Reconfiguration Support" on page 536

Accessing the BGP6 Configuration Environment

To access the BGP6 configuration environment, enter the following command at the Config> prompt:

```
Config> protocol bgp6
BGP6 Config>
```

BGP6 Configuration Commands

This section describes the BGP6 configuration commands. These commands allow you to modify the BGP6 protocol behavior to meet your specific requirements. Some amount of configuration is necessary to produce a fully functional BGP6 router. Enter BGP6 configuration commands at the BGP6 Config> prompt.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxviii.</td>
</tr>
<tr>
<td>Add</td>
<td>Add BGP6 neighbors and policies.</td>
</tr>
<tr>
<td>Attach</td>
<td>Attaches receive and send policy-list to a particular neighbor.</td>
</tr>
<tr>
<td>Change</td>
<td>Modifies information that was originally entered with the add command.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes BGP6 configuration information that had been entered with the add command.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables certain BGP6 features that have been turned on by the enable command.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables BGP6 speakers, BGP6 neighbors.</td>
</tr>
<tr>
<td>List</td>
<td>Displays BGP6 configuration items.</td>
</tr>
<tr>
<td>Move</td>
<td>Changes the order in which policies and aggregates are defined.</td>
</tr>
<tr>
<td>Set</td>
<td>Sets the IPv6-route-table-scan-timer.</td>
</tr>
<tr>
<td>Update</td>
<td>Manipulates a policy in a configured policy-list name using the submenu add, delete, change and move commands.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See &quot;Exiting a Lower Level Environment&quot; on page xxviii.</td>
</tr>
</tbody>
</table>
**BGP6 Configuration Commands (Talk 6)**

**Add**

Use the **add** command to add BGP6 information to your configuration.

**Syntax:**
```
add

aggregate
neighbor
no-receive asnum
origin-polic y
policy-list
receive-policy
send-policy
```

**aggregate network prefix Prefix Length**

The **add aggregate** command causes the BGP6 speaker to aggregate a block of addresses, and advertise a single route to its BGP6 neighbors. You must specify the network prefix common to all the routes being aggregated and its prefix length. The following example illustrates how to aggregate a block of addresses.

1. The **network prefix** specifies the addresses being affected. The prefix is the first address in a range of addresses specified in a BGP6 policy.
   - **Valid Values:** a valid IPv6 unicast address or IPv4 compatible address, excluding the following:
     - link-local addresses (FE80::<)
     - site-local addresses (FEC0::<)
     - loopback address (::1)
     - IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)
   - **Default Value:** none

2. The **prefix length** applies to the address specified in Network Prefix to generate an address used in a BGP6 policy.
   - **Valid Values:** 8 - 128
   - **Default Value:** 64

**Example:**
```
add aggregate
```
```
Network Prefix []? 2000::<
Prefix Length [64]? 16
```

When you add an aggregate definition, remember to define a policy to block the aggregated routes from being exported. If you do not, the router will advertise both the individual routes and the aggregate you have defined. This does not apply when you are aggregating the routes, which are originated from its IGP routing table.

**neighbor neighbor address AS# init timer connect timer hold timer keep alive timer tcp segment size**

Use the **add neighbor** command to define a BGP6 neighbor. The neighbor can be internal to the BGP6 speaker’s AS, or external. To activate this neighbor dynamically use the **reset neighbor** command from BGP6 monitoring.

**Neighbor address**

The **neighbor address** is the IPv6 address of the neighbor you wish to peer with. It could be within your own autonomous system or in another autonomous system. If it is an external neighbor, both BGP6 speakers must share the same network. There is no such restriction for internal neighbors.
BGP6 Configuration Commands (Talk 6)

Valid Values: a valid IPv6 unicast address or IPv4 compatible address, excluding the following:

- link-local addresses (FE80::)
- site-local addresses (FEC0::)
- loopback address (::1)
- IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)
- zero address (::0)

Default Value: none

AS#

The AS# is your own autonomous system number for internal neighbor or neighbor’s autonomous system number. The AS number of the neighbor has:

Valid Values: An integer in the range of 1 - 65535
Default Value: 1

Init timer

The init timer to specify the amount of time the BGP6 speaker waits to initialize resources and reinitiate transport connection with the neighbor in case the speaker has previously changed to IDLE state due to an error. If the error persists, this timer increases exponentially.

Valid Values: 0 to 65535 seconds.
Default Value: 12 seconds

Connect timer

The connect timer specifies the amount of time the BGP6 speaker waits to reinitiate transport connection to its neighbor, if the TCP connection fails while in either CONNECT or ACTIVE state. In the mean time, the BGP6 speaker continues to listen for any connection that may be initiated by its neighbor.

Valid Values: 0 to 65535 seconds.
Default Value: 120 seconds

Hold timer

Enter the hold timer to specify the length of time the BGP6 speaker waits before assuming that the neighbor is unreachable. Both neighbors exchange the configured information in OPEN message and choose the smaller of the two timers as their negotiated Hold Timer value.

Once neighbors have established BGP6 connection, they exchange Keepalive messages at frequent intervals to ensure that the connection is still alive and the neighbors are reachable. The Keep-Alive timer interval is calculated to be one-third of the negotiated hold timer value. Hence the hold timer value must be either zero or at least three seconds.

Note that on switched lines, you may wish to use the Hold Timer value of zero to save bandwidth by not sending Keepalives at frequent intervals.

Valid Values: 0 to 65535 seconds.
Default Value: 90 seconds

TCP segment size

The TCP segment size specifies the maximum data size that may be exchanged on the TCP connection with a neighbor. This value is used for active TCP connection with the neighbor.

Valid Values: 1 to 65535 bytes.
BGP6 Configuration Commands (Talk 6)

Default Value: 1220 bytes

Example:

```
add neighbor
```

Neighbor address []? 2002:9::6205
AS [1]? 2002
Init timer [12]?
Connect timer [120]?
Hold timer [90]?
TCP segment size [1220]?

**no-receive AS#**

Use the `add no-receive AS#` to exclude AS-paths if the particular AS number appears anywhere inside the AS-path list.

The **AS#** has:

- **Valid Values**: 1 to 65535
- **Default Value**: 1

Example:

```
add no-receive
```

Enter AS: [1]? 2003

**originate-policy** (exclusive/ inclusive) network prefix Prefix Length address match (Exact/Range) tag

Use the `add originate-policy` command to specify the value to use in selecting routes for advertisement.

**Exclusive**

Exclusive policies prevent route information from being included in the BGP6 speaker’s routing table.

**Inclusive**

Inclusive policies ensure that specific routes will be included in the BGP6 speaker’s routing table.

**Network prefix**

This parameter specifies the network address affected by this policy.

- **Valid Values**: a valid IPv6 unicast address or IPv4 compatible address, excluding the following:
  - link-local addresses (FE80::)
  - site-local addresses (FEC0::)
  - loopback address (::1)
  - IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)
- **Default Value**: none

**Prefix length**

The `prefix length` applies to the address specified in Network Prefix to generate an address used in a BGP6 policy.

- **Valid Values**: 0 - 128
- **Default Value**: 0

**Address match**

The address, or range of addresses, that will be affected by the policy statement.

- **Valid Values**: Exact or Range
- **Default Value**: Range

**Tag**

The tag value represents the AS number from which the route is
The following example includes all routes in the BGP6 speaker’s IGP routing table to be advertised.

Example:
```
add originate-policy inclusive
```

**policy-list**

Use the `add policy-list` command to configure a group of policies, which can be attached to a specific neighbor using the `attach policy-to-neighbor` command.

**Name** Specifies the name to be used to identify the group of policies.

- **Valid Values**: A string of 1 - 15 ASCII characters
- **Default Value**: None

**Example: add policy-list**
```
Name[]? nbr1-rcv
Policy Type(Receive/Send)[Receive]? Receive
```

**Example: add policy-list**
```
Name[]? nbr1-snd
Policy Type(Receive/Send)[Receive]? Send
```

**receive-policy** (exclusive/ inclusive) network prefix Prefix Length address match originating AS# adjacent AS# igpmetric (inclusive only)

Use the `add receive-policy` command to determine what routes will be imported to the BGP6 speaker’s routing table.

Exclusive policies prevent route information from being included in the BGP6 speaker’s routing table.

Inclusive policies ensure that specific routes will be included in the BGP6 speaker’s routing table.

**Network prefix**

Specifies the addresses being affected.

- **Valid Values**: a valid IPv6 unicast address or IPv4 compatible address, excluding the following:
  - link-local addresses (FE80::)
  - site-local addresses (FEC0::)
  - loopback address (::1)
  - IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)
- **Default Value**: none

**Prefix Length**

The **prefix length** applies to the address specified in network prefix to generate an address used in a BGP6 policy.

- **Valid Values**: 0 - 128
- **Default Value**: 0
BGP6 Configuration Commands (Talk 6)

Address match
The address match is a range of addresses or an exact address.
Valid Values: Exact or Range
Default Value: Range

Originating AS#
An originating AS# has:
Valid Values: 0 to 65535
Default Value: 0

Adjacent AS#
The adjacent AS# specifies the neighboring AS number.
Valid Values: 0 to 65535
Default Value: 0

IGP metric
The IGP metric (for inclusive receive-policies only) specifies the metric value with which the accepted routes are imported into the speaker’s IGP routing table. If the IGP metric is -1, these routes will not be imported into the IGP; thus, these routes are not re-advertiseable.
Valid Values: -1 to 65535
Default Value: 0

Example:
add receive-policy exclusive
Network Prefix [:]: 2003::
Prefix length [0]: 16
Address Match [Exact/Range] [Range]?
Originating AS# [0]: 168
Adjacent AS# [0]: 165

Example:
add receive-policy inclusive
Network Prefix [:]: 2000::
Prefix Length [0]: 64
Address Match [Exact/Range] [Range]?
Originating AS# [0]?
Adjacent AS# [0]?
IGP-metric [0]?

send-policy (exclusive/ inclusive) network prefix Prefix Length address match tag adjacent AS#

Use the add send-policy command to create policies that determine which of the BGP6 speaker’s learned routes will be readvertised. These routes could be internal or external to the BGP6 speaker’s AS.

Exclusive policies prevent route information in the BGP6 speaker’s routing table from being advertised to BGP6 neighbors.

Inclusive policies ensure that specific routes in the BGP6 speaker’s routing table will be advertised to BGP6 neighbors.

Network prefix
The network prefix is for the addresses being affected.
Valid Values: a valid IPv6 unicast address or IPv4 compatible address, excluding the following:
– link-local addresses (FE80::)
– site-local addresses (FEC0::)
– loopback address (::1)
– IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)
Default Value: none
Prefix length
The prefix length applies to the address specified in Network Prefix to generate an address used in a BGP6 policy.
Valid Values: 0 - 128
Default Value: 0

Address match
The Address match is a range of addresses or an exact address.
Valid Values: Exact or Range
Default Value: Range

Tag
The tag value represents the AS number from which the route is learned. The tag value is used for interacting with an IGP, like RIP6. See "Set" on page 507 for information on importing BGP6 routes and BGP6 autotag generation.
Valid Values: 0 to 65535
Default Value: 0

Adjacent AS#
The adjacent AS# specifies the neighboring AS number.
Valid Values: 0 to 65535
Default Value: 0

Example:
add send exclusive
Network Prefix []? 2003::
Prefix length[0]? 16
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]?

Attach
Use the attach policy-to-neighbor command to attach a configured policy-list name to a specific neighbor. You can attach up to three receive and three send policy-list names.

Syntax:
attach policy-to-neighbor

Example: attach policy-to-neighbor
Neighbor address [:]?: 2003::
First receive policy list name (none for global AS based policy)[ ]? nbr1-rcv
Second receive policy list name (none for exit)[ ]?
First send policy list name (none for global AS based policy)[ ]? nbr1-snd
Second send policy list name (none for exit)[ ]?

Change
Use the change command to change a BGP6 configuration item previously installed by the add command.

Syntax:
change aggregate . . .
eighbor . . .
origin-polic y . . .
policy-to-neighbor
receive-policy . . .
BGP6 Configuration Commands (Talk 6)

send-policy...

generate index# network prefix Prefix Length
This example changes the current aggregate (aggregate 1).
Example:
change generate 1
    Network Prefix [2000::]? 2001::
    Prefix Length [16]?

neighbor neighbor IPv6 address AS# init timer connect timer hold timer keep alive
timer tcp segment size
Use this command to change the configuration parameter values for an
existing neighbor. This command may not be used to change the address
for an existing neighbor.

To reactivate the neighbor dynamically use the reset neighbor command
from BGP6 monitoring.

The neighbor address to be modified has:
    Valid Values: Any currently configured neighbor address
    Default Value: none

The following example changes the value of the hold timer to zero for
neighbor 2002:0::6205.
Example:
change neighbor 2002:0::6205
    AS [2002]? 2002::
    Init timer [12]? 12
    Connect timer [60]? 60
    Hold timer [12]? 0
    TCP segment size [1220]?

originate-policy index# (exclusive/inclusive) network prefix Prefix Length address
match tag
Use the change originate-policy command to alter an existing originate
policy definition.

This example alters the BGP6 speaker's originate policy.
Example:
change originate-policy
    Enter index of originate-policy to be modified [1]?
    Policy Type (Inclusive/Exclusive) [Exclusive]?
    inclusive
    Network Prefix [2003::]? 2004::
    Prefix Length [16]? 16
    Address Match (Exact/Range) [Range]?
    Tag [0]?

policy-to-neighbor
Use the change policy-to-neighbor command to change a policy-list
attachment to a particular neighbor.
Example:
change policy-to-neighbor
    Neighbor address [0::0]? 2003::
    First receive policy list name to be changed[nbr1-rcv]?
    Second receive policy list name to be changed[]?
    Third receive policy list name to be changed[]?
    First send policy list name to be changed[nbr1-snd]?
    Second send policy list name to be changed[]?
    Third send policy list name to be changed[]?

receive-policy index# (exclusive/inclusive) network prefix Prefix Length address
match originating AS# adjacent AS# igpmetric (inclusive only)
Use the change receive-policy command to alter an existing receive policy
definition.
This example adds a restriction to the BGP6 speaker’s receive-policy. Rather than import route information from every BGP6 peer into its IGP routing table, it will now prevent routes from AS 165 from being imported.

Example:
```
code
change receive-policy
Enter index of receive-policy to be modified [1]? 1
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [2003::]? 2003::
Prefix Length [16]? 16
Address Match (Exact/Range) [Range]? 16
Originating AS# [0]? 0
Adjacent AS# [0]? 165

send-policy index# (exclusive/ inclusive) network prefix Prefix Length address
match tag adjacent AS#
```

Use the `change send-policy` command to alter an existing send policy to one that is more inclusive, or more exclusive.

This example adds a restriction to the BGP6 speaker’s send policy.

Example:
```
code
change send-policy
Enter index of send-policy to be modified [1]? 1
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0::0]? 2003::
Prefix Length [16]? 16
Address Match (Exact/Range) [Range]? Tag [0]
Adjacent AS# [0]? 165
```

Delete

Use the `delete` command to delete a BGP6 configuration item previously installed by the `add` command.

Syntax:
```
code
delete aggregate .
neighbor .
noreceive .
originatelpolicy .
policy-list .
policy-to-neighbor
receive-policy .
send-policy .
```

```
code
aggregate index#
You must specify the index number of the aggregate you want to delete.

Example: delete aggregate 1
```

```
code
neighbor neighbor IPv6 address
Use this command to delete a BGP6 neighbor. You must specify the neighbor’s network address.

The neighbor’s network address to be deleted has:
Valid Values: Any currently configured neighbor address
Default Value: none
```

To deactivate this neighbor dynamically use the `reset neighbor` command from BGP6 monitoring.
BGP6 Configuration Commands (Talk 6)

Example: delete neighbor 2002:9::6024

no-receive AS#
Use this command to delete the no-receive policy set up for a particular AS.
You must specify the AS number.

The AS# has:
  Valid Values: 1 to 65535
  Default Value: none

Example: delete no-receive 168

origin-pc[00]ey index#
Use this command to delete a specific originate policy. You must specify the
index number associated with the policy.

Example: delete originate-pc[00]ey 2

policy-list
Use the delete policy-list command to delete a policy-list.

Example: delete policy-list

Name of policy-list to delete []? nbr1-rcv
All policies defined for 'nbr1-rcv' will be deleted.
Are you sure you want to delete (Yes or [No])? Yes
Policy-list 'nbr1-rcv' is deleted.

The policy-to-neighbor attachment will be adjusted accordingly.

policy-to-neighbor
Use the delete policy-to-neighbor command to delete an existing
policy-list name attachment to a particular neighbor.

