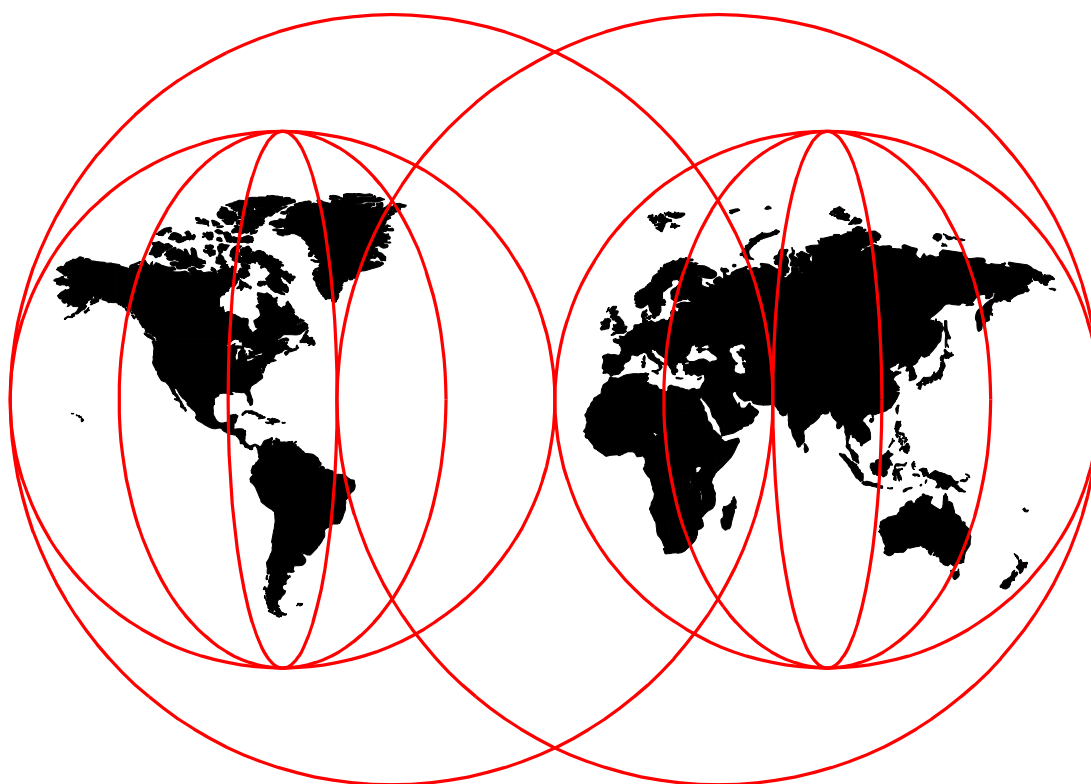


Mobile Computing: The eNetwork Wireless Solution

*Juan R. Rodriguez, Werner Schollenberger,
Muchsin Anzib, Bhaktianto Widyarso*



International Technical Support Organization

<http://www.redbooks.ibm.com>



International Technical Support Organization

SG24-5299-00

Mobile Computing: The eNetwork Wireless Solution

March 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, "Special Notices" on page 243.

First Edition (March 1999)

This edition applies to Version 4.1.2 of IBM eNetwork Wireless Gateway for use with the AIX Operating System, Version 4.1.3 of IBM eNetwork Emulator Express for Windows and AIX, and Version 2.1.1 of IBM eNetwork Web Express for Windows and AIX.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1999. All rights reserved

Note to U.S Government Users - Documentation related to restricted rights - Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	vii
Tables	xi
Preface	xiii
The Team That Wrote This Redbook	xiii
Comments Welcome	xiv
<hr/>	
Part 1. Introduction	1
Chapter 1. Introduction	3
1.1 eNetwork Wireless Gateway and Client	4
1.2 eNetwork Emulator Express	5
1.3 eNetwork Web Express	6
1.4 Putting It All Together	8
1.5 When Express Software Can Be Used Efficiently	9
1.6 Optimizing Other TCP/IP-Based Applications	10
<hr/>	
Part 2. eNetwork Wireless Gateway and Client	15
Chapter 2. Technical Basics of Wireless Communication	17
2.1 Mobile versus Wireless	17
2.2 Wireless Mobile Network Technologies	19
2.2.1 DataTAC	21
2.2.2 Motorola Private Mobile Radio (PMR)	27
2.2.3 Mobitex	29
2.2.4 Cellular Digital Packet Data (CDPD)	31
2.2.5 PSTN	33
2.2.6 Analog Cellular Phone Systems (AMPS)	34
2.2.7 GSM	35
2.2.8 Dataradio	40
2.3 Connections via X.25	41
2.4 Which Wireless Network Is the Best?	43
2.5 Functions of the eNetwork Wireless Gateway and Client	44
2.5.1 eNetwork Wireless Gateway Software Architecture	45
2.5.2 IP Addressing with eNetwork Wireless	46
2.5.3 Data Transmission Techniques	46
2.5.4 Optimization Techniques	48
2.5.5 IP Packet Filtering and Mapping	50
2.5.6 DataTAC Transmission Parameters for Motorola PMR	51
2.5.7 Broadcast Messages	52
Chapter 3. Install, Configure and Manage the Wireless Gateway	53
3.1 eNetwork Wireless Gateway Requirements	53
3.1.1 Hardware Requirements	54
3.1.2 Software Requirements	54
3.2 Preparing the System	55
3.2.1 Before You Start	55
3.2.2 Setting the Language Environment	57
3.2.3 AIX System Resources	58
3.2.4 Configuring X.25 Support	59