Example: delete policy-to-neighbor

Neighbor address []? 2009:9::6205
Remove first receive policy-list name [nbr1-rcv]
Are you sure you want to remove (Yes or [No])? yes
Remove first send policy-list name [nbr1-snd]
Are you sure you want to remove (Yes or [No])? yes

receive-policy index#
Use this command to delete a specific receive policy. You must specify the
index number associated with the policy.

Example: delete receive-policy

Enter index of receive-policy to be deleted [1]?

send-policy index#
Use this command to delete a specific send policy. You must specify the
index number associated with the policy.

Example: delete send-policy 4

Disable

Use the disable command to disable a previously enabled BGP6 neighbor or
speaker. Note that neighbors are implicitly enabled whenever added with the add
command.

Syntax:

  disable                      BGP6 speaker
                               compare-med-from-diff-AS
                               neighbor . . .
BGP6 Configuration Commands (Talk 6)

BGP6 speaker
Use the disable BGP6 speaker command to disable the BGP6 protocol.
Example: disable BGP6 speaker

compare-med-from-diff-AS
Use this command to disable a MED comparison between different ASs.
Example: disable compare-med-from-diff-AS

neighbor neighbor IPv6 address
Use this command to disable a currently configured neighbor. The neighbor address has:
Valid Values: Any valid IPv6 address
Default Value: none
Example: disable neighbor 2002:9::6205

Enable
Use the enable command to activate the BGP6 features, capabilities, and information added to your BGP6 configuration.

Syntax:
enable BGP6 speaker compare-med-from-diff-AS neighbor...

BGP6 speaker AS# tcp segment size
Use the enable BGP6 speaker command to enable the BGP6 protocol.
1. The AS# is associated with this collection of routers and nodes.
   Valid Values: 1 to 65535
   Default Value: 1
2. Enter the TCP segment size to specify the maximum segment size that BGP6 should use for passive TCP connections.
   Valid Values: 1 to 65535 bytes.
   Default Value: 1220 bytes
Example:
enable BGP6 speaker
AS [0]? 165
TCP segment size [1220]?

compare-med-from-diff-AS
Use this command to enable MED comparison between different ASs.
Example: enable compare-med-from-diff-AS

neighbor neighbor IPv6 address
Use this command to enable a BGP6 neighbor.
The neighbor address has:
Valid Values: Any currently configured neighbor address
Default Value: none
Example: enable neighbor 2002:9::6205

List
Use the list command to display various pieces of the BGP6 configuration data, depending on the particular subcommand invoked.
BGP6 Configuration Commands (Talk 6)

Syntax:

list aggregate
  all
  BGP6 speaker
  neighbor
  no-receive
  originate-policy
  policy-list . . .
  policy-to-neighbor
  receive-policy
  send-policy

aggregate

Use the list aggregate command to list all aggregated routes defined with the add aggregate command.

Example: list aggregate

Aggregation:
Index Prefix/Prefix length
1 2000::/16

all

Use the list all command to list the BGP6 neighbors, policies, aggregated routes, and no-receive-as records in the current BGP6 configuration.

Example: list all

BGP6 Configuration Commands (Talk 6)

 Syntax:

 list aggregate
   all
   BGP6 speaker
   neighbor
   no-receive
   originate-policy
   policy-list . . .
   policy-to-neighbor
   receive-policy
   send-policy

aggregate

Use the list aggregate command to list all aggregated routes defined with the add aggregate command.

Example: list aggregate

Aggregation:
Index Prefix/Prefix length
1 2000::/16

all

Use the list all command to list the BGP6 neighbors, policies, aggregated routes, and no-receive-as records in the current BGP6 configuration.

Example: list all

BGP6 Protocol: Enabled
AS: 710
TCP-Segment Size: 1220

Neighbors and their AS:

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>AS</th>
<th>Timer</th>
<th>Hold</th>
<th>TCPSEG</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003:7:8:2::820</td>
<td>ENABL</td>
<td>710</td>
<td>12</td>
<td>120</td>
<td>90</td>
</tr>
<tr>
<td>2002:9::6205</td>
<td>ENABL</td>
<td>2002</td>
<td>12</td>
<td>120</td>
<td>90</td>
</tr>
</tbody>
</table>

Receive-Policies:
Index Type Prefix/Prefix length Match OrgAS AdjAS IGPmet
1 INCL ::/0 Range 0 0 0
2 EXCL 2003::/16 Range 0 0

Send-Policies:
Index Type Prefix/Prefix length Match Tag AdjAS
1 INCL ::/0 Range 0 0
2 EXCL 2003::/16 Range 0 0

Originate-Policies:
Index Type Prefix/Prefix Length Match Tag
1 INCL ::/0 Range 0
2 EXCL 2003::/16 Range 0

Aggregation:
Index Prefix/Prefix Length
1 2000::/16

AS-PATH with following ASs will be discarded:
AS 2003

ipv6-route-table-scan-timer value is 2 seconds.

BGP6 speaker

Use the list BGP6 speaker command to derive information on the BGP6 speaker. The information provided is as follows:
BGP6 Configuration Commands (Talk 6)

Example:

```
list BGP6 speaker
```

<table>
<thead>
<tr>
<th>Protocol</th>
<th>AS</th>
<th>TCP-Segment Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP6</td>
<td>165</td>
<td>1220</td>
</tr>
</tbody>
</table>

neighbor

Use the `list neighbor` command to derive information on BGP6 neighbors.

Example: `list neighbor`

Neighbors and their AS along with attached policy-list name(s):

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>AS</th>
<th>Init timer</th>
<th>Conn timer</th>
<th>Hold timer</th>
<th>TCPSEG</th>
<th>Timer</th>
<th>Timer</th>
<th>Timer</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003:7:8:2::820</td>
<td>ENABLD</td>
<td>820</td>
<td>12</td>
<td>120</td>
<td>90</td>
<td>1220</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2002:9::6205</td>
<td>ENABLD</td>
<td>2002</td>
<td>12</td>
<td>120</td>
<td>90</td>
<td>1220</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

no-receive

Use the `list no-receive` command to derive information on no-receive-AS definitions that have been added to the BGP6 configuration.

Example: `list no-receive`

AS-PATH with following autonomous systems will be discarded:

- AS 178
- AS 165

originate-policy `all index prefix`

Use the `list originate-policy` command to derive information on the originate policies that have been added to the BGP6 configuration.

Example: `list originate-policy`

```
Originate-Policies:
Index Type Prefix/Prefix Length Match Tag
1 INCL ::/0 Range 0
2 EXCL 2003::/16 Range 0
```

policy-list

Use the `list policy-list` command to list configured policy-list names.

Example: `list policy-list`

If `list policy-list` is issued without the policy list name, the list of configured policy-list names is displayed.

```
Policy list: nbr1-rcv Receive
            nbr1-snd Send
```

policy-to-neighbor

Use the `list policy-to-neighbor` command to list policies attached to neighbors.

Example: `list policy-to-neighbor`

```
Neighbor address         Receive  Send
-----------------------------------------
2002:9::6205             rec1      send1
```

receive-policy `adj-as-number all or index or prefix`

Use the `list receive-policy` command to derive information on the receive policies that have been added to the BGP6 configuration. You can display all receive policies defined for an AS, or display policies by index or prefix number.

Example: `list receive-policy`

```
Receive-Policies:
Index Type Prefix/Prefix length Match OrgAS AdjAS IGPmet
1 INCL ::/0 Range 0 0 0
2 EXCL 2003::/16 Range 0 0
```

send-policy `adj-as-number all or index or prefix`

Use the `list send-policy` command to display information on send policies.
BGP6 Configuration Commands (Talk 6)

defined for specified autonomous systems. You can display all send policies defined for an AS, or display policies by index or prefix number.

Example: list send-policy

Send-Policies:

<table>
<thead>
<tr>
<th>Index</th>
<th>Type</th>
<th>Prefix/Prefix length</th>
<th>Match</th>
<th>Tag</th>
<th>AdjAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>INCL</td>
<td>::/0</td>
<td>Range</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>EXCL</td>
<td>2003::/16</td>
<td>Range</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Move

Use the move command to change the order in which policies and aggregates have been defined. This changes the order in which the router applies existing policies to route information. Before using this command, it is advisable to use the list command to see what policies have been defined.

Syntax:

move aggregate or originate-policy or receive-policy or send-policy

Example:

move originate-policy
Enter index of originate-policy to move [1]? 3
Move record AFTER record number [0]?

Set

Use the set command to set the IPv6-route-table-scan-timer. The IPv6-route-table-scan-timer value is used to set the IPv6 forwarding table scanning time interval for BGP6 updates.

Syntax:

set ipv6-route-table-scan-timer

Valid Values: 1 to 10
Default Value: 1

Example:

set ipv6-route-table-scan-timer
Timer Value in seconds [1]? 2

Update

Use the update command and sub-commands to manipulate policies.

Syntax:

update policy-list

Receive Policy Example:

update policy-list
Name[]? nbr1-rcv

Add

Use the Add command to add receive or send policies within the update command.

Example: Adding a receive policy
BGP6 Configuration Commands (Talk 6)

BGP6 Config>add POLICY-LIST
Policy-list name []? rec1
Policy Type (Receive/Send) [Receive]?
BGP6 Config>UPDATE POLICY-LIST
Policy-list name []? rec1
Policy-list rec1:Receive Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]?
Network Prefix []: ? 1234::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
Policy-list rec1:Receive Config>list
Receive Policy list for rec1:
Idx T Prefix/Length/Match OrgAS AnyAS MED Weight
LP IGPm
1 E 1234::/16/R 0 0
Policy-list rec1:Receive Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]? inc
Network Prefix []: ? 5678::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Local-pref [0]?
Weight [0]?
IGP-metric [0]?
Policy-list rec1:Receive Config>list
Receive Policy list for rec1:
Idx T Prefix/Length/Match OrgAS AnyAS MED Weight
LP IGPm
1 E 1234::/16/R 0 0
2 I 5678::/16/R 0 0 0 0

Example: Adding a send policy
BGP6 Config>add POLICY-LIST
Policy-list name []? send1
Policy Type (Receive/Send) [Receive]? send
BGP6 Config>UPDATE POLICY-LIST
Policy-list name []? send1
Policy-list send1:Send Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]? i
Network Prefix []: ? 1234::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
Tag [0]?
MED [0]?
# of AS padding [0]?
Policy-list send1:Send Config>list
Send Policy list for send1:
Idx T Prefix/Length/Match OrgAS AnyAS Tag MED
ASpad
1 I 1234::/16/R 0 0 0 0

Notes:
1. There will be no prompting for MED, Local-pref, Weight, and IGP-metric parameters for exclusive receive policy. MED, Local-pref values will be used from received advertisement if they are configured as value ‘0’. The value ‘0’ for the Weight parameter indicates to ignore the weight value in the route selection process.
2. Prompting for MED and # of AS padding parameter values occurs only for inclusive send policies.
BGP6 Configuration Commands (Talk 6)

**Change**
Use the *Change* command to change policies within the *update* command.

**Example:**
Enter index of receive-policy to be modified [1]?

**Delete**
Use the *delete* command to delete policies within the *update* command.

**Example:**
Enter index of receive-policy to be deleted [1]?

**Move**
Use the *move* command to move policies within the *update* command.

**Example:**
Enter index of receive-policy to move [1]?
Move record after record number [0]?

**List**
Use the *list policy-list* command to list receive policies within the *update* command.

**Example:**
list policy-list

<table>
<thead>
<tr>
<th>Receive Policy list for rec1:</th>
<th>OrgAS</th>
<th>AnyAS</th>
<th>MED</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idx T Prefix/Length/Match</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LP</td>
<td>IGPm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>E 1234::/16/R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>I 5678::/16/R</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Send Policy Example:**
update policy-list
Name[]? nbr1-rcv

Accessing the BGP6 Monitoring Environment

To access the BGP6 monitoring environment, enter the following command at the + prompt:

```
+ protocol bgp6
BGP6>
```

**BGP6 Monitoring Commands**

This section describes the BGP6 monitoring commands. These commands allow you to modify the BGP6 protocol behavior to meet your specific requirements. Some amount of configuration is necessary to produce a fully functional BGP6 router. Enter BGP6 monitoring commands at the BGP6> monitoring prompt.

**Table 123. BGP6 Monitoring Command Summary**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (Help)</td>
<td>Displays all the commands available for this command level or lists the options for specific commands (if available). See &quot;Getting Help&quot; on page xxvii.</td>
</tr>
<tr>
<td>Disable neighbor</td>
<td>Disables a particular neighbor or all neighbors.</td>
</tr>
<tr>
<td>Dump routing tables</td>
<td>Lists the contents of the IPv6 routing table.</td>
</tr>
<tr>
<td>List</td>
<td>Lists all BGP routing table entries.</td>
</tr>
<tr>
<td>Enable neighbor</td>
<td>Enables a particular neighbor or all neighbors.</td>
</tr>
</tbody>
</table>
Table 123. BGP6 Monitoring Command Summary (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbors</td>
<td>Displays currently active neighbors.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Displays installed BGP6 globals in the BGP6 system.</td>
</tr>
<tr>
<td>Paths</td>
<td>Displays all available paths in the database.</td>
</tr>
<tr>
<td>Ping6</td>
<td>Sends ICMP Echo Requests to another host once a second and watch for a response. This command can be used to isolate trouble in an internetwork environment.</td>
</tr>
<tr>
<td>Policy-list</td>
<td>Displays the current installed policy for specific neighbor and usage statistics of each policy.</td>
</tr>
<tr>
<td>Reset neighbor</td>
<td>Resets a particular neighbor.</td>
</tr>
<tr>
<td>Traceroute6</td>
<td>Displays the complete path (hop-by-hop) to a particular destination.</td>
</tr>
<tr>
<td>Exit</td>
<td>Returns you to the previous command level. See [Exiting a Lower Level Environment] on page xxvii.</td>
</tr>
</tbody>
</table>

Disable Neighbor

Use the disable neighbor command to disable a particular neighbor or all neighbors that have been enabled. This command brings down the BGP6 session and removes the routes learned from that neighbor.

Syntax:

`disable neighbor IPv6 neighbor address`

Example: `disable neighbor`

Enter a Neighbor address or :: for all neighbors [ ]? ::

neighbor 2003:1::6105 disabled

Dump Routing Tables

For a complete explanation of the dump routing tables command, refer to the Dump Routing Tables command on page "Dump routing tables" on page 464.

Example:

<table>
<thead>
<tr>
<th>Type</th>
<th>Dest net/Prefix</th>
<th>Cost</th>
<th>Age</th>
<th>Next hop(s)/Net</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGPR</td>
<td>2001:6::/64</td>
<td>0</td>
<td>193</td>
<td>IP64/0</td>
</tr>
<tr>
<td>BGPR</td>
<td>2001:7::/64</td>
<td>0</td>
<td>187</td>
<td>IP64/0</td>
</tr>
<tr>
<td>BGPR</td>
<td>2001:9::/64</td>
<td>0</td>
<td>200</td>
<td>IP64/0</td>
</tr>
<tr>
<td>BGPR</td>
<td>2001:17::/64</td>
<td>0</td>
<td>200</td>
<td>IP64/0</td>
</tr>
<tr>
<td>Dir*</td>
<td>2002:2::/64</td>
<td>1</td>
<td>7889</td>
<td>Eth/1</td>
</tr>
<tr>
<td>RIP6</td>
<td>2002:5::/64</td>
<td>3</td>
<td>10</td>
<td>FE80::220:35FF:FE45:2488</td>
</tr>
<tr>
<td>Eth/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIP6</td>
<td>2002:6::/64</td>
<td>2</td>
<td>10</td>
<td>FE80::220:35FF:FE45:2488</td>
</tr>
<tr>
<td>Eth/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIP6</td>
<td>2002:9::/64</td>
<td>2</td>
<td>10</td>
<td>FE80::220:35FF:FE45:2488</td>
</tr>
<tr>
<td>Eth/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIP6</td>
<td>2002:99::/64</td>
<td>3</td>
<td>10</td>
<td>FE80::220:35FF:FE45:2488</td>
</tr>
<tr>
<td>Eth/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIP6</td>
<td>2002:1111::/64</td>
<td>3</td>
<td>10</td>
<td>FE80::220:35FF:FE45:2488</td>
</tr>
<tr>
<td>Eth/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dir*</td>
<td>2003:1::/64</td>
<td>1</td>
<td>7889</td>
<td>IP64/0</td>
</tr>
</tbody>
</table>

IPV6 Routing table size: 768 nets (79872 bytes), 11 nets known
0 nets hidden, 0 nets deleted, 1 nets inactive
0 routes used internally, 756 routes free
Enable Neighbor

Use the **enable neighbor** command to enable a particular neighbor or enable all neighbors that have been disabled. This command starts the BGP6 session with neighbor.