3.2.5	Installing and Configuring Serial Line Support	65
3.2.6	Configuring TCP/IP	69
3.2.7	Enabling the Portmap Daemon for Automatic Startup	71
3.3	Installing and Removing eNetwork Wireless Gateway Product Files	72
3.3.1	Installing eNetwork Wireless Gateway Product Files	72
3.3.2	Installing CSDs	74
3.3.3	Removing eNetwork Wireless Gateway Product Files	74
3.3.4	Upgrading from Earlier Versions	75
3.4	Configuring the eNetwork Wireless Gateway	75
3.4.1	Defining X.25 Reset Delay Timer Interval	76
3.4.2	Creating Mobile Network Interface	77
3.4.3	Configuring the Mobile Network Interface for the Desired Networks	79
3.4.4	Registering eNetwork Wireless Client	88
3.4.5	Configuring Mobile Client Connections	91
3.4.6	Advanced Configuration	94
3.5	Starting/Stopping eNetwork Wireless Gateway	95
3.5.1	Starting a Mobile Network Interface	95
3.5.2	Stopping a Mobile Network Interface	97
3.6	eNetwork Wireless Network Management	97
3.6.1	Configuring eNetwork Wireless Network Management	98
3.6.2	Monitoring eNetwork Wireless Configuration	100
Chapter 4.	Wireless Client	107
4.1	Introduction	107
4.2	Installation and Configuration	108
4.2.1	Checklist	108
4.2.2	Setting Up the installation Environment	109
4.2.3	Setting Up the Wireless Modems	110
4.2.4	Registering a Mobile Client at eNetwork Wireless Gateway	113
4.2.5	Wireless Client Installation and Removal	113
4.2.6	Configuring the eNetwork Wireless Client	116
4.2.7	Advanced Configuration Issues	127
4.2.8	Managing eNetwork Wireless Client Connection Profiles	130
4.2.9	Preparing and Running the eNetwork Wireless Client	133
Chapter 5.	Troubleshooting	141
5.1	A Communication Problem Overview	141
5.2	Categories of Problems in Wireless Network Environments	141
5.3	Accessing the Wireless Network	143
5.4	X.25 Problems	144
5.5	Mobile User Reports Problem	145
5.6	Some Problem Scenarios, Analysis and Troubleshooting	146
5.6.1	General Information	146
5.6.2	The Problem Scenarios	146
5.6.3	DataTAC ARDIS Network Problem	147
Chapter 6.	Performance and Security Issues	153
6.1	Measuring Performance	153
6.1.1	Measuring Wireless Network Transmission Parameters	153
6.1.2	Benchmarking Application Scenarios	156
6.2	Optimizing IP MTU Sizes for Single Radio Networks	159
6.3	How eNetwork Wireless Scales	162
6.4	Security Issues	164
6.4.1	Not Connected to the Internet	165

6.4.2 Gateway Connected to the Internet	166
---	-----

Part 3. The eNetwork Express Software Family171

Chapter 7. IBM eNetwork Emulator Express	173
7.1 Overview	173
7.2 IBM eNetwork Emulator Express Architecture	174
7.2.1 IBM eNetwork Emulator Express Components	174
7.2.2 Data Reduction Process	175
7.2.3 3270 File Transfer	176
7.3 Emulator Express Server Installation	176
7.3.1 Installing Emulator Express Server for Windows NT	176
7.3.2 Installing Emulator Express Server for AIX	177
7.4 Emulator Express Server Configuration	178
7.4.1 Emulator Express Server for Windows NT Configuration	178
7.4.2 Emulator Express Server for AIX Configuration	182
7.5 Emulator Express Client Installation	188
7.5.1 Installing Emulator Express Client for Windows 95/NT	188
7.5.2 Re-installing Emulator Express Client for Windows 95/NT	189
7.5.3 Uninstalling Emulator Express for Windows 95/NT	189
7.6 Emulator Express Client Configuration for Windows 95/NT	189
7.6.1 Emulator Express Client for Windows 95/NT Configuration	189
7.6.2 Configuring Telnet 3270/5250 Emulator to Use Emulator Express	191
7.7 Sample Scenario	192
7.7.1 Configuring Emulator Express Server	193
7.7.2 Configuring Emulator Express Client	193
7.7.3 PCOMM Telnet 3270 Configuration	195
7.8 Troubleshooting	196
7.8.1 Monitoring	196
7.8.2 Logging	200
7.8.3 Traces	202
Chapter 8. IBM eNetwork Web Express	205
8.1 Introduction	205
8.1.1 Wireless Networks and Web-Based Applications	205
8.2 Web Express Implementation	206
8.2.1 eNetwork Web Express Components	207
8.2.2 eNetwork Web Express Optimization Methods	208
8.2.3 Web Express Solution Highlights	208
8.2.4 Supported Platforms	209
8.2.5 Web Express Server Installation - Windows NT	209
8.2.6 Web Express Server Installation - AIX	209
8.3 Sample Scenario	210
8.3.1 Web Express Server Basic Configuration - Windows NT	211
8.3.2 Web Express Advanced Configuration - Windows NT	213
8.3.3 Web Express Server Configuration - AIX	217
8.3.4 Web Express Client - Basic Configuration	218
8.3.5 Advanced Configuration	220
8.3.6 Web Browser Configuration	226
8.4 Tivoli NetView Management	227
8.4.1 SNMP Installation and Configuration - AIX	227
8.4.2 SNMP Installation and Configuration - Windows NT	228
8.5 Troubleshooting	231

8.5.1 Monitoring Web Express	231
8.5.2 Viewing the Log Files	233
8.5.3 Web Express Traces	235

Part 4. Appendixes	239
Appendix A. System Requirements	241
Appendix B. Special Notices	243
Appendix C. Related Publications	245
C.1 International Technical Support Organization Publications	245
C.2 Redbooks on CD-ROMs	245
C.3 Other Publications	245
How to Get ITSO Redbooks	247
IBM Redbook Fax Order Form	248
Index	249
ITSO Redbook Evaluation	257