**Syntax:**

```
enable neighbor IPv6 neighbor address
```

**Example:**
Enter a Neighbor address or :: for all neighbors []? ::
network 2003:1::6105 enabled

List

Use the **list** command to dump all BGP6 routing table entries, or to display information on routes advertised to, or received from, specified BGP6 neighbor addresses (destinations).

**Syntax:**

```
list all

dst_network network address
rt_rcved_from_nbr network address
rt_sent_to_nbr network address

all
```

**Example:**

```
BGP6> list all
MED  Weight  LPref  AAG  AGRAS  ORG  AS-Path
0    0      0      No   0      IGP seq[2001]
Network/Prefixlen: 2001:6::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0    0      0      No   0      IGP seq[2001]
Network/Prefixlen: 2001:7::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0    0      0      No   0      IGP seq[2001]
Network/Prefixlen: 2001:9::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0    0      0      No   0      IGP seq[2001]
Network/Prefixlen: 2001:17::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0    0      0      No   0      IGP
Network/Prefixlen: 2002:2::/64
Next Hop: 2002:2::0202
Next Hop LLA: ::

0    0      0      No   0      IGP
Network/Prefixlen: 2002:5::/64
Next Hop: 2002:2::0202
Next Hop LLA: ::

0    0      0      No   0      IGP
Network/Prefixlen: 2002:6::/64
Next Hop: 2002:2::0202
Next Hop LLA: ::

0    0      0      No   0      IGP
Network/Prefixlen: 2002:9::/64
```

530 MRS V3.4 Protocol Reference V2
dst_network net address
Displays detailed information on the specified route or destination network. The command shows how a specific route was learned, the best path to a specific destination, the metric associated with the route, and other information.

Example:

BGP6> list dst_network
Destination network prefix []? 2002:1111::
Do you want specify prefix len? [No]: y
Prefix len (0-128) [64]? 64
Destination: 2002:1111::/64
Age:30, Upd#:4, LastSent: 0002:10:17
Eligible paths: 1
PathID: 0 - (Best Path)
  ASPath: Origin: IGP, Pref: 0, LocalPref: 0
  Metric: 0, Weight: 0, MED: 0
  NextHop: 2002:2::6202
  NextHop LLA: ::
  Neighbor: 2002:2::6202
  AtomicAggr: No

ASPath
Enumeration of autonomous systems along the path.
- seq: Sequence of autonomous systems in order in the path
- set: Set of autonomous systems in the path.

Origin
The originator of the destination. This is EGP, IGP, or Incomplete (originated by some other means not known).

LocalPref
The originating router’s degree of preference for the destination.

Metric
The path metric with which the route is imported.

Weight
The path weight.

MED
A multi-exit discriminator value, used to discriminate among multiple entry/exit points to the same AS.

NextHop
The address of the router to use as the forwarding address for destinations reachable via the given path.

AtomicAggr
Indicates whether the router advertising the path has included the path in an atomic-aggregate.

rt_rcved_from_nbr net address
Lists all routes received from the specified BGP neighbor.

Example:
BGP6 Monitoring Commands (Talk 5)

BGP6>list rt_rcved_from_nbr
BGP6 neighbor address []? 2003:1::6105

Destinations obtained from BGP6 neighbor 2003:1::6105

MED Weight LPref AGRAS ORG AS-Path
0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:9::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:7::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:17::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:6::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

r_t_sent_to_nbr net address
Lists all routes advertised to the specified BGP neighbor.

Example:
BGP6>list r_t_sent_to_nbr
BGP6 neighbor address []? 2003:1::6105

Destinations advertised to BGP6 neighbor 2003:1::6105

MED Weight LPref AGRAS ORG AS-Path
0 0 0 No 0 IGP
Network/Prefixlen: 2002:9::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:5::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:99::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:1111::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:6::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

Neighbors

Use the neighbors command to display information on all active BGP6 neighbors.

Syntax:
neighbors IPv6 neighbor address

Example:
BGP6>neighbors

Address: 2003:1::6105
bgp6-ID: 20.1.7.5
Status State DAY-HH:MM:SS AS Upd#
ENABLD Established 000-00:03:42 2001 11

IPv6-Address
Specifies the IPv6 address of the BGP6 neighbor.
State  Specifies the state of the connection. Possible states are:

Connect
Waiting for the TCP connection to the neighbor to be completed.

Active  In the event of TCP connection failure, the state is changed to Active, and the attempt to acquire the neighbor continues.

OpenSent
In this state OPEN has been sent, and BGP6 waits for an OPEN message from the neighbor.

OpenConfirm
In this state a KEEPALIVE has been sent in response to neighbor's OPEN, and waits for a KEEPALIVE/NOTIFICATION from the neighbor.

Established
A BGP6 connection has been successfully established, and can now start to exchange UPDATE messages.

BGP-ID
Specifies the neighbor's BGP6 Identification number.

AS
Specifies the neighbor's AS number.

Upd#
Specifies the sequence number of the last UPDATE message sent to the neighbor.

IPv6 neighbor address
Use the neighbor command to display detailed data on a particular BGP6 neighbor.

Example:
```
BGP6>neighbors 2000::662:0
Active Conn: None
Passive Conn: Sprt:179 Dprt:1026 State: Established KeepAlive/Hold Time: 30/90
TCP connection errors: 1 TCP state transitions: 1
BGP6 Messages: Sent Received Sent Received
Open: 2 2 Update: 2 2
Notification: 1 0 KeepAlive: 2 2
Total Messages: 7 6
Msg Header Errs: Sent Received Sent Received
Conn sync err: 0 0 Bad msg length: 0 0
Bad msg type: 0 0
Open Msg Errs: Sent Received Sent Received
Unsupp versions: 0 0 Unsupp auth code: 0 0
Bad peer AS ident: 0 0 Auth failure: 0 0
Bad BGP Ident: 0 0 Bad hold time: 0 0
Update Msg Errs: Sent Received Sent Received
Bad attr list: 0 0 AS routing loop: 0 0
Bad wkm attr: 0 0 Bad NEXT_HOP attr: 0 0
Msg wkm attr: 0 0 Optional attr err: 0 0
Attr flags err: 0 0 Bad network field: 0 0
Attr length err: 0 0 Bad AS_PATH attr: 0 0
Bad ORIGIN attr: 0 0
Total Errors: Sent Received Sent Received
Msg Header Errs: 0 0 Hold Timer Expired: 0 0
Open Msg Errs: 0 0 FSM Errs: 0 0
Update Msg Errs: 0 0 Cease: 1 0
```

Parameter

Use the BGP6 parameter command to display installed BGP6 globals in the BGP6 system.

Syntax:
BGP6 Monitoring Commands (Talk 5)

parameter

Example:
compare-med-from-diff-as is disabled.
IPv6-route-table-scan-timer value is 1 seconds.

Paths

Use the BGP6 **paths** command to display the paths stored in the path description database.

Syntax:
paths

Example:
paths
PathId MED AAG AGRAS RefCnt ORG AS_PATH
0 0 No 0 6 IGP
Next Hop: 2002:2::6202
Next Hop LLA: ::
1 0 No 0 2 IGP seq[2001]
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B
2 0 No 0 2 IGP seq[2001]
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

**PathId**
Path identifier

**NextHop**
The address of the router to use as the forwarding address for the destinations that can be reached via the given path.

**MED**
The multi-exit discriminator used to discriminate among multiple entry/exit points to the same AS.

**AAG**
Indicates if the path has been atomic-aggregated that is the router that is advertising the given path has selected less specific route over the more specific one when presented with overlapping routes.

**AGRAS**
Indicates the AS number of the BGP6 speaker that aggregated the routes.

**RefCnt**
Indicates the number of path entities referring to the descriptor.

**ORG**
Specifies the originator of the advertised destinations in the given path: either EGP, IGP, or Incomplete (originated by some other means not known).

**AS Path**
Enumeration of autonomous systems along the path.

**seq:** Sequence of autonomous systems in order in the path.

**set:** Set of autonomous systems in the path.

Ping6

For an explanation of the **ping6** command, see "Ping6" on page 468.
Policy-List

Use the policy-list command to display the current installed policy for specific neighbor and usage statistics of each policy.

Example:

```
BGP6>policy-list
Destination network prefix []? 2003:1::6105
Policy Type (Receive/Send/Origin) [All]? r

Receive policy list for all neighbors:
Idx T Match OrgAS AdjAS IGPmet Usage Prefix
 1 I Range 0 0 5 2001::/16
AS-PATH with following ASs will be discarded:

Send policy list for all neighbor:
Idx T Match TAG AdjAS Usage Prefix
 1 I Range 0 0 11 2002::/16

Origin policy list for all neighbor:
Idx T Match Tag Usage Prefix
 1 I Range 0 6 2002::/16

BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? r

Receive policy list for neighbor '2000::1':
Idx T Match OrgAS AnyAS MED Weight LPref IGPmet Usage Prefix
 1 I Range 0 0 10 0 100 0 0 ::/0

BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? s

Send policy list for neighbor '2000::1':
Idx T Match OrgAS AnyAS Tag MED ASpad Usage Prefix
 1 I Range 0 0 30 0 0 0 ::/0

BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? o

Origin policy list for all neighbor:
Idx T Match Tag Usage Prefix
 1 I Range 0 2 ::/0
```

Reset Neighbor

Use the reset neighbor command to reset the specified BGP6 neighbor, based on the neighbor configuration parameters stored in the configuration memory.

Syntax:

```
reset neighbor I Pv6 neighbor address
```

Example:

```
Enter a Neighbor address: []? 2003:1::6105
resetting neighbor 2003:1::6105
```

Sizes

Use the BGP6 sizes command to display the number of entries stored in the various data bases.

Syntax:
BGP6 Monitoring Commands (Talk 5)

sizes

Example:
sizes

# Paths: 10
# Path descriptors: 3
Update sequence#: 11
# Routing tbl entries (allocated): 10
# Current tbl entries (not imported): 0
# Current tbl entries (imported to IGP): 4

Paths  Total number of eligible paths for all the routes in the BGP6 routing table.
Path descriptors  Total number of path descriptors in the database used to hold common path information.
Update sequence#  Indicates the current update sequence number.
Routing tbl entries (allocated)  Indicates the number of entries in BGP6 routing table.
Current tbl entries (not imported)  Indicates the number of BGP6 routes not imported into IGP.
Current tbl entries (imported to IGP)  Indicates the number of BGP6 routes imported into IGP.

Traceroute6

For an explanation of the traceroute6 command, see “Traceroute6” on page 468.

BGP6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Border Gateway Protocol for IPv6 (BGP6) supports the CONFIG (Talk 6) delete interface command with the following consideration:

Deletes configured BGP6 external neighbors if the neighbor address has a common IPv6 prefix with an IPv6 address deleted on that interface.

GWCON (Talk 5) Activate Interface

The GWCON (Talk 5) activate interface command is not applicable for BGP6. BGP6 has no SRAM records associated with an interface.

GWCON (Talk 5) Reset Interface

The GWCON (Talk 5) reset interface command is not applicable for BGP6. BGP6 has no SRAM records associated with an interface.

GWCON (Talk 5) Component Reset Commands

BGP6 supports the following BGP6-specific GWCON (Talk 5) reset commands:

GWCON, Protocol Bgp6, Reset Neighbor Command

Description:

Adds or deletes a BGP6 neighbor. Changes neighbor parameters & policies.
Network Effect:
BGP6 neighbor connection and learned routes are updated based on configuration change.

Limitations:
None.

The following table summarizes the BGP6 configuration changes that are activated when the GWCON, protocol bgp6, reset neighbor command is invoked:

<table>
<thead>
<tr>
<th>Commands whose changes are activated by the GWCON, protocol bgp6, reset neighbor command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG, protocol BGP6, add neighbor</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, change neighbor</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, delete neighbor</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, attach policy-to-neighbor</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, change policy-to-neighbor</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, delete policy-to-neighbor</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, add policy-list</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, update policy-list</td>
</tr>
</tbody>
</table>

GWCON (Talk 5) Temporary Change Commands
BGP6 supports the following GWCON commands that temporarily change the operational state of the device. These changes are lost whenever the device is reloaded, restarted, or you execute any dynamically reconfigurable command.

<table>
<thead>
<tr>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>GWCON, protocol BGP6, enable neighbor</td>
</tr>
<tr>
<td>GWCON, protocol BGP6, disable neighbor</td>
</tr>
</tbody>
</table>

Non-Dynamically Reconfigurable Commands
The following table describes the BGP6 configuration commands that cannot be dynamically changed. To activate these commands, you need to reload or restart the device.

<table>
<thead>
<tr>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG, protocol BGP6, enable bgp6</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, disable bgp6</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, add no-receive</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, delete no-receive</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, add/change/delete/move aggregate</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, add/change/delete/move originate-policy</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, add/change/delete/move receive-policy</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, add/change/delete/move send-policy</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, enable compare-med-from-diff-as</td>
</tr>
<tr>
<td>CONFIG, protocol BGP6, set ipv6-route-table-scan-timer</td>
</tr>
</tbody>
</table>
Appendix A. Comparison of Protocols

This appendix compares some of the well-known protocols that your router supports. It is provided as a memory aid and is not meant as a reference.

Protocol Comparison Table

The following table compares the protocols.

Table 124. Comparison Protocols

<table>
<thead>
<tr>
<th>ISO OSI Model</th>
<th>TCP/IP</th>
<th>IPX</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 Application</td>
<td>Telnet, FTP, TFTP, SGMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Presentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Session</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Transport</td>
<td>TCP, UDP</td>
<td>PXP, SPX</td>
<td></td>
</tr>
<tr>
<td>3 Network</td>
<td>IP, RIP, BGP, ICMP</td>
<td>RIP, SAP</td>
<td></td>
</tr>
<tr>
<td>2 Data Link</td>
<td>Local Net</td>
<td></td>
<td>HDLC</td>
</tr>
<tr>
<td>1 Physical</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key to Protocols

Table 125 is a key to the protocols.

Table 125. Protocol Key

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP, TFTP</td>
<td>File Transfer Protocol; Trivial File Transfer Protocol.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol. Used to send network level error and control messages between routers and hosts.</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol. IP is a widely used standard transport protocol. IP is the 2210 routers’ basic protocol. IP leaves some error-checking to higher-level (end-to-end) protocols.</td>
</tr>
<tr>
<td>IPX</td>
<td>Internet Packet Exchange Protocol.</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol (Routing protocols are used to determine network topology and data paths). RIP is the most common IP routing protocol.</td>
</tr>
<tr>
<td>TCP</td>
<td>Transport Control Protocol. An end-to-end (host-to-host) protocol that is often used with IP. Useful for sending streams of data. Uses checksums, acknowledgments, and timeouts to ensure the correct delivery and sequence of data.</td>
</tr>
</tbody>
</table>
Comparison of Protocols
Appendix B. Packet Sizes

This appendix discusses the sizes of packets for the various networks and protocols supported. Included are the following sections:

- General Issues
- Network-Specific Size Limits
- Protocol-Specific Size Limits
- Changing Maximum Packet Sizes

General Issues

For the purposes of this discussion, the packets that the routers handle consist of user data and header information.

The amount of user data within a packet is limited by the amount of header information on the packet. The amount of header information depends on (at least):

- The network-types over which the packet must travel.
- The protocols in use on these networks.

The following factors affect the size of the packet contents:

- Length of the Data-Link header information that the current network type and interface require the packet to have.
- Length of the trailer information (if any) that the current network type and interface require the packet to have.

On any given network, the sum of the maximum data size together with header and trailer sizes will equal the network’s maximum packet size. When routing between networks of different maximum packet size, fragmentation of the packet may result.

Network-Specific Size Limits

Given the information in the previous section, the maximum amount of network layer data supported by each data link layer (network interface) can be determined. Table 126 lists the default maximum packet sizes for common interface types.

<table>
<thead>
<tr>
<th>Network Type (Data Link)</th>
<th>Network Layer max packet size (bytes)</th>
<th>Length of Network Header</th>
<th>Information Trailer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token-Ring 4-Mbps</td>
<td>2052</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>Token-Ring 16-Mbps</td>
<td>2052</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>Ethernet</td>
<td>1500</td>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td>PPP</td>
<td>2046</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>2048 (see notes)</td>
<td>variable</td>
<td>2</td>
</tr>
</tbody>
</table>

Note: For Frame Relay interfaces, you configure the maximum frame size not the network layer maximum packet size. To determine the maximum network layer packet size for a protocol, see the description of the set frame-size command in the chapter entitled Configuring and Monitoring Frame Relay Interfaces in Software User’s Guide.
Packet Sizes

Note: You can change the maximum packet size for interfaces other than Ethernet. Use the network command from the Config> prompt to access the interface’s configuration commands.

The maximum packet size is the maximum amount of data the protocol forwarder can pass to the device.

Note: These numbers correspond to the MTUs in 4.2 BSD UNIX.

For an IP packet, this includes the IP header, the UDP or TCP header, and all data.