Figures

1. eNetwork Wireless Gateway and Client Configuration	5
2. eNetwork Emulator Express Configuration	6
3. eNetwork Web Express	7
4. Putting It All Together.	8
5. Effective Use of eNetwork Express Software.	10
6. Models to Enable Applications for Wireless Mobile Communication	12
7. Mobile Versus Wireless	18
8. The Principle of Cellular Wireless Networks	20
9. DataTAC Network Architecture	23
10. Motorola Private Mobile Radio Architecture	28
11. Mobitex Network Architecture	29
12. CDPD Protocol Architecture.	32
13. Connections over PSTN Networks.	33
14. Modem Pools in Analog Cellular Networks	34
15. Modem Pools in Digital Cellular Networks	38
16. Transition from Digital Cellular Networks to ISDN (Digital) Using UDI.	39
17. Wireless Gateway Connecting to a DataTAC Provider Using an X.25 Network	41
18. Wireless Gateway Connecting to a DataTAC Provider Using a Leased Line .	42
19. Multiplexing Several X.25 Connections over a Single Leased Line	43
20. Selection of Wireless Networks	44
21. eNetwork Wireless Gateway Architecture	45
22. IP Addressing in the eNetwork Wireless Gateway and Client	46
23. Protocol and Encapsulation Hierarchy of eNetwork Wireless	48
24. Retransmission Optimization	50
25. Configuring NUA to the X.25 Connection Interface	65
26. Adding a PSTN Modem Type	69
27. SMITTY Wireless Gateway and Client Mobile Network Interface Panel	80
28. Configuring ARDIS X.25 Adapter Interface	82
29. Configuring Mobitex X.25 Adapter Interface	83
30. Configuring PSTN Parameters on the Mobile Network Interface.	86
31. Applying Modem and Configuring Local PSTN Address	87
32. CDPD Mobile Network Interface Configuration Panel	88
33. Add a Mobile Client Panel	91
34. Configuring ARDIS Gateway and SUI	92
35. Configuring Mobitex Gateway, Local MAN and Remote MAN.	93
36. Configuring PSTN Mobile Network Connection	93
37. Configuring CDPD Client IP Address.	94
38. Changing Current State Field to Start/Stop Mobile Network Interface.	96
39. eNetwork Wireless General Configuration	98
40. The Submap IP Internet.	100
41. Mobile Network Interface Status	102
42. Mobitex Mobile Network Interface Screen Panel	103
43. Mobitex Device Information Panel	104
44. eNetwork Wireless Gateway and Client Configuration	107
45. An Architectural View of the Wireless Client and Gateway Components . . .	108
46. PC Card Status Information	112
47. The eNetwork Wireless Client Connect Window	117
48. General Modem Selection	118
49. Selection of Dial Modems	118
50. COM Port and Speed Selection	119

51. User's Mobile Phone ID Input Field	120
52. Entering the Wireless Gateway Phone Number	120
53. Data Compression and Authentication Options	121
54. Profile Name Field.	121
55. eNetwork Wireless Client Startup Window	122
56. Modem Selection for DataTAC Networks	123
57. DataTAC Specific Settings	123
58. Modem Selection for Mobitex Networks	124
59. Mobitex Specific Settings	125
60. Modem Selection for CDPD Networks	126
61. Mobitex Specific Settings	126
62. The eNetwork Wireless Client Icon in OS/2 Folder.	127
63. The eNetwork Wireless Client Connect Window on OS/2	127
64. Settings Panel for PSTN Connections (Options Tab in Front)	131
65. Settings Panel for CDPD Connections (Toolbar Tab in Front.	132
66. Settings Panel for PSTN Connections (Connection Details Tab in Front) . . .	133
67. Antenna Module and LEDs on the Back.	135
68. Connection Progress.	135
69. Toolbar's Button Information	136
70. Modem Information for CDPD.	137
71. Gateway Information.	138
72. Transmission Statistics for CDPD.	138
73. The eNetwork Wireless Components	142
74. Host Down Error Message	147
75. Gateway Available Error Message	147
76. ARTour Log File (X.25 Problem).	148
77. ARTour Log (X.25 UP)	148
78. The Gateway Down Error Message	149
79. Unknown Modem Error Message	150
80. Invalid Gateway Address Error Message	151
81. Invalid Password Error Message	151
82. Locked Account Error Message	152
83. Showing a Mobile Client Status	152
84. eNetwork Wireless Client Statistics after a Small Packet PING Command . .	154
85. eNetwork Wireless Account File	155
86. Setting the MTU Size of the eNetwork Wireless Interface on Windows 95. . .	161
87. Intranet Access via eNetwork Wireless Gateway	165
88. Using a Firewall to Protect Corporate Intranets	166
89. eNetwork Wireless Gateway Positioned Inside a Firewall	168
90. Gateway Inside a Firewall with Separate Connection to the Wireless Network . .	169
91. eNetwork Wireless Gateway Positioned Outside a Firewall	170
92. eNetwork Emulator Express in a Wireless Network	173
93. Telnet 3270/5250 and Emulator Express	174
94. Emulator Express Server - Basic Configuration	178
95. Emulator Express Server - Advanced Configuration.	179
96. Emulator Express Client - Basic Configuration	190
97. Emulator Express Client - Advanced Settings Configuration	191
98. eNetwork Emulator Express - Sample Scenario	192
99. Emulator Express Server - Sample Configuration	193
100.Emulator Express Client - Configuration	194
101.Emulator Express Client - Host Connection Configuration.	194
102.PCOMM Telnet Client Configuration - Target IP Address	196