The packet size in use is displayed when the router’s GWCON memory command is used. The “Pkt” size is the Network layer packet size. The Hdr (header) and Tlr (trailer) sizes depend on the networks and their network interfaces.

Protocol-Specific Size Limits

This section explains the protocol-specific size limits.

IP Packet Lengths

The IP protocol specifications do not require a host IP implementation to accept IP packets of more than 576 octets; however, router IP implementations must accommodate IP packets of any length up to the limits imposed by the network-specific packets in use.

Furthermore, router IP performs transparent fragmentation and reassembly of packets that would otherwise exceed network-specific length restrictions, as required by the IP specification.

Packet size mismatches do not cause connectivity problems. However, fragment reassembly does pose a performance penalty, so fragmentation should be avoided whenever possible.

Changing Maximum Packet Sizes

Normally, the router automatically sets the maximum network layer packet size to the size of the largest possible packet on all the connected networks. It then adds any headers and trailers required by the networks to determine the internal buffer size, which is larger than the network layer size.

Some networks (Token-Ring 4 Mbps and Token-Ring 16 Mbps) allow you to configure maximum packet sizes. Configuring maximum packet sizes affects the size of buffers used on the router and this in turn affects the number of buffers available for a given memory size. Routers automatically determine what size buffer it is going to need. You can change the maximum Network layer packet size that the router handles by using the set packet-size command; however, do not use this command unless specifically directed to by Customer Service.
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AARP</td>
<td>AppleTalk Address Resolution Protocol</td>
</tr>
<tr>
<td>ABR</td>
<td>area border router</td>
</tr>
<tr>
<td>ack</td>
<td>acknowledgment</td>
</tr>
<tr>
<td>AIX</td>
<td>Advanced Interactive Executive</td>
</tr>
<tr>
<td>AMA</td>
<td>arbitrary MAC addressing</td>
</tr>
<tr>
<td>AMP</td>
<td>active monitor present</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>AP2</td>
<td>AppleTalk Phase 2</td>
</tr>
<tr>
<td>APPN</td>
<td>Advanced Peer-to-Peer Networking</td>
</tr>
<tr>
<td>ARE</td>
<td>all-routes explorer</td>
</tr>
<tr>
<td>ARI</td>
<td>ATM real interface</td>
</tr>
<tr>
<td>ARI/FCl</td>
<td>address recognized indicator/frame copied indicator</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>AS</td>
<td>autonomous system</td>
</tr>
<tr>
<td>ASBR</td>
<td>autonomous system boundary router</td>
</tr>
<tr>
<td>ASCII</td>
<td>American National Standard Code for Information Interchange</td>
</tr>
<tr>
<td>ASN.1</td>
<td>abstract syntax notation 1</td>
</tr>
<tr>
<td>ASRT</td>
<td>adaptive source routing transparent</td>
</tr>
<tr>
<td>ASYNC</td>
<td>asynchronous</td>
</tr>
<tr>
<td>ATCP</td>
<td>AppleTalk Control Protocol</td>
</tr>
<tr>
<td>ATP</td>
<td>AppleTalk Transaction Protocol</td>
</tr>
<tr>
<td>AUI</td>
<td>attachment unit interface</td>
</tr>
<tr>
<td>AVI</td>
<td>ATM virtual interface</td>
</tr>
<tr>
<td>ayt</td>
<td>are you there</td>
</tr>
<tr>
<td>BAN</td>
<td>Boundary Access Node</td>
</tr>
<tr>
<td>BBCM</td>
<td>Bridging Broadcast Manager</td>
</tr>
<tr>
<td>BECN</td>
<td>backward explicit congestion notification</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BNC</td>
<td>bayonet Niell-Concelman</td>
</tr>
<tr>
<td>BNCP</td>
<td>Bridging Network Control Protocol</td>
</tr>
<tr>
<td>BOOTP</td>
<td>BOOT protocol</td>
</tr>
<tr>
<td>BPDU</td>
<td>bridge protocol data unit</td>
</tr>
<tr>
<td>bps</td>
<td>bits per second</td>
</tr>
<tr>
<td>BR</td>
<td>bridging/routing</td>
</tr>
</tbody>
</table>

© Copyright IBM Corp. 1994, 1999
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRS</td>
<td>bandwidth reservation</td>
</tr>
<tr>
<td>BSD</td>
<td>Berkeley software distribution</td>
</tr>
<tr>
<td>BTP</td>
<td>BOOTP relay agent</td>
</tr>
<tr>
<td>BTU</td>
<td>basic transmission unit</td>
</tr>
<tr>
<td>CAM</td>
<td>content-addressable memory</td>
</tr>
<tr>
<td>CCITT</td>
<td>Consultative Committee on International Telegraph and Telephone</td>
</tr>
<tr>
<td>CD</td>
<td>collision detection</td>
</tr>
<tr>
<td>CGWCON</td>
<td>Gateway Console</td>
</tr>
<tr>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>CIP</td>
<td>Classical IP</td>
</tr>
<tr>
<td>CIR</td>
<td>committed information rate</td>
</tr>
<tr>
<td>CLNP</td>
<td>Connectionless-Mode Network Protocol</td>
</tr>
<tr>
<td>CPU</td>
<td>central processing unit</td>
</tr>
<tr>
<td>CRC</td>
<td>cyclic redundancy check</td>
</tr>
<tr>
<td>CRS</td>
<td>configuration report server</td>
</tr>
<tr>
<td>CTS</td>
<td>clear to send</td>
</tr>
<tr>
<td>CUD</td>
<td>call user data</td>
</tr>
<tr>
<td>DAF</td>
<td>destination address filtering</td>
</tr>
<tr>
<td>DB</td>
<td>database</td>
</tr>
<tr>
<td>DBsum</td>
<td>database summary</td>
</tr>
<tr>
<td>DCD</td>
<td>data channel received line signal detector</td>
</tr>
<tr>
<td>DCE</td>
<td>data circuit-terminating equipment</td>
</tr>
<tr>
<td>DCS</td>
<td>Directly connected server</td>
</tr>
<tr>
<td>DDLC</td>
<td>dual data-link controller</td>
</tr>
<tr>
<td>DDN</td>
<td>Defense Data Network</td>
</tr>
<tr>
<td>DDP</td>
<td>Datagram Delivery Protocol</td>
</tr>
<tr>
<td>DDT</td>
<td>Dynamic Debugging Tool</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>dir</td>
<td>directly connected</td>
</tr>
<tr>
<td>DL</td>
<td>data link</td>
</tr>
<tr>
<td>DLC</td>
<td>data link control</td>
</tr>
<tr>
<td>DLCI</td>
<td>data link connection identifier</td>
</tr>
<tr>
<td>DLS</td>
<td>data link switching</td>
</tr>
<tr>
<td>DLSw</td>
<td>data link switching</td>
</tr>
<tr>
<td>DMA</td>
<td>direct memory access</td>
</tr>
<tr>
<td>DNA</td>
<td>Digital Network Architecture</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DNCP</td>
<td>DECnet Protocol Control Protocol</td>
</tr>
<tr>
<td>DNIC</td>
<td>Data Network Identifier Code</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOS</td>
<td>Disk Operating System</td>
</tr>
<tr>
<td>DR</td>
<td>designated router</td>
</tr>
<tr>
<td>DRAM</td>
<td>Dynamic Random Access Memory</td>
</tr>
<tr>
<td>DSAP</td>
<td>destination service access point</td>
</tr>
<tr>
<td>DSE</td>
<td>data switching equipment</td>
</tr>
<tr>
<td>DSE</td>
<td>data switching exchange</td>
</tr>
<tr>
<td>DSR</td>
<td>data set ready</td>
</tr>
<tr>
<td>DSU</td>
<td>data service unit</td>
</tr>
<tr>
<td>DTE</td>
<td>data terminal equipment</td>
</tr>
<tr>
<td>DTR</td>
<td>data terminal ready</td>
</tr>
<tr>
<td>Dtype</td>
<td>destination type</td>
</tr>
<tr>
<td>DVMRP</td>
<td>Distance Vector Multicast Routing Protocol</td>
</tr>
<tr>
<td>E&amp;M</td>
<td>Ear &amp; Mouth</td>
</tr>
<tr>
<td>E1</td>
<td>2.048 Mbps transmission rate</td>
</tr>
<tr>
<td>EDEL</td>
<td>end delimiter</td>
</tr>
<tr>
<td>EDI</td>
<td>error detected indicator</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>EIA</td>
<td>Electronics Industries Association</td>
</tr>
<tr>
<td>ELAN</td>
<td>Emulated LAN</td>
</tr>
<tr>
<td>ELAP</td>
<td>EtherTalk Link Access Protocol</td>
</tr>
<tr>
<td>ELS</td>
<td>Event Logging System</td>
</tr>
<tr>
<td>ESI</td>
<td>End system identifier</td>
</tr>
<tr>
<td>EST</td>
<td>Eastern Standard Time</td>
</tr>
<tr>
<td>Eth</td>
<td>Ethernet</td>
</tr>
<tr>
<td>fa-ga</td>
<td>functional address-group address</td>
</tr>
<tr>
<td>FCS</td>
<td>frame check sequence</td>
</tr>
<tr>
<td>FECN</td>
<td>forward explicit congestion notification</td>
</tr>
<tr>
<td>FIFO</td>
<td>first in, first out</td>
</tr>
<tr>
<td>FLT</td>
<td>filter library</td>
</tr>
<tr>
<td>FR</td>
<td>Frame Relay</td>
</tr>
<tr>
<td>FRL</td>
<td>Frame Relay</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>FXO</td>
<td>Foreign Exchange Office</td>
</tr>
<tr>
<td>FXS</td>
<td>Foreign Exchange Station</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>GMT</td>
<td>Greenwich Mean Time</td>
</tr>
<tr>
<td>GOSIP</td>
<td>Government Open Systems Interconnection Profile</td>
</tr>
<tr>
<td>GTE</td>
<td>General Telephone Company</td>
</tr>
<tr>
<td>GWCON</td>
<td>Gateway Console</td>
</tr>
<tr>
<td>HDLC</td>
<td>high-level data link control</td>
</tr>
<tr>
<td>HEX</td>
<td>hexadecimal</td>
</tr>
<tr>
<td>HPR</td>
<td>high-performance routing</td>
</tr>
<tr>
<td>HST</td>
<td>TCP/IP host services</td>
</tr>
<tr>
<td>HTF</td>
<td>host table format</td>
</tr>
<tr>
<td>IBD</td>
<td>Integrated Boot Device</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>ICP</td>
<td>Internet Control Protocol</td>
</tr>
<tr>
<td>ID</td>
<td>identification</td>
</tr>
<tr>
<td>IDP</td>
<td>Initial Domain Part</td>
</tr>
<tr>
<td>IDP</td>
<td>Internet Datagram Protocol</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>Ifc#</td>
<td>interface number</td>
</tr>
<tr>
<td>IGP</td>
<td>interior gateway protocol</td>
</tr>
<tr>
<td>InARP</td>
<td>Inverse Address Resolution Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPCP</td>
<td>IP Control Protocol</td>
</tr>
<tr>
<td>IPPN</td>
<td>IP Protocol Network</td>
</tr>
<tr>
<td>IPX</td>
<td>Internetwork Packet Exchange</td>
</tr>
<tr>
<td>IPXCP</td>
<td>IPX Control Protocol</td>
</tr>
<tr>
<td>ISDN</td>
<td>integrated services digital network</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>Kbps</td>
<td>kilobits per second</td>
</tr>
<tr>
<td>LAC</td>
<td>L2TP Network Access Concentrator</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LAPB</td>
<td>link access protocol-balanced</td>
</tr>
<tr>
<td>LAT</td>
<td>local area transport</td>
</tr>
<tr>
<td>LCP</td>
<td>Link Control Protocol</td>
</tr>
<tr>
<td>LED</td>
<td>light-emitting diode</td>
</tr>
<tr>
<td>LF</td>
<td>largest frame; line feed</td>
</tr>
<tr>
<td>LIS</td>
<td>Logical IP subnet</td>
</tr>
<tr>
<td>LLC</td>
<td>logical link control</td>
</tr>
</tbody>
</table>
LLC2  logical link control 2
LMI   local management interface
LNS   L2TP Network Server
LRM   LAN reporting mechanism
LS    link state
LSA   link state advertisement
LSB   least significant bit
LSI   LAN shortcuts interface
LSreq link state request
LSrxl link state retransmission list
LU    logical unit
MAC   medium access control
Mb    megabit
MB    megabyte
Mbps  megabits per second
MBps  megabytes per second
MC    multicast
MCF   MAC filtering
MIB   Management Information Base
MIB II Management Information Base II
MILNET military network
MOS   Micro Operating System
MOSDBG Micro Operating System Debugging Tool
MOSPF Open Shortest Path First with multicast extensions
MSB   most significant bit
MSDU  MAC service data unit
MRU   maximum receive unit
MTU   maximum transmission unit
nak   not acknowledged
NBMA  Non-Broadcast Multiple Access
NBP   Name Binding Protocol
NBR   neighbor
NCP   Network Control Protocol
NCP   Network Core Protocol
NetBIOS Network Basic Input/Output System
NHRP  Next Hop Resolution Protocol
NIST  National Institute of Standards and Technology
NPDU  Network Protocol Data Unit
NRZ  non-return-to-zero
NRZI  non-return-to-zero inverted
NSAP  Network Service Access Point
NSF  National Science Foundation
NSFNET  National Science Foundation NETwork
NVCNFG  nonvolatile configuration
OOS  Out of Service
OPCON  Operator Console
OSI  open systems interconnection
OSICP  OSI Control Protocol
OSPF  Open Shortest Path First
OUI  organization unique identifier
PC  personal computer
PCR  peak cell rate
PDN  public data network
PING  Packet internet groper
PDU  protocol data unit
PID  process identification
P-P  Point-to-Point
PPP  Point-to-Point Protocol
PROM  programmable read-only memory
PU  physical unit
PVC  permanent virtual circuit
RAM  random access memory
RD  route descriptor
REM  ring error monitor
REV  receive
RFC  Request for Comments
RI  ring indicator; routing information
RIF  routing information field
RII  routing information indicator
RIP  Routing Information Protocol
**RISC** reduced instruction-set computer  
**RNR** receive not ready  
**ROM** read-only memory  
**ROpcon** Remote Operator Console  
**RPS** ring parameter server  
**RTMP** Routing Table Maintenance Protocol  
**RTP** Routing update Protocol  
**RTS** request to send  
**Rtype** route type  
**rxmits** retransmissions  
**rxmt** retransmit  
**SAF** source address filtering  
**SAP** service access point  
**SAP** Service Advertising Protocol  
**SCR** Sustained cell rate  
**SCSP** Server Cache Synchronization Protocol  
**sdel** start delimiter  
**SDLC** SDLC relay, synchronous data link control  
**seqno** sequence number  
**SGID** sever group id  
**SGMP** Simple Gateway Monitoring Protocol  
**SL** serial line  
**SMP** standby monitor present  
**SMTP** Simple Mail Transfer Protocol  
**SNA** Systems Network Architecture  
**SNAP** Subnetwork Access Protocol  
**SNMP** Simple Network Management Protocol  
**SNPA** subnetwork point of attachment  
**SPF** OSPF intra-area route  
**SPE1** OSPF external route type 1  
**SPE2** OSPF external route type 2  
**SPIA** OSPF inter-area route type  
**SPID** service profile ID  
**SPX** Sequenced Packet Exchange  
**SQE** signal quality error  
**SRAM** static random access memory  
**SRB** source routing bridge
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRF</td>
<td>specifically routed frame</td>
</tr>
<tr>
<td>SRLY</td>
<td>SDLC relay</td>
</tr>
<tr>
<td>SRT</td>
<td>source routing transparent</td>
</tr>
<tr>
<td>SR-TB</td>
<td>source routing-transparent bridge</td>
</tr>
<tr>
<td>STA</td>
<td>static</td>
</tr>
<tr>
<td>STB</td>
<td>spanning tree bridge</td>
</tr>
<tr>
<td>STE</td>
<td>spanning tree explorer</td>
</tr>
<tr>
<td>STP</td>
<td>shielded twisted pair; spanning tree protocol</td>
</tr>
<tr>
<td>SVC</td>
<td>switched virtual circuit</td>
</tr>
<tr>
<td>TB</td>
<td>transparent bridge</td>
</tr>
<tr>
<td>TCN</td>
<td>topology change notification</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TEI</td>
<td>terminal point identifier</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TKR</td>
<td>token ring</td>
</tr>
<tr>
<td>TMO</td>
<td>timeout</td>
</tr>
<tr>
<td>TOS</td>
<td>type of service</td>
</tr>
<tr>
<td>TSF</td>
<td>transparent spanning frames</td>
</tr>
<tr>
<td>TTL</td>
<td>time to live</td>
</tr>
<tr>
<td>TTY</td>
<td>teletypewriter</td>
</tr>
<tr>
<td>TX</td>
<td>transmit</td>
</tr>
<tr>
<td>UA</td>
<td>unnumbered acknowledgment</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UI</td>
<td>unnumbered information</td>
</tr>
<tr>
<td>UTP</td>
<td>unshiled twisted pair</td>
</tr>
<tr>
<td>VCC</td>
<td>Virtual Channel Connection</td>
</tr>
<tr>
<td>VINES</td>
<td>Virtual NEtworking System</td>
</tr>
<tr>
<td>VIR</td>
<td>variable information rate</td>
</tr>
<tr>
<td>VL</td>
<td>virtual link</td>
</tr>
<tr>
<td>VNI</td>
<td>Virtual Network Interface</td>
</tr>
<tr>
<td>VoFR</td>
<td>Voice over Frame Relay</td>
</tr>
<tr>
<td>VR</td>
<td>virtual route</td>
</tr>
<tr>
<td>WAN</td>
<td>wide area network</td>
</tr>
<tr>
<td>WRS</td>
<td>WAN restoral/reroute</td>
</tr>
<tr>
<td>X.25</td>
<td>packet-switched networks</td>
</tr>
<tr>
<td><strong>X.251</strong></td>
<td>X.25 physical layer</td>
</tr>
<tr>
<td><strong>X.252</strong></td>
<td>X.25 frame layer</td>
</tr>
<tr>
<td><strong>X.253</strong></td>
<td>X.25 packet layer</td>
</tr>
<tr>
<td><strong>XID</strong></td>
<td>exchange identification</td>
</tr>
<tr>
<td><strong>XNS</strong></td>
<td>Xerox Network Systems</td>
</tr>
<tr>
<td><strong>XSUM</strong></td>
<td>checksum</td>
</tr>
<tr>
<td><strong>ZIP</strong></td>
<td>AppleTalk Zone Information Protocol</td>
</tr>
<tr>
<td><strong>ZIP2</strong></td>
<td>AppleTalk Zone Information Protocol 2</td>
</tr>
<tr>
<td><strong>ZIT</strong></td>
<td>Zone Information Table</td>
</tr>
</tbody>
</table>
Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology* Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users’ Glossary*

The following cross-references are used in this glossary:

Contrast with:

This refers to a term that has an opposed or substantively different meaning.