103.PCOMM Telnet 3270 Configuration - Port Number	196
104.Monitoring Emulator Express Client	197
105.Monitoring Emulator Express Server	198
106.Monitoring Telnet 3270/5250 Active Ports in CS/NT Server	199
107.Monitoring Telnet 3270/5250 Active Sessions in CS/NT Server	200
108.Emulator Express Client - Log File	201
109.Emulator Express Server - Log File	201
110.Emulator Express Client - Trace File	202
111.Emulator Express Server - Trace File	203
112.Web Express in a Wireless Network	206
113.Web Express Client/Server Components and Connectivity.	207
114.IBM eNetwork Web Express - Sample Scenario	211
115.Web Express Basic Configuration	212
116.Web Express Server - Basic Configuration Summary	212
117.Web Express Server Properties - Addresses Configuration	213
118.Web Express Server Properties - Cache Configuration	214
119.Web Express Server Properties - Logging Configuration	215
120.Web Express Server Properties - Advanced Configuration	216
121.Web Express Server - Sample Trace	216
122.Web Express Server Properties - Options Configuration	217
123.Web Express Client Configuration Profile - Summary	219
124.Web Express Client Properties - IP Addresses and Ports	221
125.Web Express Client Properties - Cache Information	222
126.Web Express Client Properties - Logging Configuration	223
127.Web Express Client Properties - Advanced Configuration	224
128.Web Express Client Properties - Connection Configuration	225
129.Windows NT - SNMP Service Installation	228
130.Windows NT SNMP Properties - Traps Configuration for Web Express	229
131.Web Express Initialization - SNMP Connection	229
132.Tivoli NetView - Event Browser	230
133.Tivoli NetView Event Browser - Web Express Event Details	231
134.Web Express Client - Problems	232
135.Web Express Server - Monitoring	233
136.Web Express Client -Log File	234
137.Web Express Server - Log File	234
138.Web Express Client - Trace File	236
139.Web Express Server - Trace File	237

Tables

1. X.25 Adapter Hardware Settings	61
2. Status of Mobile Devices	101
3. Parent Object Status	101
4. Important Information to Register a Wireless Modem	110
5. Modem Names	146
6. Scalability of the eNetwork Wireless Gateway	164
7. Emulator Express Client - Emulation Sessions Configuration	195
8. Charged by Amount of Data Transferred - Initial Default Values	225
9. Not Charged by Amount of Data Transferred - Initial Default Values	226

Preface

This redbook helps you to understand the functionality included in the latest releases of the IBM eNetwork Wireless Gateway and Client, IBM eNetwork Emulator Express and IBM eNetwork Web Express products.

It focuses on the architectures and technologies implemented in these products, and helps you plan, install, and configure the new functions quickly in a wide variety of environments. In this redbook you will find information on the installation and configuration of the eNetwork Wireless and eNetwork Express family of products.

You will also find numerous configuration examples showing ways to set up the wireless gateway and client stations when connected to wireless networks (such as DataTAC, Mobitex, GSM, AMPS). This includes IP-based networks (for example Cellular Digital Packed Data or CDPD), and dial networks.

A basic knowledge of networking concepts and terminology used in wireless communications and TCP/IP is assumed.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Raleigh Center.

Juan R. Rodriguez is a networking professional at the IBM ITSO Center, Raleigh. He received his M.S. degree in Computer Science from Iowa State University, writes extensively and teaches IBM classes worldwide on areas such as networking and data security. Before joining the IBM ITSO, he worked at the IBM laboratory in Research Triangle Park (North Carolina, USA) as a designer and developer of networking products.

Werner Schollenberger is a Technical Consultant at IBM Global Service in Heidelberg, Germany. With ten years of experience in the networking field he has worked in customer and research projects dealing with mobile data communication, for the last three years. His areas of expertise include TCP/IP, Communication Architectures and Protocols, Wireless Data Networks, Remote Access, and Traffic Telematics. He is a member of the team that initially developed the eNetwork Wireless Gateway and Client Software.

Muchsin Anzib is an Advisory Networking Specialist in IBM Indonesia. He has 9 years experience in IBM handling PC, AS/400, OS/2, Windows NT, Communications Servers and Networking Products. He provides network design, installation and post-sale services for IBM customers.

Bhaktianto Widyorso is an AS/400 System Software Specialist with IBM Indonesia. He has 9 years working with IBM. He has 6 years of experience in the area of network management and installation. His expertise has been in network and system management on the Midrange platform (OS/400 and AIX). He is currently involved in delivering networking services to IBM customers in his country.

Thanks to the following people for their invaluable contributions to this project:

George Hall, John Kari, Henry Welborn, Jim Rutledge
IBM Research Triangle Park, North Carolina, USA

Reed Bittinger, Ian Shields, Charles Le Vay, Ivan Heninger
IBM Research Triangle Park, North Carolina, USA

Shawn Walsh
IBM International Technical Support Organization, Raleigh Center

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in "ITSO Redbook Evaluation" on page 257 to the fax number shown on the form.
- Use the online evaluation form found at <http://www.redbooks.ibm.com>
- Send your comments in an Internet note to redbook@us.ibm.com

Part 1. Introduction

The chapters in this part of the redbook give you a brief overview of the eNetwork Wireless Software product family. It provides general technical information that relates to the eNetwork Wireless Gateway and Client, the eNetwork Emulator Express and the eNetwork Web Express products.