Synonym for:

This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with:

This is a backward reference from a defined term to all other terms that have the same meaning.

See:

This refers the reader to multiple-word terms that have the same last word.

See also:

This refers the reader to terms that have a related, but not synonymous, meaning.

A

AAL. ATM Adaptation Layer, the layer that adapts user data to/from the ATM network by adding/removing headers and segmenting/reassembling the data into/from cells.

AAL-5. ATM Adaptation Layer 5, one of several standard AALs. AAL-5 was designed for data communications, and is used by LAN Emulation and Classical IP.

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in the following standards:


See also basic encoding rules (BER).

ACCESS. In the Simple Network Management Protocol (SNMP), the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active. (1) Operational. (2) Pertaining to a node or device that is connected or is available for connection to another node or device.

active monitor. In a token-ring network, a function performed at any one time by one ring station that
initiates the transmission of tokens and provides token error recovery facilities. Any active adapter on the ring has the ability to provide the active monitor function if the current active monitor fails.

**address.** In data communication, the unique code assigned to each device, workstation, or user connected to a network.

**address mapping table (AMT).** A table, maintained within the AppleTalk router, that provides a current mapping of node addresses to hardware addresses.

**address mask.** For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with subnet mask and subnetwork mask.

**address resolution.** (1) A method for mapping network-layer addresses to media-specific addresses. (2) See also Address Resolution Protocol (ARP) and AppleTalk Address Resolution Protocol (AARP).

**Address Resolution Protocol (ARP).** (1) In the Internet suite of protocols, the protocol that dynamically maps an IP address to an address used by a supporting metropolitan or local area network such as Ethernet or token-ring. (2) See also Reverse Address Resolution Protocol (RARP).

**addressing.** In data communication, the way in which a station selects the station to which it is to send data.

**adjacent nodes.** Two nodes connected together by at least one path that connects no other node. (T)

**Administrative Domain.** A collection of hosts and routers, and the interconnecting networks, managed by a single administrative authority.

**Advanced Peer-to-Peer Networking (APPN).** An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

**Advanced Peer-to-Peer Networking (APPN) end node.** A node that provides a broad range of end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to a subarea network as a peripheral node or to other end nodes.

**Advanced Peer-to-Peer Networking (APPN) network.** A collection of interconnected network nodes and their client end nodes.

**Advanced Peer-to-Peer Networking (APPN) network node.** A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

**Advanced Peer-to-Peer Networking (APPN) node.** An APPN network node or an APPN end node.

**agent.** A system that assumes an agent role.

**alert.** A message sent to a management services focal point in a network to identify a problem or an impending problem.

**all-stations address.** In communications, synonym for broadcast address.

**American National Standards Institute (ANSI).** An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

**analog.** (1) Pertaining to data consisting of continuously variable physical quantities. (A) (2) Contrast with digital.

**AppleTalk.** A network protocol developed by Apple Computer, Inc. This protocol is used to interconnect network devices, which can be a mixture of Apple and non-Apple products.

**AppleTalk Address Resolution Protocol (AARP).** In AppleTalk networks, a protocol that (a) translates AppleTalk node addresses into hardware addresses and (b) reconciles addressing discrepancies in networks that support more than one set of protocols.

**AppleTalk Transaction Protocol (ATP).** In AppleTalk networks, a protocol that provides client/server request and response functions for hosts accessing the Zone Information Protocol (ZIP) for zone information.

**APPN network.** See Advanced Peer-to-Peer Networking (APPN) network.

**APPN network node.** See Advanced Peer-to-Peer Networking (APPN) network node.
arbitrary MAC addressing (AMA). In DECnet architecture, an addressing scheme used by DECnet Phase IV-Prime that supports universally administered addresses and locally administered addresses.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by definition of the network administrator. Each area is self-contained; knowledge of an area’s topology remains hidden from other areas.

asynchronous (ASYNC). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

ATM. Asynchronous Transfer Mode, a connection-oriented, high-speed networking technology based on cell switching.

ATMARP. ARP in Classical IP.

attachment unit interface (AUI). In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (I) (A)

Attribute Value Pair (AVP). A uniform method of encoding message types and bodies. This method maximizes the extensibility while permitting interoperability of L2TP.

authentication failure. In the Simple Network Management Protocol (SNMP), a trap that may be generated by an authentication entity when a requesting client is not a member of the SNMP community.

autonomous system. In TCP/IP, a group of networks and routers under one administrative authority. These networks and routers cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. In TCP/IP, a number assigned to an autonomous system by the same central authority that also assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges or routers. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected.

backbone network. A central network to which smaller networks, normally of lower speed, connect. The backbone network usually has a much higher capacity than the networks it helps interconnect or is a wide-area network (WAN) such as a public packet-switched datagram network.

backbone router. (1) A router used to transmit data between areas. (2) One in a series of routers that is used to interconnect networks into a larger Internet.

Bandwidth. The bandwidth of an optical link designates the information-carrying capacity of the link and is related to the maximum bit rate that a fiber link can support.

basic transmission unit (BTU). In SNA, the unit of data and control information passed between path control components. A BTU can consist of one or more path information units (PIUs).

baud. In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud. (A)

bootstrap. (1) A sequence of instructions whose execution causes additional instructions to be loaded and executed until the complete computer program is in storage. (T) (2) A technique or device designed to bring itself into a desired state by means of its own action, for example, a machine routine whose first few instructions are sufficient to bring the rest of itself into the computer from an input device. (A)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems.

border router. In Internet communications, a router, positioned at the edge of an autonomous system, that communicates with a router that is positioned at the edge of a different autonomous system.

bridge. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address.

bridge identifier. An 8-byte field, used in a spanning tree protocol, composed of the MAC address of the port with the lowest port identifier and a user-defined value.

bridging. In LANs, the forwarding of a frame from one LAN segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadcast. (1) Transmission of the same data to all destinations. (T) (2) Simultaneous transmission of data to more than one destination. (3) Contrast with multicast.
broadcast address. In communications, a station address (eight 1's) reserved as an address common to all stations on a link. Synonymous with all-stations address.

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) A functional unit, controlled by the processor, that handles the transfer of data between processor storage and local peripheral equipment.

canonical address. In LANs, the IEEE 802.1 format for the transmission of medium access control (MAC) addresses for token-ring and Ethernet adapters. In canonical format, the least significant (rightmost) bit of addresses for token-ring and Ethernet adapters is set to 1 and 0, respectively, and the host ID occupies the two high-order (most significant) and next-to-most significant bits of the IP address. In class A and class B networks, the two high-order (most significant) bits of the IP address are set to 0 and 1, respectively, and the host ID occupies the three low-order octets.

class A network. In Internet communications, a network in which the high-order (most significant) bit of the IP address is set to 0 and the host ID occupies the three low-order octets.

class B network. In Internet communications, a network in which the two high-order (most significant) and next-to-most significant bits of the IP address are set to 1 and 0, respectively, and the host ID occupies the two low-order octets.

class of service (COS). A set of characteristics (such as route security, transmission priority, and bandwidth) used to construct a route between session partners. The class of service is derived from a mode name specified by the initiator of a session.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with line switching.

clock. (1) In binary synchronous communication, the use of clock pulses to control synchronization of

CCITT. International Telegraph and Telephone Consultative Committee. This was an organization of the International Telecommunication Union (ITU). On 1 March 1993 the ITU was reorganized, and responsibilities for standardization were placed in a subordinate organization named the Telecommunication Standardization Sector of the Telecommunication Union (ITU-TS). "CCITT" continues to be used for recommendations that were approved before the reorganization.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. (4) To place, hide, or store in a cache.

call request packet. (1) A call supervision packet that a data terminal equipment (DTE) transmits to ask that a connection for a call be established throughout the network. (2) In X.25 communications, a call supervision packet transmitted by a DTE to ask for a call establishment through the network.

carrier. An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system. (T)

carrier detect. Synonym for received line signal detector (RLSD).

carrier sense. In a local area network, an ongoing activity of a data station to detect whether another station is transmitting. (T)

carrier sense multiple access with collision detection (CSMA/CD). A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again. (T) (A)

class service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal's performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loopback testing, which includes the transmission of test signals between the CSU and the network carrier’s office channel unit. See also data service unit (DSU).

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

clocking. (1) In binary synchronous communication, the use of clock pulses to control synchronization of
data and control characters. (2) A method of controlling the number of data bits sent on a telecommunication line in a given time.

**collision.** An unwanted condition that results from concurrent transmissions on a channel. (T)

**collision detection.** In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

**Committed information rate.** The maximum amount of data in bits that the network agrees to deliver.

**community.** In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

**community name.** In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

**compression.** (1) The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. (2) Any encoding to reduce the number of bits used to represent a given message or record.

**configuration.** (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

**configuration database (CDB).** A database that stores the configuration parameters of one or several devices. It is prepared and updated using the configuration program.

**configuration file.** A file that specifies the characteristics of a system device or network.

**configuration parameter.** A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

**configuration report server (CRS).** In the IBM Token-Ring Network Bridge Program, the server that accepts commands from the LAN Network Manager (LNM) to get station information, set station parameters, and remove stations on its ring. This server also collects and forwards configuration reports generated by stations on its ring. The configuration reports include the new active monitor reports and the nearest active upstream neighbor (NAUN) reports.

**congestion.** See network congestion.

**connection.** In data communication, an association established between functional units for conveying information. (I) (A)

**control point (CP).** (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENC) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

**control point management services (CPMS).** A component of a control point, consisting of management services function sets, that provides facilities to assist in performing problem management, performance and accounting management, change management, and configuration management. Capabilities provided by the CPMS include sending requests to physical unit management services (PUMS) to test system resources, collecting statistical information (for example, error and performance data) from PUMS about the system resources, and analyzing and presenting test results and statistical information collected about the system resources. Analysis and presentation responsibilities for problem determination and performance monitoring can be distributed among multiple CPMSs.

**control point management services unit (CP-MSU).** The message unit that contains management services data and flows between management services function sets. This message unit is in general data stream (GDS) format. See also management services unit (MSU) and network management vector transport (NMVT).

**D**

**D-bit.** Delivery-confirmation bit. In X.25 communications, the bit in a data packet or call-request packet that is set to 1 if end-to-end acknowledgment (delivery confirmation) is required from the recipient.

**daemon.** A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

**data carrier detect (DCD).** Synonym for received line signal detector (RLSD).

**data circuit.** (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (I) (2) In SNA, synonym for link connection. (3) See also physical circuit and virtual circuit.
Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.

2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.

2. A DCE may perform other functions that are usually performed at the network end of the line.

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

<table>
<thead>
<tr>
<th>DLCI Values</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–15</td>
<td>in-channel signaling</td>
</tr>
<tr>
<td>16–991</td>
<td>assigned using frame-relay connection procedures</td>
</tr>
<tr>
<td>992–1007</td>
<td>Layer 2 management of frame-relay bearer service</td>
</tr>
<tr>
<td>1008–1022</td>
<td>reserved</td>
</tr>
<tr>
<td>1023</td>
<td>in-channel layer management</td>
</tr>
</tbody>
</table>

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link layer. In the Open Systems Interconnection reference model, the layer that provides services to transfer data between entities in the network layer over a communication link. The data link layer detects and possibly corrects errors that may occur in the physical layer. (T)

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. See also packet level and physical level. (2) In X.25 communications, synonym for frame level.

data link switching (DLSw). A method of transporting network protocols that use IEEE 802.2 logical link control (LLC) type 2. SNA and NetBIOS are examples of protocols that use LLC type 2. See also encapsulation and spoofing.

data packet. In X.25 communications, a packet used for the transmission of user data on a virtual circuit at the DTE/DCE interface.

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

data set ready (DSR). Synonym for DCE ready.

data switching exchange (DSE). The equipment installed at a single location to provide switching functions, such as circuit switching, message switching, and packet switching. (I)

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (I)

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.

2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs
and the network. (1) (2) In TCP/IP, the basic unit of
information passed across the Internet environment. A
datagram contains a source and destination address
along with the data. An Internet Protocol (IP) datagram
consists of an IP header followed by the transport layer
data. (3) See also packet and segment.

Datagram Delivery Protocol (DDP). In AppleTalk
networks, a protocol that provides network connectivity
by means of connectionless socket-to-socket delivery
service on the internet layer.

DCE ready. In the EIA 232 standard, a signal that
indicates to the data terminal equipment (DTE) that the
local data circuit-terminating equipment (DCE) is
connected to the communication channel and is ready
to send data. Synonymous with data set ready (DSR).

DECnet. A network architecture that defines the
operation of a family of software modules, databases,
and hardware components typically used to tie Digital
Equipment Corporation systems together for resource
sharing, distributed computation, or remote system
configuration. DECnet network implementations follow
the Digital Network Architecture (DNA) model.

default. Pertaining to an attribute, condition, value, or
option that is assumed when none is explicitly
specified. (I)

dependent LU requester (DLUR). An APPN end node
or an APPN network node that owns dependent LUs,
but requests that a dependent LU server provide the
SSCP services for those dependent LUs.

designated router. A router that informs end nodes
of the existence and identity of other routers. The selection
of the designated router is based upon the router with
the highest priority. When several routers share the
highest priority, the router with the highest station
address is selected.

destination node. The node to which a request or
data is sent.

destination port. The 8-port asynchronous adapter
that serves as a connection point with a serial service.

destination service access point (DSAP). In SNA
and TCP/IP, a logical address that allows a system to
route data from a remote device to the appropriate
communications support. Contrast with source service
access point (SSAP).

device. A mechanical, electrical, or electronic
contrivance with a specific purpose.

digital. (1) Pertaining to data that consist of digits. (T)
(2) Pertaining to data in the form of digits. (A) (3)
Contrast with analog.

Digital Network Architecture (DNA). The model for
all DECnet hardware and software implementations.

direct memory access (DMA). The system facility
that allows a device on the Micro Channel bus to get
direct access to the system or bus memory without the
intervention of the system processor.

directory. A table of identifiers and references to the
corresponding items of data. (I) (A)

directory service (DS). An application service element
that translates the symbolic names used by application
processes into the complete network addresses used in
an OSI environment. (T)

directory services (DS). A control point component of
an APPN node that maintains knowledge of the location
of network resources.