Chapter 1. Introduction

Wireless communication technology, in combination with portable and mobile computers, notebooks, like ThinkPads, presents an awesome opportunity for unprecedented access to information and applications by mobile workers and professionals. Yet the limited bandwidth, high latency, high cost, poor reliability and security risks of wireless networks greatly inhibit supporting today's applications over wireless networks. eNetwork Wireless and Express Software significantly reduce the amount of data and latency of wireless communications by performing protocol reduction, data compression, filtering, and intelligent caching, while providing authentication and encryption for secure communications.

eNetwork Wireless Software is a family of products that enables immediate and optimized mobile communications for customers, allowing them to use their existing applications unchanged across wireless and wired networks. In addition, eNetwork Wireless Software enables new mobile applications to be developed to industry standards (application programming interfaces and protocols) for mobile environments.

The following three sections describe briefly the eNetwork Wireless Software components, which are:

- eNetwork Wireless Gateway and Client
- eNetwork Emulator Express
- eNetwork Web Express

Each of the three components can be used independently, but there is a significant performance boost when the wireless communication platform is combined with Express products. eNetwork Wireless Gateway and Client enable and speed up wireless communication, while Emulator and Web Express do a good job in reducing the amount of data to be transmitted over the air.

In this chapter, we:

- Briefly describe these products individually.
- Show, how these components fit together to build an integrated solution for mobile communication.
- Explain the various abstraction layers, which should be kept in mind when you deal with this rather complex type of installation.
- Give you some general hints to decide whether the user gains a significant performance advantage by using eNetwork Emulator Express and Web Express in certain situations.
- Discuss the basic models for optimizing TCP/IP-based applications and explain the key points as to why applications deployed in a mobile environment may sometimes be inherently slow, leading to a considerable communication overhead.

This redbook assumes that you have read the program documentation including the Technical Overview carefully and understand the underlying concepts. This book provides various background information that will help when you install, configure, and operate the eNetwork Wireless Software. By understanding how

the wireless networks interface with eNetwork Wireless Software, which is described in Chapter 2, you will be able to set the various parameters according to your environment for optimum performance. Chapters 3 and 4 can be used as a *cookbook*, since they document how we installed and configured the eNetwork Wireless Software. Chapter 5 gives you some troubleshooting hints and Chapter 6 helps you to operate an eNetwork Wireless configuration giving you tips on performance and network security issues. Chapter 7 covers the eNetwork Emulator Express Software again in the form of a cookbook while Chapter 8 addresses eNetwork Web Express.

You as the reader of this redbook, are assumed to have the following background knowledge:

- You understand the TCP/IP concepts and are able to configure a wireline IP network correctly.
- If installing the AIX-based products, you have sufficient AIX skills to install and configure software and device drivers using **smitty** or **smit** and to work with the command shell.
- If you are about to configure DataTAC or Mobitex wireless networks, you have sufficient X.25 skills or at least have someone at hand when you run into X.25 connectivity problems.
- You understand how the TCP/IP stack interfaces the operating systems you use as eNetwork Wireless Clients. You know the commands and utilities to check TCP/IP status and other parameters.

For the eNetwork Wireless Software product documentation, see Appendix C.3, "Other Publications" on page 245.

1.1 eNetwork Wireless Gateway and Client

The eNetwork Wireless Gateway is a software component for mobile computing that integrates data access from multiple data packet radio, cellular and wireline networks to enterprise LAN and WAN networks. Mobile workers with the eNetwork Wireless Client (Windows 3.1/3.11, Windows 95/98, Windows NT and OS/2 platforms) can be linked to the same eNetwork Wireless Gateway, regardless of the wireless network they use. Thus, all members of a mobile workforce may access the same applications and/or services as in a LAN environment. Working with TCP/IP products the eNetwork Wireless Client provides the functionality to access existing or newly developed IP applications. eNetwork Wireless Gateway and Client not only can be used for extending enterprise networks to the wireless world, but can also be used by carriers and service companies to allow them to offer wireless IP extensions to their customers.

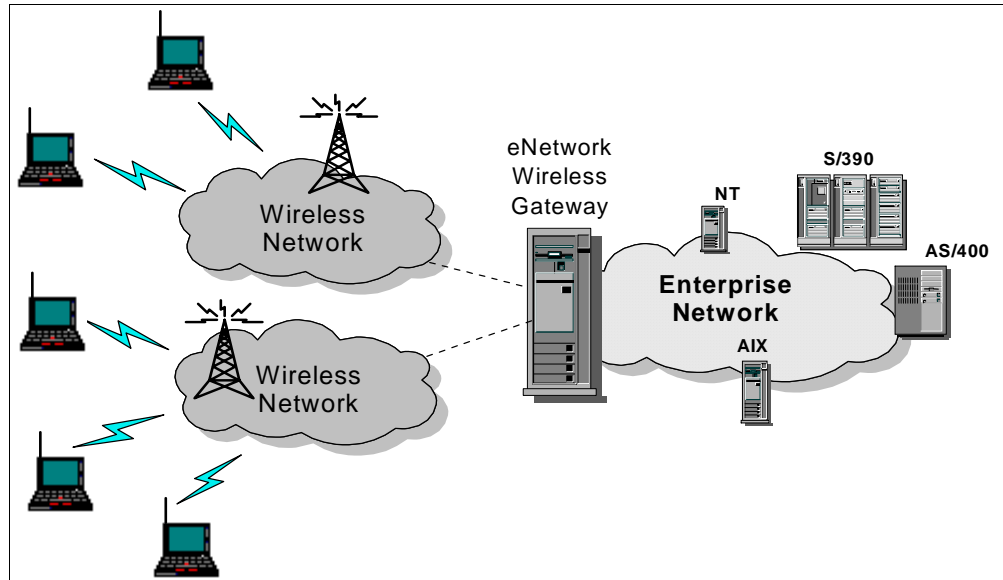


Figure 1. eNetwork Wireless Gateway and Client Configuration

The eNetwork Wireless Gateway and Client enable existing TCP/IP applications to have access to intranets or the Internet over wireless networks. As shown in Figure 1 on page 5, the Wireless Gateway may be connected to several wireless networks simultaneously. This gives the mobile user the choice to select the wireless network according to coverage and bandwidth requirements.

1.2 eNetwork Emulator Express

eNetwork Emulator Express significantly improves the access to mainframe and AS/400 applications over wireless or low-bandwidth networks and consists of a server and client software component. In order to provide efficient access for mobile computers using IP protocols over wireless or dial-up connections, they intercept the Telnet 3270 or Telnet 5250 sessions between the existing mainframe and AS/400 applications and the terminal emulators on the client side.

The eNetwork Emulator Express Client does not have any function to display 3270/5250 sessions. This is accomplished by a terminal emulator such as *eNetwork Personal Communicator (PCOMM)* or *Host On-Demand (HOD)*. So everything you can do over Telnet 3270/5250 with your emulator, you can do using eNetwork Emulator Express. This is true even if the emulator is Java-based and/or has an application-specific graphical user interface.

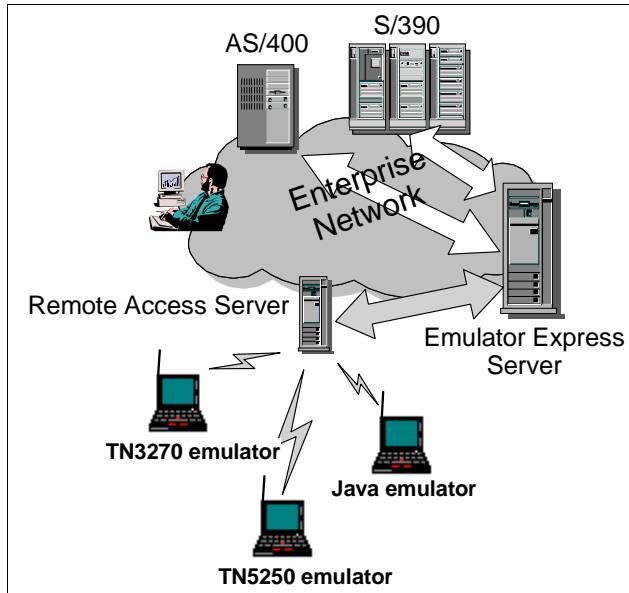


Figure 2. eNetwork Emulator Express Configuration

The basic idea of eNetwork Emulator Express is that in the *screen-oriented* host environment the amount of data to be transferred over the radio network can substantially be reduced if both mobile and stationary hosts cache portions of the screens already transmitted in memory and exchange only the different portions when the screen is updated. eNetwork Emulator Express also provides for immediate application access with no changes to applications or new code development by the customer. eNetwork Emulator Express was developed to support existing operational applications on IBM mainframe and AS/400 host systems efficiently over radio networks. The client component resides on the mobile device; the server component runs on a system at the customer location. The server component communicates with the IBM host through SNA protocols and passes the transmission to the mobile unit through the IP protocol.

Figure 2 on page 6 shows an eNetwork Emulator Express configuration. Note that the Emulator Express Server and Client communicate over any TCP/IP platform supported by the operating system. So the Remote Access Server in Figure 2 can be an eNetwork Wireless Gateway but also any other IP access router. If the mobile clients communicate over a wireless network that is not enabled for IP, then eNetwork Wireless Gateway and Client is required. Moreover, security and performance issues strongly indicate the need for the use of eNetwork Wireless Gateway and Client even if the wireless network is already IP-enabled. Examples for these kinds of networks are Cellular Digital Packet Data (CDPD) and wireless or wireline connections to the Public Switched Telephone Network (PSTN).

1.3 eNetwork Web Express

eNetwork Web Express consists of server and client software components as well. eNetwork Web Express will enable customers to run any Web browser to access any Web server without imposing any changes to either, but it significantly reduces the amount of data transmitted. The eNetwork Web Express client appears as a local Web proxy that is co-resident with the Web browser and communicates with it using a local TCP/IP connection and the HTTP protocol.

When the browser makes requests to access information on a Web site, the Web Express Client and Server enable the optimized exchange of information (HTML, GIF and CGI responses) across wireless and wireline networks using intelligent caching, protocol reduction, header reduction, and data compression. In addition, Web Express also supports foreground and background queuing of browser requests and disconnected operations. This enhances the productivity of the mobile worker by allowing him or her to browse through preloaded information while being disconnected and to request information that will be automatically retrieved, when he or she reconnects. Once requests are queued, mobile workers can adjust the priority of requests.