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit
that prevents the occurrence of certain types of
interruptions. (2) Pertaining to the state in which a
transmission control unit or audio response unit cannot
accept incoming calls on a line.

domain. (1) That part of a computer network in which
the data processing resources are under common
control. (T) (2) In Open Systems Interconnection (OSI),
a part of a distributed system or a set of managed
objects to which a common policy applies. (3) See
Administrative Domain and domain name.

domain name. In the Internet suite of protocols, a
name of a host system. A domain name consists of a
sequence of subnames separated by a delimiter
character. For example, if the fully qualified domain
name (FQDN) of a host system is ralvm7.vnet.ibm.com,
each of the following is a domain name:
• ralvm7.vnet.ibm.com
• vnet.ibm.com
• ibm.com

domain name server. In the Internet suite of
protocols, a server program that supplies
name-to-address translation by mapping domain names
to IP addresses. Synonymous with name server.

Domain Name System (DNS). In the Internet suite of
protocols, the distributed database system used to map
domain names to IP addresses.

dotted decimal notation. The syntactical
representation for a 32-bit integer that consists of four
8-bit numbers written in base 10 with periods (dots)
separating them. It is used to represent IP addresses.

dump. (1) Data that has been dumped. (T) (2) To
copy the contents of all or part of virtual storage for the
purpose of collecting error information.

dynamic reconfiguration (DR). The process of
changing the network configuration (peripheral PUs and
without regenerating complete configuration tables or deactivating the affected major node.

**Dynamic Routing.** Routing using learned routes rather than routes statically configured at initialization.

**E**

echo. In data communication, a reflected signal on a communications channel. For example, on a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

**EIA 232.** In data communication, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

**Electronic Industries Association (EIA).** An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

**EIA unit.** A unit of measure, established by the Electronic Industries Association, equal to 44.45 millimeters (1.75 inches).

**encapsulation.** (1) In communications, a technique used by layered protocols by which a layer adds control information to the protocol data unit (PDU) from the layer it supports. In this respect, the layer encapsulates the data from the supported layer. In the Internet suite of protocols, for example, a packet would contain control information from the physical layer, followed by control information from the network layer, followed by the application protocol data. (2) See also data link switching.

**encode.** To convert data by the use of a code in such a manner that reconversion to the original form is possible. (T)

**end node (EN).** (1) See Advanced Peer-to-Peer Networking (APPN) end node and low-entry networking (LEN) end node. (2) In communications, a node that is frequently attached to a single data link and cannot perform intermediate routing functions.

**entry point (EP).** In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

**Ethernet.** A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

**exception.** An abnormal condition such as an I/O error encountered in processing a data set or a file.

**exception response (ER).** In SNA, a protocol requested in the form-of-response-requested field of a request header that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, can be returned. Contrast with definite response and no response.

**exchange identification (XID).** A specific type of basic link unit that is used to convey node and link characteristics between adjacent nodes. XIDs are exchanged between link stations before and during link activation to establish and negotiate link and node characteristics, and after link activation to communicate changes in these characteristics.

**explicit route (ER).** In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with virtual route (VR).

**explorer frame.** See explorer packet.

**explorer packet.** In LANs, a packet that is generated by the source host and that traverses the entire source routing part of a LAN, gathering information on the possible paths available to the host.

**exterior gateway.** In Internet communications, a gateway on one autonomous system that communicates with another autonomous system. Contrast with interior gateway.

**Exterior Gateway Protocol (EGP).** In the Internet suite of protocols, a protocol, used between domains and autonomous systems, that enables network reachability information to be advertised and exchanged. IP network addresses in one autonomous system are advertised to another autonomous system by means of EGP-participating routers. An example of an EGP is the Border Gateway Protocol (BGP). Contrast with Interior Gateway Protocol (IGP).

**F**

**fax.** Hardcopy received from a facsimile machine. Synonymous with telexcopy.

**File Transfer Protocol (FTP).** In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.
**flash memory.** A data storage device that is programmable, erasable, and does not require continuous power. The chief advantage of flash memory over other programmable and erasable data storage devices is that it can be reprogrammed without being removed from the circuit board.

**flow control.** (1) In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the rate of flow of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units. (2) See also pacing.

**fragment.** See fragmentation.

**fragmentation.** (1) The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted. (2) See also segmenting.

**frame.** (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDL, the vehicle for every command, every response, and all information that is transmitted using SDL procedures. **frame level.** Synonymous with data link level. See link level.

**frame relay.** (1) An interface standard describing the boundary between a user’s equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

**front-end processor.** A processor such as the IBM 3745 or 3174, that relieves a main frame from the communication control tasks.

**G**

**gateway.** (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols. (3) In TCP/IP, synonym for router.

**general data stream (GDS).** The data stream used for conversations in LU 6.2 sessions.

**general data stream (GDS) variable.** A type of RU substructure that is preceded by an identifier and a length field and includes either application data, user control data, or SNA-defined control data.

**H**

**header.** (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

**heap memory.** The amount of RAM used to dynamically allocate data structures.

**Hello.** A protocol used by a group of cooperating, trusting routers to allow them to discover minimal delay routes.

**hello message.** (1) A message sent periodically to establish and test reachability between routers or between routers and hosts. (2) In the Internet suite of protocols, a message defined by the Hello protocol as an Interior Gateway Protocol (IGP).

**heuristic.** Pertaining to exploratory methods of problem solving in which solutions are discovered by evaluation of the progress made toward the final result.

**high-level data link control (HDLC).** In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

**high-performance routing (HPR).** An addition to the Advanced Peer-to-Peer Networking (APPN) architecture that enhances data routing performance and reliability, especially when using high-speed links.

**hop.** (1) In APPN, a portion of a route that has no intermediate nodes. It consists of only a single transmission group connecting adjacent nodes. (2) To the routing layer, the logical distance between two nodes in a network.

**hop count.** (1) A metric or measure of distance between two points. (2) In Internet communications, the number of routers that a datagram passes through on its way to its destination. (3) In SNA, a measure of the number of links to be traversed in a path to a destination.
host. In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe.

hub (intelligent). A wiring concentrator, such as the IBM 8260, that provides bridging and routing functions for LANs with different cables and protocols.

hysteresis. The amount the temperature must change past the set alert threshold before the alert condition is cleared.

I-frame. Information frame.

information (I) frame. A frame in I format used for numbered information transfer.

input/output channel. In a data processing system, a functional unit that handles transfer of data between internal and peripheral equipment. (I) (A)

Integrated Digital Network Exchange (IDNX). A processor integrating voice, data, and image applications. It also manages the transmission resources, and connects to multiplexers and network management support systems. It allows integration of equipment from different vendors.

integrated services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data.

Note: ISDNs are used in public and private network architectures.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interior gateway. In Internet communications, a gateway that communicates only with its own autonomous system. Contrast with exterior gateway.

Interior Gateway Protocol (IGP). In the Internet suite of protocols, a protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

interleaving. (1) The alternating of two or more operations or functions through the overlapped use of a computer facility. (2) In data transmission, the alternating of packets from one data stream with packets from another.

intermediate node. A node that is at the end of more than one branch. (T)

intermediate session routing (ISR). A type of routing function within an APPN network node that provides session-level flow control and outage reporting for all sessions that pass through the node but whose end points are elsewhere.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

International Telecommunication Union (ITU). The specialized telecommunication agency of the United Nations, established to provide standardized communication procedures and practices, including frequency allocation and radio regulations worldwide.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also Internet.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See IP address.

Internet Architecture Board (IAB). The technical body that oversees the development of the Internet suite of protocols that are known as TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Control Protocol (ICP). The VIrtual NEtworking System (VINES) protocol that provides exception notifications, metric notifications, and PING support. See also Routing update Protocol (RTP).

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet.

Internetwork Packet Exchange (IPX). (1) The network protocol used to connect Novell’s servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology. (2) See also Xerox Network Systems (XNS).
Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units. (T)

intra-area routing. In Internet communications, the routing of data within an area.

Inverse Address Resolution Protocol (InARP). In the Internet suite of protocols, the protocol used for locating a protocol address through the known hardware address. In a frame-relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IP PN. The interface that other protocols can use to transport data over IP.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comments (RFC) 791. It is usually represented in dotted decimal notation.

IP datagram. In the Internet suite of protocols, the fundamental unit of information transmitted through an internet. It contains source and destination addresses, user data, and control information such as the length of the datagram, the header checksum, and flags indicating whether the datagram can be or has been fragmented.

IP router. A device in an IP internet that is responsible for making decisions about the paths over which network traffic will flow. Routing protocols are used to gain information about the network and to determine the best route over which the datagram should be forwarded toward the final destination. The datagrams are routed based on IP destination addresses.

IPXWAN. A Novell protocol that is used to exchange router-to-router information before exchanging standard Internetwork Packet Exchange (IPX) routing information and traffic over wide area networks (WANs).

L2TP Network Server (LNS). An LNS operates on any platform capable that can be a PPP end station. The LNS handles the server side of the L2TP protocol. Since L2TP relies only on the single media over which L2TP tunnels arrive, the LNS has only a single LAN or WAN interface, yet is still able to terminate calls arriving from any the full range of PPP interfaces supported by a LAC. These include asynchronous ISDN, synchronous ISDN, V.120, and other types of connections.

LAN bridge server (LBS). In the IBM Token-Ring Network Bridge Program, the server that keeps statistical information about frames forwarded between two or more rings (through a bridge). The LBS sends these statistics to the appropriate LAN managers through the LAN reporting mechanism (LRM).

LAN Emulation (LE). An ATM Forum standard that supports legacy LAN applications over ATM networks.

LAN Emulation Client (LEC). A LAN Emulation component that represents users of the Emulated LAN.

LAN Emulation Configuration Server (LECS). A LAN Emulation Service component that centralizes and disseminates configuration data.

LAN Emulation Server (LES). A LAN Emulation Service component that resolves LAN Destinations to ATM Addresses.

LAN Network Manager (LNM). An IBM licensed program that enables a user to manage and monitor LAN resources from a central workstation.

LAN segment. (1) Any portion of a LAN (for example, a bus or ring) that can operate independently, but that is connected to other parts of the network by means of bridges. (2) A ring or bus network without bridges.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture. (T) (2) In the Open Systems Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols, that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions in other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

LE. LAN Emulation. An ATM Forum standard that supports legacy LAN applications over ATM networks.

LEC. LAN Emulation Client. A LAN Emulation component that represents users of the Emulated LAN.

LECS. LAN Emulation Configuration Server. A LAN Emulation Service component that centralizes and disseminates configuration data.
**LES.** LAN Emulation Server. A LAN Emulation Service component that resolves LAN Destinations to ATM Addresses.

**line switching.** Synonym for circuit switching.

**link.** The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

**link access protocol balanced (LAPB).** A protocol used for accessing an X.25 network at the link level. LAPB is a duplex, asynchronous, symmetric protocol, used in point-to-point communication.

**link-attached.** (1) Pertaining to devices that are connected to a controlling unit by a data link. (2) Contrast with channel-attached. (3) Synonymous with remote.

**link connection.** (1) The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). (2) In SNA, synonymous with data circuit.

**link level.** (1) A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber’s machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT. (2) See data link level.

**link-state.** In routing protocols, the advertised information about the usable interfaces and reachable neighbors of a router or network. The protocol’s topological database is formed from the collected link-state advertisements.

**link station.** (1) The hardware and software components within a node representing a connection to an adjacent node over a specific link. For example, if node A is the primary end of a multipoint line that connects to three adjacent nodes, node A will have three link stations representing the connections to the adjacent nodes. (2) See also adjacent link station (ALS).

**local.** (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with remote. (3) Synonym for channel-attached.

**local area network (LAN).** (1) A computer network located on a user’s premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. (3) See also Ethernet and token ring. (4) Contrast with metropolitan area network (MAN) and wide area network (WAN).

**local bridging.** A function of a bridge program that allows a single bridge to connect multiple LAN segments without using a telecommunication link. Contrast with remote bridging.

**local management interface (LMI).** See local management interface (LMI) protocol.

**local management interface (LMI) protocol.** In NCP, a set of frame-relay network management procedures and messages used by adjacent frame-relay nodes to exchange line status information over DLCI X’00’. NCP supports both the American National Standards Institute (ANSI) and International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) versions of LMI protocol. These standards refer to LMI protocol as link integrity verification tests (LIVT).

**locally administered address.** In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with universally administered address.

**logical channel.** In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

**logical link.** A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network.

**logical link control (LLC).** The data link control (DLC) LAN sublayer that provides two types of DLC operation for the orderly exchange of information. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery.

**logical link control (LLC) protocol.** In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is
shared. (T) The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

**logical link control (LLC) protocol data unit.** A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP), a source service access point (SSAP), a control field, and user data.

**logical unit (LU).** A type of network accessible unit that enables users to gain access to network resources and communicate with each other.

**loopback test.** A test in which signals from a tester are looped at a modem or other network element back to the tester for measurements that determine or verify the quality of the communications path.

**low-entry networking (LEN).** A capability of nodes to attach directly to one another using basic peer-to-peer protocols to support multiple and parallel sessions between logical units.

**low-entry networking (LEN) end node.** A LEN node receiving network services from an adjacent APPN network node.

**low-entry networking (LEN) node.** A node that provides a range of end-user services, attaches directly to other nodes using peer protocols, and derives network services implicitly from an adjacent APPN network node, that is, without the direct use of CP-CP sessions.

**M**

**Management Information Base (MIB).** (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

**management station.** In Internet communications, the system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol, such as the Simple Network Management Protocol (SNMP).

**mapping.** The process of converting data that is transmitted in one format by the sender into the data format that can be accepted by the receiver.

**mask.** (1) A pattern of characters used to control retention or elimination of portions of another pattern of characters. (l) (A) (2) To use a pattern of characters to

**maximum transmission unit (MTU).** In LANs, the largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for Ethernet is 1500 bytes.

**medium access control (MAC).** In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

**medium access control (MAC) protocol.** In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T)

**medium access control (MAC) sublayer.** In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

**metric.** In Internet communications, a value, associated with a route, which is used to discriminate between multiple exit or entry points to the same autonomous system. The route with the lowest metric is preferred.

**metropolitan area network (MAN).** A network formed by the interconnection of two or more networks which may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with local area network (LAN) and wide area network (WAN).

**MIB.** (1) MIB module. (2) Management Information Base.

**MIB object.** Synonym for MIB variable.

**MIB variable.** In the Simple Network Management Protocol (SNMP), a specific instance of data defined in a MIB module. Synonymous with MIB object.

**MIB view.** In the Simple Network Management Protocol (SNMP), the collection of managed objects, known to the agent, that is visible to a particular community.

**MILNET.** The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

**modem (modulator/demodulator).** (1) A functional unit that modulates and demodulates signals. One of
the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A)
(2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

modulo.  (1) Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. (2) See also modulus.

modulus.  A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 (9 - 4 = 5; 4 - 9 = -5; and 5 divides both 5 and -5 without leaving a remainder).

monitor.  (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

multicast.  (1) Transmission of the same data to a selected group of destinations. (T) (2) A special form of broadcast in which copies of a packet are delivered to only a subset of all possible destinations.

multiple-domain support (MDS).  A technique for transporting management services data between management services function sets over LU-LU and CP-CP sessions. See also multiple-domain support message unit (MDS-MU).

multiple-domain support message unit (MDS-MU).  The message unit that contains management services data and flows between management services function sets over the LU-LU and CP-CP sessions used by multiple-domain support. This message unit, as well as the actual management services data that it contains, is in general data stream (GDS) format. See also control point management services unit (CP-MSU), management services unit (MSU), and network management vector transport (NMVT).

name server.  In the Internet suite of protocols, synonym for domain name server.

nearest active upstream neighbor (NAUN).  In the IBM Token-Ring Network, the station sending data directly to a given station on the ring.

neighbor.  A router on a common subnetwork that has been designated by a network administrator to receive routing information.

NetBIOS.  Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols.

network.  (1) A configuration of data processing devices and software connected for information interchange. (2) A group of nodes and the links interconnecting them.

Network Access Server (NAS).  A device providing temporary, on-demand network access to users. This access is point-to-point using PSTN or ISDN lines.

network accessible unit (NAU).  A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the destination of information transmitted by the path control network. Synonymous with network addressable unit.

network address.  According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU).  Synonym for network accessible unit.

network architecture.  The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion.  An undesirable overload condition caused by traffic in excess of what a network can handle.

network identifier.  (1) In TCP/IP, that part of the IP address that defines a network. The length of the network ID depends on the type of network class (A, B, or C). (2) A 1- to 8-byte customer-selected name or an 8-byte IBM -registered name that uniquely identifies a specific subnetwork.

Network Information Center (NIC).  In Internet communications, local, regional, and national groups
throughout the world who provide assistance, documentation, training, and other services to users.

**network layer.** In Open Systems Interconnection (OSI) architecture, the layer that is responsible for routing, switching, and link-layer access across the OSI environment.

**network management.** The process of planning, organizing, and controlling a communication-oriented data processing or information system.

**network management station.** In the Simple Network Management Protocol (SNMP), a station that executes management application programs that monitor and control network elements.

**network management vector transport (NMVT).** A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

**network manager.** A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

**network node (NN).** See Advanced Peer-to-Peer Networking (APPN) network node.

**network user address (NUA).** In X.25 communications, the X.121 address containing up to 15 binary code digits.

**node.** (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data.

**noncanonical address.** In LANs, a format for the transmission of medium access control (MAC) addresses for token-ring adapters. In noncanonical format, the most significant (leftmost) bit of each address byte is transmitted first. Contrast with canonical address.

**Non-Return-to-Zero Changes-on-Ones Recording (NRZ-1).** A recording method in which the ones are represented by a change in the condition of magnetization, and zeros are represented by the absence of change. Only the one signals are explicitly recorded. (Previously called non-return-to-zero inverted, NRZI, recording.)

**nonseed router.** In AppleTalk networks, a router that acquires network number range and zone list information from a seed router attached to the same network.

**Open Shortest Path First (OSPF).** In the Internet suite of protocols, a function that provides intradomain information transfer. An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

**Open Systems Interconnection (OSI).** (1) The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) (2) The use of standardized procedures to enable the interconnection of data processing systems.

**Note:** OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

**Open Systems Interconnection (OSI) architecture.** Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

**Open Systems Interconnection (OSI) reference model.** A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

**origin.** An external logical unit (LU) or application program from which a message or other data originates. See also destination.

**orphan circuit.** A non-configured circuit whose availability is learned dynamically.

**P**

**pacing.** (1) A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. (2) See also flow control, receive pacing, send pacing, session-level pacing, and virtual route (VR) pacing.

**packet.** In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

**packet internet groper (PING).** (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

---

Glossary 567
packet loss ratio. The probability that a packet will not reach its destination or not reach it within a specified time.

packet mode operation. Synonym for packet switching.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with packet mode operation. See also circuit switching.

parallel bridges. A pair of bridges connected to the same LAN segment, creating redundant paths to the segment.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also explicit route (ER), route extension, and virtual route (VR).

path cost. In link-state routing protocols, the sum of the link costs along the path between two nodes or networks.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment.

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with global character and wildcard character.

permanent virtual circuit (PVC). In X.25 and frame-relay communications, a virtual circuit that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with switched virtual circuit (SVC).

physical circuit. A circuit established without multiplexing. See also data circuit. Contrast with virtual circuit.

physical layer. In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain, and release physical connections over the transmission medium. (T)

physical unit (PU). (1) The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. (2) See also peripheral PU and subarea PU.

ping command. The command that sends an Internet Control Message Protocol (ICMP) echo-request packet to a gateway, router, or host with the expectation of receiving a reply.

Point-to-Point Protocol (PPP). A protocol that provides a method for encapsulating and transmitting packets over serial point-to-point links.

classification. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (6) Synonymous with socket.

port number. In Internet communications, the identification of an application entity to the transport service.
private branch exchange (PBX). A private telephone exchange for transmission of calls to and from the public telephone network.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (T) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with line control discipline and line discipline. See bracket protocol and link protocol.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

pulse code modulation (PCM). A standard adopted for the digitalization of an analog voice signal. In PCM, the voice is sampled at a rate of eight kHz and each sample is coded in an 8-bit frame.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See RNR packet.

received line signal detector (RLSD). In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE). Synonymous with carrier detect and data carrier detect (DCD).

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Synonym for link-attached. (3) Contrast with local.

remote bridging. The function of a bridge that allows two bridges to connect multiple LANs using a telecommunication link. Contrast with local bridging.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any host in the network. The local host receives the results of the command execution.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

reset request packet. In X.25 communications, a packet transmitted by the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE) to request that a virtual call or a permanent virtual circuit be reset. The reason for the request can also be specified in the packet.

ring. See ring network.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.
ring segment. A section of a ring that can be isolated (by unplugging connectors) from the rest of the ring. See LAN segment.

rlogin (remote login). A service, offered by Berkeley UNIX-based systems, that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes information about the user’s environment (for example, terminal type) to the remote machine.

RNR packet. A packet used by a data terminal equipment (DTE) or by a data circuit-terminating equipment (DCE) to indicate a temporary inability to accept additional packets for a virtual call or permanent virtual circuit.

root bridge. The bridge that is the root of a spanning tree formed between other active bridges in the bridging network. The root bridge originates and transmits bridge protocol data units (BPDUs) to other active bridges to maintain the spanning tree topology. It is the bridge with the highest priority in the network.

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunication link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also explicit route (ER), path, and virtual route (VR).

Route Selection control vector (RSCV). A control vector that describes a route within an APPN network. The RSCV consists of an ordered sequence of control vectors that identify the TGs and nodes that make up the path from an origin node to a destination node.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. (3) In OSI terminology, a function that determines a path by which an entity can be reached. (4) In TCP/IP, synonymous with gateway. (5) Contrast with bridge.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing domain. In Internet communications, a group of intermediate systems that use a routing protocol so that the representation of the overall network is the same within each intermediate system. Routing domains are connected to each other by exterior links.

Routing Information Protocol (RIP). In the Internet suite of protocols, an interior gateway protocol used to exchange intradomain routing information and to determine optimum routes between internet hosts. RIP determines optimum routes on the basis of route metrics, not link transmission speed.

routing loop. A situation that occurs when routers circulate information among themselves until convergence occurs or until the networks involved are considered unreachable.

routing protocol. A technique used by a router to find other routers and to remain up to date about the best way to get to reachable networks.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). In AppleTalk networks, a protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

Routing update Protocol (RTP). The Virtual NETworking System (VINES) protocol that maintains the routing database and allows the exchange of routing information between VINES nodes. See also Internet Control Protocol (ICP).

rsh. A variant of the rlogin command that invokes a command interpreter on a remote UNIX machine and passes the command-line arguments to the command interpreter, skipping the login step completely.

S

SAP. See service access point.

seed router. In AppleTalk networks, a router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed
router must be initially set up using the configurator tool. Contrast with nonseed router.

**segment.** (1) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

**segmenting.** In OSI, a function performed by a layer to map one protocol data unit (PDU) from the layer it supports into multiple PDUs.

**sequence number.** In communications, a number assigned to a particular frame or packet to control the transmission flow and receipt of data.

**Serial Line Internet Protocol (SLIP).** A protocol used over a point-to-point connection between two IP hosts over a serial line, for example, a serial cable or an RS232 connection into a modem, over a telephone line.

**server.** A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

**service access point (SAP).** (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

**Service Advertising Protocol (SAP).** In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and address recorded in all file servers running NetWare.
- A mechanism that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type.
- A mechanism that allows a workstation to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

**session.** (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session. (3) In L2TP, L2TP creates a session when an end-to-end PPP connection is attempted between a dial user and the LNS; regardless of whether the user initiates the session or the LNS initiates an outbound call. The datagrams for the session are sent over the tunnel between the LAC and LNS. The LNS and LAC maintain the state information for each user attached to an LAC.

**Simple Network Management Protocol (SNMP).** In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application’s Management Information Base (MIB).

**SNA management services (SNA/MS).** The services provided to assist in management of SNA networks.

**socket.** (1) An endpoint for communication between processes or application programs. (2) The abstraction provided by the University of California’s Berkeley Software Distribution (commonly called Berkeley UNIX or BSD UNIX) that serves as an endpoint for communication between processes or applications.

**source route bridging.** In LANs, a bridging method that uses the routing information field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The routing information field is inserted into the MAC header by the source node. The information in the routing information field is derived from explorer packets generated by the source host.

**source routing.** In LANs, a method by which the sending station determines the route the frame will follow and includes the routing information with the frame. Bridges then read the routing information to determine whether they should forward the frame.

**source service access point (SSAP).** In SNA and TCP/IP, a logical address that allows a system to send data to a remote device from the appropriate communications support. Contrast with destination service access point (DSAP).

**spanning tree.** In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topology to ensure that there is only one route between any two LANs in the bridged network. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

**sphere of control (SOC).** The set of control point domains served by a single management services focal point.
sphere of control (SOC) node. A node directly in the sphere of control of a focal point. A SOC node has exchanged management services capabilities with its focal point. An APPN end node can be a SOC node if it supports the function to exchange management services capabilities.

split horizon. A technique for minimizing the time to achieve network convergence. A router records the interface over which it received a particular route and does not propagate its information about the route back over the same interface.

spoofing. For data links, a technique in which a protocol initiated from an end station is acknowledged and processed by an intermediate node on behalf of the final destination. In IBM 6611 data link switching, for example, SNA frames are encapsulated into TCP/IP packets for transport across a non-SNA wide area network, unpacked by another IBM 6611, and passed to the final destination. A benefit of spoofing is the prevention of end-to-end session timeouts.

standard MIB. In the Simple Network Management Protocol (SNMP), a MIB module that is located under the management branch of the Structure of Management Information (SMI) and that is considered a standard by the Internet Engineering Task Force (IETF).

static route. The route between hosts, networks, or both that is manually entered into a routing table.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

StreetTalk. In the Virtual NEtworking System (VINES), a unique network-wide naming and addressing system that allows users to locate and access any resource on the network without knowing the networking topology. See also Internet Control Protocol (ICP) and Routing update Protocol (RTP).

Structure of Management Information (SMI). (1) In the Simple Network Management Protocol (SNMP), the rules used to define the objects that can be accessed by means of a network management protocol. (2) In OSI, the set of standards relating to management information. The set includes the Management Information Model and the Guidelines for the Definition of Managed Objects.

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for subnetwork.

subnet address. In Internet communications, an extension to the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnet mask. Synonym for address mask.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with subnet.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use $\$AA$ as their service access point (SAP) value.

subnet network mask. Synonym for address mask.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

switched virtual circuit (SVC). An X.25 circuit that is dynamically established when needed. The X.25 equivalent of a switched line. Contrast with permanent virtual circuit (PVC).

synchronous. (1) Pertaining to two or more processes that depend upon the occurrence of specific events such as common timing signals. (T) (2) Occurring with a regular or predictable time relationship.

Synchronous Data Link Control (SDLC). (1) A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I) (2) Contrast with binary synchronous communication (BSC).

SYNTAX. In the Simple Network Management Protocol (SNMP), a clause in the MIB module that defines the abstract data structure that corresponds to a managed object.

system. In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions. (I) (A)

system configuration. A process that specifies the devices and programs that form a particular data processing system.
system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for users of the network. Multiple S SCPs, cooperating as peers with one another, can divide the network into domains of control, with each S SCP having a hierarchical control relationship to the physical units and logical units within its own domain.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

TCP/IP. (1) Transmission Control Protocol/Internet Protocol. (2) A UNIX-like/Ethernet-based system-interconnect protocol originally developed by the US Department of Defense. TCP/IP facilitated ARPANET (Advanced Research Projects Agency Network), a packet-switched research network for which Layer 4 was TCP and Layer 3, IP.

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a “threshold exceeded” occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

throughput class. In packet switching, the speed at which data terminal equipment (DTE) packets travel through the packet switching network.

time to live (TTL). A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also local area network (LAN).

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

topology database update (TDU). A message about a new or changed link or node that is broadcast among APPN network nodes to maintain the network topology database, which is fully replicated in each network node. A TDU contains information that identifies the following:

- The sending node
- The node and link characteristics of various resources in the network
- The sequence number of the most recent update for each of the resources described.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

transceiver (transmitter-receiver). In LANs, a physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and that sense collisions.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

transmission group (TG). (1) A connection between adjacent nodes that is identified by a transmission group number. (2) In a subarea network, a single link or a group of links between adjacent nodes. When a transmission group consists of a group of links, the links are viewed as a single logical link, and the transmission group is called a multilink transmission group (MLTG). A mixed-media multilink transmission group (MMMLTG) is one that contains links of different medium types (for example, token-ring, switched SDLC, nonswitched SDLC, and frame-relay links). (3) In an APPN network, a single link between adjacent nodes. (4) See also parallel transmission groups.

transmission header (TH). Control information, optionally followed by a basic information unit (BIU) or a BIU segment, that is created and used by path control to route message units and to control their flow within the network. See also path information unit.

transparent bridging. In LANs, a method for tying individual local area networks together through the medium access control (MAC) level. A transparent bridge stores the tables that contain MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

transport layer. In the Open Systems Interconnection reference model, the layer that provides a reliable end-to-end data transfer service. There may be relay open systems in the path. (T) See also Open Systems Interconnection reference model.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Tunnel. A tunnel is defined by an LNS-LAC pair. The tunnel carries PPP datagrams between the LAC and the LNS. A single tunnel can multiplex many sessions. A control connection operating over the same tunnel controls the establishment, release, and maintenance of all sessions and of the tunnel itself.

tunneling. To treat a transport network as though it were a single communication link or LAN. See also encapsulation.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The European version (E1) transmits 2.048 Mbps.

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with locally administered address.

User Datagram Protocol (UDP). In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

V.24. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

V.25. In data communication, a specification of the CCITT that defines the automatic answering equipment and parallel automatic calling equipment on the General Switched Telephone Network, including procedures for disabling of echo controlled devices for both manually and automatically established calls.

V.34. An ITU-T Recommendation for modem communication over standard commercially available voice-grade 33.6-Kbps (and slower) channels.

V.35. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

V.36. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at rates of 48, 56, 64, or 72 kilobits per second.

version. A separately licensed program that usually has significant new code or new function.

VINES. Virtual NEtworking System.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also data circuit. Contrast with physical circuit. (2) A logical connection established between two DTEs.

virtual connection. In frame relay, the return path of a potential connection.

virtual link. In Open Shortest Path First (OSPF), a point-to-point interface that connects border routers that are separated by a non-backbone transit area. Because area routers are part of the OSPF backbone, the virtual link connects the backbone. The virtual links ensure that the OSPF backbone does not become discontinuous.
Virtual Networking System (VINES). The network operating system and network software from Banyan Systems, Inc. In a VINES network, virtual linking allows all devices and services to appear to be directly connected to each other, when they may actually be thousands of miles apart. See also StreetTalk.

Virtual route (VR). (1) In SNA, either (a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or (b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). (2) Contrast with explicit route (ER). See also path and route extension (REX).

Wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communication network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. (3) Contrast with local area network (LAN) and metropolitan area network (MAN).

Wildcard character. Synonym for pattern-matching character.

Wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communication network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. (3) Contrast with local area network (LAN) and metropolitan area network (MAN).

Wildcard character. Synonym for pattern-matching character.

X21. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for a general-purpose interface between data terminal equipment and data circuit-terminating equipment for synchronous operations on a public data network.

X.25. (1) An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. (2) See also packet switching.

Xerox Network Systems (XNS). The suite of internet protocols developed by the Xerox Corporation. Although similar to TCP/IP protocols, XNS uses different packet formats and terminology. See also Internetwork Packet Exchange (IPX).

Zone Information Protocol (ZIP). In AppleTalk networks, a protocol that provides zone management service by maintaining a mapping of the zone names and network numbers across the internet on the session layer.