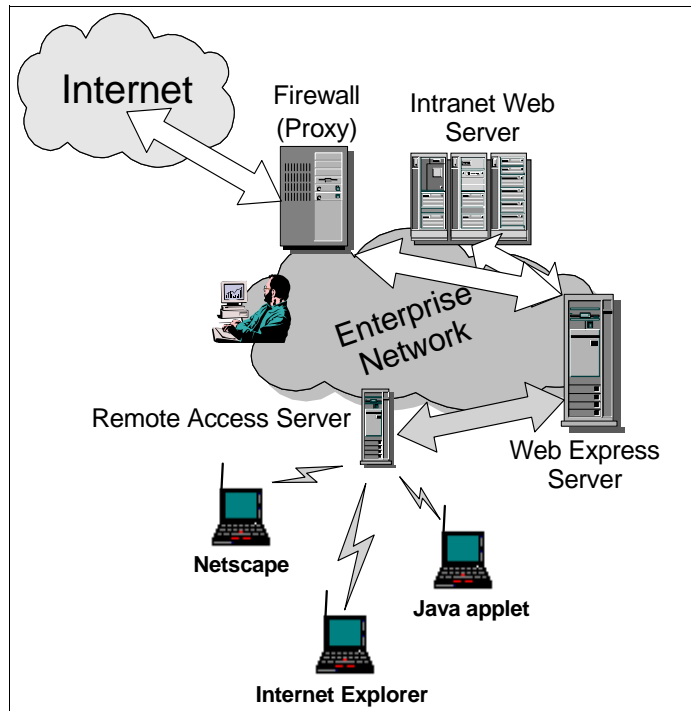


Figure 3. eNetwork Web Express

The client component (Windows 95 and Windows NT) resides on the mobile device. The Web Express Server component (Windows/NT and AIX platforms), which usually resides on a system at the customer location, communicates with the Web servers using TCP/IP and HTTP protocols. Instead of communicating with the Web servers directly, the Web Express Server can also connect to an HTTP proxy server. The Web Express Server passes the Web traffic to the mobile unit across a single persistent TCP/IP connection. This traffic is compressed and optionally without graphics, regardless to the settings in the Web browser.

The Web Express Server and Client communicate over every communication platform that supports TCP/IP. If the wireless network to be used is not enabled for IP, then the eNetwork Wireless Gateway and Client or an alternate platform are required. However, similar to eNetwork Emulator Express, security and performance reasons may strongly indicate the need for the use of eNetwork Wireless Gateway and Client even if the wireless network is IP-enabled, such as CDPD or PSTN dial-up access.

Although the Web Express Client works together most efficiently with the Web Express Server, it can also be configured to access an HTTP proxy server or a Web server directly. In that case there will be a significant performance improvement with the Web Express Client across wireless networks or networks with relatively small bandwidth per user.

1.4 Putting It All Together

As stated in the preceding sections, the eNetwork Wireless communication platform is structured into a client and a gateway component, while for the Express software the clients talk to an application-specific Express server.

Figure 4 on page 8 depicts a typical mobile solution. It shows how the software products covered in this redbook work together to provide remote access to host applications and information in the World Wide Web.

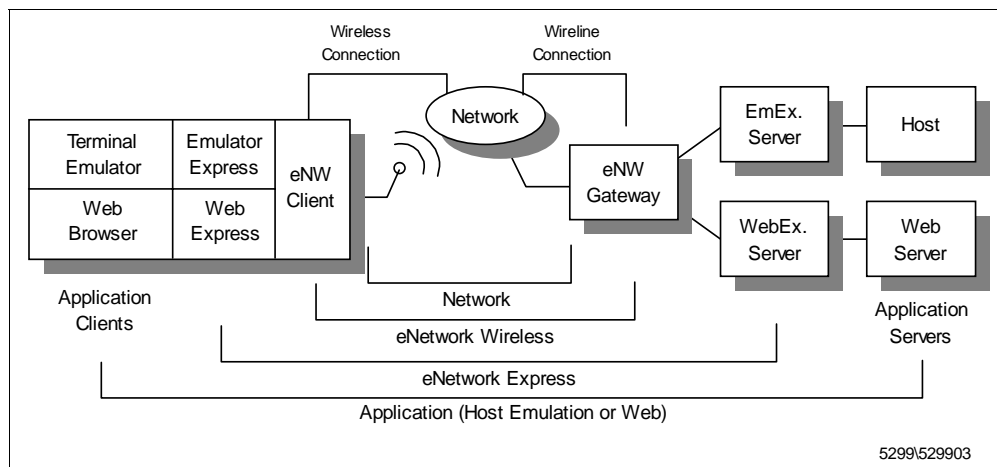


Figure 4. Putting It All Together

An interconnection between a mobile, wireless device and a wireline device usually has two parts. The wireless connection between the radio modem and the wireless network and the wireline connection between the transition point and the wireline device. From the point of view of the eNetwork Wireless software, these two parts disappear in the cloud of the wireless network, but the interfaces at the end points on both sides are totally different.

Note

While it may be technically possible to connect the eNetwork Wireless Gateway to a wireless network via a normal radio modem, it is strongly recommended not to do this. Every packet exchanged between the mobile client and the gateway would have to be transmitted over the air two times and would soon congest the wireless network.

A mobile solution has several peer-to-peer relations, which have to be paid attention to. These relations build a layered structure. The network layer comprises the basic communication functions that are covered by the wireless network service provider. It includes the radio modems, the wireless connection,

the transition to the wireline world, and the wireline connection to the eNetwork Wireless Gateway. eNetwork Wireless can be regarded as another layer, which is based upon this network layer and allows application programs on the mobile computer to connect to applications in the intranet or Internet for the exchange of data using standard TCP/IP interfaces and protocols.

On the application layer, the most important programs on the mobile side are terminal emulators such as *eNetwork Personal Communicator* (PCOMM) and Web browsers such as *Netscape* or *Microsoft Internet Explorer*. They actually act as application clients. Their counterparts are the application servers, the host computers and Web servers in the wireline network. To optimize the communication for wireless networks, the Express clients and servers intercept this communication relation. This creates a layer between the eNetwork Wireless layer and the application layer, the eNetwork Express layer.

1.5 When Express Software Can Be Used Efficiently

The interception of the client/server communication for Web browsing or host terminal emulation with Emulator Express or Web Express is truly optional from a functional point of view. However, it usually leads to dramatic performance improvement in mobile, wireless environments. In some cases, it even makes sense to use the Express software, when the client has a wireline connection to its IP network. However there are situations where the products of the Express family might lead to performance degradation and therefore to customer dissatisfaction. This discussion applies to both, the eNetwork Emulator Express and eNetwork Web Express.