Zone information table (ZIT). A listing of network numbers and their associated zone name mappings in the internet. This listing is maintained by each internet router in an AppleTalk internet.
Index

A
access-control
   IPv6 monitoring command 464
accounting and node statistics 34
activate
   APPN monitoring command 234
activate_new_config
   APPN configuration command 214
add
   AppleTalk Phase 2 configuration command 285
   APPN configuration command 141
   IPv6 configuration command 445
   IPv6 update packet filter configuration command 459
   NDP configuration command 473
   OSI configuration command 367
   RIP6 configuration command 501
   VINES configuration command 305
Address Resolution Protocol (ARP)
   VINES 302
addresses
   OSI/DECnet V monitoring command 392
aping
   APPN monitoring command 234
AppleTalk Control Protocol
   for PPP 278
AppleTalk Phase 2
   basic configuration procedures 277, 279
   configuring 277
   monitoring 285
   network parameters 277, 280
   router parameters 277
AppleTalk Phase 2 configuration commands
   add 285
   delete 287
   disable 288
   enable 289
   list 290
   set 291
AppleTalk Phase 2 monitoring commands
   atecho 293
   cache 294
   clear counters 294
   counters 294
   dump 295
   interface 295
APPN 75
   monitoring 231
APPN (DLSw) 21
APPN configuration commands
   activate_new_config 214
   add 141
   delete 213
   enable/disable 96
   list 214
   set 97
   TN3270 95
APPN dynamic reconfiguration 275
APPN Frame Relay BAN Connection Network 38, 194, 195
APPN monitoring commands
   accessing 231
   activate 234
   aping 234
   deactivate link 235
   dump 235
   list 236
   log 257
   memory 261
   restart 264
   rtp status 263
   rtp switchpath 263
   rtp test 263
   stop 265
   summary 231
   tn3270e 265
atecho
   AppleTalk Phase 2 monitoring command 293
ATM
   APPN using 57
ATM LAN Emulation
   configuring DNA IV 314

B
before you configure 31
BGP monitoring commands
   destinations
      received 532
BGP6 configuration commands 514, 519, 521, 522, 523
   add
      aggregate 514
      neighbor 514
      no-receive 516
      receive 517
      send 518
   change
      change originate 520
      change receive 520
      change send 521
   delete
      aggregate 521
      neighbor 521
      no 522
      originate 522
      receive 522
      send 522
   disable
      BGP6 speaker 523
      classless-bgp 523
      neighbor 523
      enable 523
      BGP6 speaker 523
      compare-med-from-diff-AS 523
BGP6 configuration commands  514, 519, 521, 522, 523 (continued)
  neighbor  523
  list
    aggregate  524
    all  524
    BGP6 speaker  524
    neighbor  525
    no  525
    originate  525
    receive  525
    send  525
  move  526
  policy-to-neighbor  520, 522, 525
  set  526
  update  526
BGP6 dynamic reconfiguration  536
BGP6 monitoring commands
  disable neighbor  529
  dump routing tables  529
  enable neighbor  530
  list  530
  neighbors  532
  parameter  533
  paths  534
  ping6  534
  policy-list  535
  reset neighbor  535
  sizes  535
  traceroute6  536
Border Gateway Protocol for IPv6—see BGP6  536
Border Node
  COS mapping table  211
  routing list  207
Branch Extender  13, 16, 25, 173, 174, 175, 176, 206, 207
C
  cache
    AppleTalk Phase 2 monitoring command  294
    IPv6 monitoring command  464
  change
    IPv6 configuration command  451
    IPv6 update packet filter configuration command  461
    NDP configuration command  475
    RIP6 configuration command  502
  change metric
    OSI/DECnet V monitoring command  392
  change prefix-address  373
  clear  375
  PIM monitoring command  489
  CLNP protocol  349
  clnp-Stats
    OSI/DECnet V monitoring command  393
  command summary
    BGP  513, 528
    DNA IV  329
  configurable Held Alert Queue  19, 31, 139
  configuration changes, affect on the router  20
  configuration options  21
configuration requirements  21
configuring TN3270 under APPN  75
connection networks  12
COS  31
CoS mapping table  29
  counters
    AppleTalk Phase 2 monitoring command  294
    IPv6 monitoring command  464
    VINES monitoring command  309
D
  DDDLU  79
  Creating LUs at VTAM  79
  Deleting LUs from VTAM  80
  example VTAM PU definition  80
  using Network Dispatcher with  80
  deactivate link
    APPN monitoring command  235
  deactivate LU
    TN3270E monitoring command  265
DECnet NCP
  See NCP  313
  delete
    AppleTalk Phase 2 configuration command  287
    APPN configuration command  213
    IPv6 configuration command  452
    IPv6 update packet filter configuration command  462
    NDP configuration command  477
    OSI configuration command  376
    PIM configuration command  484
    RIP6 configuration command  504
    VINES configuration command  306
  destination devices  416
  dhcpv6-relay
    NDP monitoring command  479
  Dial on Demand  45
    APPN using  45
  Digital Network Architecture (DNA) phase IV  313
  disable
    AppleTalk Phase 2 configuration command  288
    APPN configuration command  96
    IPv6 configuration command  452
    IPv6 update packet filter configuration command  462
    NDP configuration command  477
    OSI configuration command  378
    PIM configuration command  485
    RIP6 configuration command  504
    VINES configuration command  306
  DLUR  8, 30, 35
  DLUR retry algorithm  35
  DNA IV
    access control
      configuring  318
      exclusive  319
      inclusive  318
      managing traffic  317
    addressing
      802.5 Token  314
      description  314
      Ethernet data link  314
DNA IV (continued)

X.25 data link 314
area routers
description 315
level 1 315
level 2 316
area routing filters 320
area support of 313
blending domains 322
configuration
for X.25 326
configuring over ATM LAN Emulation 314
designated router for 315
LAT protocol 313
MOP support of 313
Network Control Program (NCP) 316
See NCP 313
routings 315
routings parameters 316
routings tables 315
special considerations and limitations 313
terminology and concepts 314

DNA IV configuration commands
define
circuit 330
executor 333
module access 336
module routing 337
node 337
help 330
purge
module access 338
module routing 338
show
area 338
node 340
show/list
circuit 341
executor 344
module access 346
module routing 346
zero
circuit 347
executor 347
module access 347

DNA IV monitoring commands
define
circuit 330
executor 333
module access 336
module routing 337
node 337
help 330
purge
module access 338
module routing 338
show
area 338
node 340
show/list
circuit 341
Extended Border Node 14, 16
configuring 25
CoS mapping table 29
network requirements 16
routing list 28
extensions
IBM vendor-private extensions. 417
path information extensions 417

F
features
IP version 6 (IPv6) 439
focal point 17, 30

G
getting help 285

H
help
console command 285
HIDLU 81
HPR 6, 30

I
IBM-specific extensions
NHRP 417
implementation on the router 3
implicit focal point 19, 204
interface
AppleTalk Phase 2 monitoring command 295
IPv6 monitoring command 465
PIM monitoring command 489
intermediate session data, collecting 34
internal
IPv6 monitoring command 465
IP
packet size 542
IPv6
configuring 445
overview 439
using 439
ipv6 command 445
IPv6 configuration commands
add 445
change 451
delete 452
disable 452
enable 452
list 453
move 455
set 455
summary 445
update 458
IPv6 dynamic reconfiguration 469
IPv6 monitoring commands
access-control 464
accessing 463
IPv6 monitoring commands (continued)
cache 464
counters 464
dump 464
interface 465
internal 465
mcast 465
mld 465
packet-filter 467
path-mtu 467
ping6 468
reset 466
route 466
sizes 466
sniffer 466
static 467
summary of 463
traceroute6 468
tunnels 469
IPv6 update packet filter configuration commands
add 459
change 461
delete 462
list 462
move 462
is-adjacencies
OSI/DECnet V monitoring command 398
IS-IS messages
IS to IS hello (IIH) messages 355
point-to-point 356
IS-IS protocol
description 353
IS-IS areas 353
IS-IS domain 353
IS to IS hello (IIH) messages
L1 355
IS to IS Hello (IIH) messages
L2 356
overview 349
is-is-stats
OSI/DECnet V monitoring command 398
ISDN Permanent Circuit
APPN using 43
ISDN permanent connection 43

J
join
PIM monitoring command 490

L
l1-routes
OSI/DECnet V monitoring command 399
l1-Summary
OSI/DECnet V monitoring command 400
l1-Update
OSI/DECnet V monitoring command 402
l2-Routes
OSI/DECnet V monitoring command 400
l2-Summary
OSI/DECnet V monitoring command 401
N2-Update
OSI/DECnet V monitoring command 403
lane shortcut interface (LSI)
NHRP 414
leave
PIM monitoring command 490
link level parameter lists 42
list
AppleTalk Phase 2 configuration command 290
APPN configuration command 214
APPN monitoring command 236
IPv6 configuration command 453
IPv6 update packet filter configuration command 462
NDP configuration command 478
NDP monitoring command 479
OSI configuration command 379
PIM configuration command 485
RIP6 configuration command 507
RIP6 monitoring command 511
TN3270E monitoring command 266
VINES configuration command 307
Local Area Terminal (LAT) protocol 313
log
APPN monitoring command 257
LSI 414
LU parameter list 42

M
managing network nodes 17
managing the router network node 17
mcache
PIM monitoring command 490
mcast
IPv6 monitoring command 465
memory
APPN monitoring command 261
message units, supported, APPN-related alerts 18
MFC dynamic reconfiguration 498
MFC for IPv6 dynamic reconfiguration 498
mgroups
PIM monitoring command 491
mld
IPv6 monitoring command 465
monitoring
APPN 231
IPv6 monitoring commands 463
NDP monitoring commands 479
PIM monitoring commands 489
RIP6 monitoring commands 510
move
IPv6 configuration command 455
IPv6 update packet filter configuration command 462
mstats
PIM monitoring command 492
Multicast Forwarding Cache- -see MFC 498

N
NCP
description of 316
NCP configuration commands
purge 338
set 338
show 338
show circuit 341
summary of 329
zero 347
NCP monitoring commands
purge 338
set 338
show 338
show circuit 341
summary of 329
zero 347
NDP
configuring 473
NDP command 473
NDP configuration commands
add 473
change 475
delete 477
disable 477
enable 477
list 478
set 478
summary 473
NDP monitoring commands
accessing 478
dhcpv6-relay 479
dump 479
list 479
ping6 480
summary of 479
NDP6 dynamic reconfiguration 480
neighbor
PIM monitoring command 493
neighbor discovery protocol for IPv6--see NDP6 480
Network Control Protocols (NCP)
for PPP interfaces
AppleTalk Control Protocol 278
Next Hop Resolution Protocol
overview 407
next-hop routers 416
NHRP 407
benefits 408
destination devices 416
examples
classic IP environment 409
classic IP environment with non-NHRP device 410
Egress Router 413
LAN emulation 411
LAN switches 411
mixed classical IP and ELAN 412
exclude lists 416
implementation 414
disallowed router-to-router shortcuts 417
IBM-specific extensions 417
LANE shortcuts 414
limitations 409
next-hop routers 416
Open System Interconnection (OSI) (continued)
link state databases 357
link state updates 357
multicast addresses 352
network address structure 350
network addresses 350
Network Entity Title (NET) 351
network protocol data units (NPDU) 349
NSAP addressing 350
protocols running under 349
pseudonode 356
routing metric 358
routing tables 358
synonymous areas 354
unattached L2 IS routers 358
optional features 5
OSI
configuring 363
X.25 over OSI 369
OSI configuration commands
add 367
change prefix address 373
clear 375
delete 376
disable 378
enable 378
list 379
set 385
summary of 367
OSI/DECnet V
monitoring 367
OSI/DECnet V monitoring commands
addresses 392
change metric 392
clnp-stats 393
designated-router 394
DNAV-info 395
es-adjacencies 395
es-is-stats 396
is-adjacencies 398
is-is-stats 398
I1-routes 399
I1-summary 400
I1-update 402
I2-routes 400
I2-summary 401
I2-update 403
OSI/DECnet V monitoring command 394
ping-1139 403
route 403
send (echo packet) 404
subnets 404
summary of 391
toggle (alias/no alias) 405
trace route 405

P
packet-filter
IPv6 monitoring command 467
packet size 541
path-mtu
  IPv6 monitoring command 467
pim
  PIM monitoring command 494
PIM
  configuring 483
  PIM command 484
PIM configuration commands
  delete 484
  disable 485
  enable 485
  list 485
  set 486
  summary 484
PIM dynamic reconfiguration 496
PIM for IPv6 dynamic reconfiguration 497
PIM monitoring commands
  accessing 488
  clear 489
  dump 489
  interface 489
  join 490
  leave 490
  mcache 490
  mgroups 491
  mstats 492
  neighbor 493
  pim 494
  ping 495
  reset 495
  summary of 489
  summary pim 494
  traceroute 495
  variables 495
ping
  PIM monitoring command 495
  ping-1139
    OSI/DECnet V monitoring command 403
ping6
  BGP6 monitoring command 534
  IPv6 monitoring command 468
  NDP monitoring command 480
  RIP6 monitoring command 511
Point-to-Point Protocol (PPP)
  AppleTalk Control Protocol 278
policy-list
  BGP6 monitoring command 535
port level parameter lists 42
port types supported 20
Protocol Independent Multicast Routing Protocol--see
  PIM 496
protocols
  Digital Network Architecture (DNA) Phase IV 313
Protocols
  BGP 539
  comparison table 539
  FTP 539
  ICMP 539
  IP 539
  IPX 539
  key to 539

Protocols (continued)
  RIP 539
  SGMP 539
  SNMP 539
  TCP 539
  TFTP 539

R
reset
  IPv6 monitoring command 466
  PIM monitoring command 495
  RIP6 monitoring command 511
restart
  APPN monitoring command 264
restrictions 37
RIP6
  configuring 501
  RIP6 command 501
RIP6 configuration commands
  add 501
  change 502
  delete 504
  disable 504
  enable 506
  list 507
  set 507
  summary 501
RIP6 dynamic reconfiguration 511
RIP6 monitoring commands
  accessing 510
  dump 511
  list 511
  ping6 511
  reset 511
  summary of 510
  traceroute6 511
route
  IPv6 monitoring command 466
  OSI/DECnet V monitoring command 403
routing information protocol for IPv6--see RIP6 511
routing list 28
routing tables
  BGP6 dump command 529
rtp status
  APPN monitoring command 263
rtp switchpath
  APPN monitoring command 263
rtp test
  APPN monitoring command 263
RU size 33, 117

S
SDLC 59
  APPN using 59
Seed router
  AppleTalk Phase 2 277, 280
send (Echo Packet)
  OSI/DECnet V monitoring command 404
set
  AppleTalk Phase 2 configuration command 291
set (continued)

APPN configuration command 97
IPv6 configuration command 455
NDP configuration command 478
OSI configuration command 385
PIM configuration command 486
IPv6 configuration command 507
VINES configuration command 308
sizes
IPv6 monitoring command 466
sniffer
IPv6 monitoring command 466
SNMP managed node, using the router as 19
sphere of control 17
static
IPv6 monitoring command 467
stop
APPN monitoring command 265
subnets
OSI/DECnet V monitoring command 404
summary of
NCP configuration commands 329
NCP monitoring commands 329
summary pim
PIM monitoring command 494
supported message units 18
supported message units, APPN-related alerts 18

T

talk
OPCON command 231, 445, 463, 473, 478, 484, 488, 501, 510
TG characteristics 31
the router as entry point 17
TN3270 71
  tn3270E server configuration 75
  what is 71
tn3270e
APPN monitoring command 265
TN3270E monitoring commands
deactivate LU 265
list 266
TN3270E server 72
TN3270E Server
  client IP Address to LU/Pool Mapping 83
customer to LU mapping 82
configuration commands 215
Configuration parameters 215
Configuring, using DLUR 88
Configuring, using local node identifier 92
example configurations 87
load balancing among multiple PUs 87
monitoring commands 265
port and IP address mapping 86
Server TCP port to pool mapping 85
tn3270E server configuration 75
toggle (Alias/No Alias)
  OSI/DECnet V monitoring command 405
Token-Ring 4/16
  packet size 541
topology Database Garbage Collection 19
traceroute
  OSI/DECnet V monitoring command 405
  PIM monitoring command 495
traceroute6
  BGP6 monitoring command 536
  IPv6 monitoring command 468
  RIP6 monitoring command 511
traces 34
tracing 34
transmission group characteristics, setting 31
transporting data 38
tunnels
  IPv6 monitoring command 469

U

update
IPv6 configuration command 458
using the router as SNMP managed node 19

V

V.25 bis 54
  APPN using 54
V.34
  APPN using 56
variables
  PIM monitoring command 495
VINES 307
  Address Resolution Protocol (ARP) 302
  basic configuration procedures 303
  client nodes 297
  configuring 297
  disabling an interface 306
  disabling globally 306
  enabling an interface 306
  enabling globally 306
  monitoring 305
  monitoring commands 309
  neighbor tables 300
dumping 310
setting size 308
network layer protocols 298
  Address Resolution Protocol (ARP) 302
  Internet Control Protocol (ICP) 302
  Routing Update Protocol (RTP) 299
  VINES IP 298
  overview 297
routing tables 299
dumping 310
setting size 308
RTP implementation 301
service nodes 297
setting number of client nodes 308
VINES configuration commands 305
VINES monitoring commands
counters 309
dump 310
exit 311
virtual network interface (VNI)
  NHRP 414
VNI 414
VTAM DSPU 10

W

WAN reroute 48
WAN restoral 53
Readers’ Comments — We’d Like to Hear from You

Nways Multiprotocol Routing Services
Protocol Configuration and Monitoring
Reference Volume 2
Version 3.4

Publication No. SC30-3865-06

Overall, how satisfied are you with the information in this book?

<table>
<thead>
<tr>
<th>Overall satisfaction</th>
<th>Very Satisfied</th>
<th>Satisfied</th>
<th>Neutral</th>
<th>Dissatisfied</th>
<th>Very Dissatisfied</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How satisfied are you that the information in this book is:

<table>
<thead>
<tr>
<th></th>
<th>Very Satisfied</th>
<th>Satisfied</th>
<th>Neutral</th>
<th>Dissatisfied</th>
<th>Very Dissatisfied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complete</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Easy to find</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Easy to understand</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Well organized</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applicable to your tasks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please tell us how we can improve this book:

Thank you for your responses. May we contact you?  □ Yes  □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.
Spine information:

IBM

Nways Multiprotocol Routing Services

MRS V3.4 Protocol Reference V2