Disregarding the memory and processing power, which have to be provided when employing the Express software, there is a trade-off between the reduction of the amount of data to be transferred between the Express clients and the server and the processing delays on both sides.

To measure the benefit of employing Express software, there are two options. The first one is to regard the transmission delays on the application level. In this case you have to compare the transaction or information retrieval times when the client is located close to the server application and when the client is connected remotely. You then look at the differences with and without the Express software.

The second is communication costs. You then have to evaluate whether the savings are worth the investment in the Express software. Both measures may correlate. This is the case in most packet and connection-oriented wireless networks. On packet-oriented wireless networks, where the user is charged by data volume, the more packets that have to be transmitted, the higher the communication costs. Since bandwidth is limited, the more data that has to be transferred, the longer the user will have to wait to get his or her results. Connection-oriented networks usually charge their customers by air time and therefore transmission delays have a direct impact on the cost.

But even on a leased line connection where several clients are connected to a server, reducing the amount of data to be transmitted lets you put more clients on that line and as a consequence reduce communication costs per client.

So, if you are short of bandwidth on the client's connection to the rest of the network or if the amount of data transferred is directly correlated with costs, then

the question is not whether the Express family will help you or not. It will help you in any case. But you still have to decide where to place the Express server. Note that response times are not only a matter of communication bandwidth but also a matter of processing times on the application and Express servers.

A general statement can be made that the Express family is of highest value when one of the following relations are true:

- The communication delays between the Express client and Express server are significantly longer than between the Express server and the application server. In this calculation the processing times on the application server have to be taken into account.
- The costs per byte transmitted between the Express client and Express server are significantly higher than between the Express server and the application.

These relations are depicted in Figure 5 on page 10.

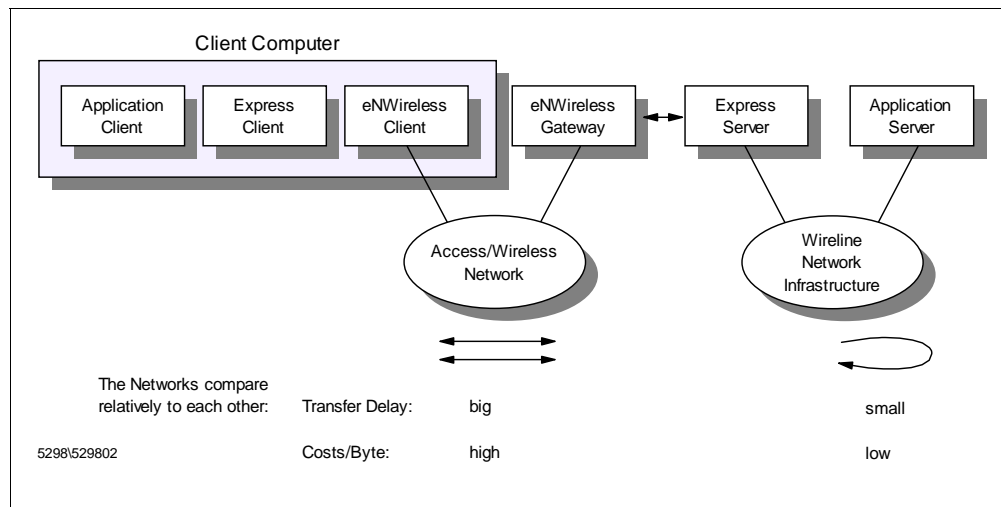


Figure 5. Effective Use of eNetwork Express Software

It is the difference in the speed and/or cost of the connection on either side of the Express Server which determines the effectiveness of the solution.

1.6 Optimizing Other TCP/IP-Based Applications

When you try to use client/server applications over wireless mobile networks, you will have to deal with the fact that radio networks usually have much less bandwidth and a higher latency than local or wide area networks and are more error prone.

The basic design goal of TCP/IP and the Internet was to enable many users to share a big networking infrastructure with reasonable transport capabilities. It is true that the TCP/IP protocol has been designed to cope with little bandwidth per user or per TCP/IP connection, but TCP/IP always assumes that packets are transmitted independently. So TCP/IP works over narrowband wireless links in principle but does not perform well, especially when several TCP connections are active over a wireless link.

TCP/IP does not expect that a long packet just sent would cause the following packet to be delayed significantly. It assumes that packet losses occur due to congestion in some intermediate devices such as an IP router and not due to link transmission errors. This leads to a considerable performance decrease on higher transmission error rates.

eNetwork Wireless Gateway and Client optimize IP communication near to the highest possible degree without sacrificing the end-to-end protocols of the TCP/IP connections. While the eNetwork Wireless software reduces unnecessary retransmissions as far as possible, a reduction of the actual data transmitted over the air can be performed much more efficiently at the application protocol level. On the other hand, existing applications typically used over an intranet or Internet are not aware that they are communicating over wireless networks. Some applications even fail when they experience high communication delays. Others are very chatty and produce an huge overhead by wrapping small pieces of data into single TCP/IP packets.

Figure 6 on page 12 shows three models to enable client/server applications for mobile wireless communication.

The simplest configuration is to leave the peer-to-peer connection between the application client and the application server intact. Place the client on the mobile device and connect it via eNetwork Wireless Gateway and Client and a wireless network to the server in the wireline network.

Many applications may run this way. Note that in most of the cases, if an application fails to run over eNetwork Wireless, it is the application that drops the connection because it thinks there is some network problem. You may possibly be able to configure higher timeout values to solve some of these problems. The TCP/IP protocol adapts easily to the transmission characteristics of the wireless networks, as long as there is not too much simultaneous but independent communication activity. However on low-bandwidth, high-latency, and high-error rate wireless networks, the application response time which may be seconds on a LAN, may easily turn into minutes on wireless networks.

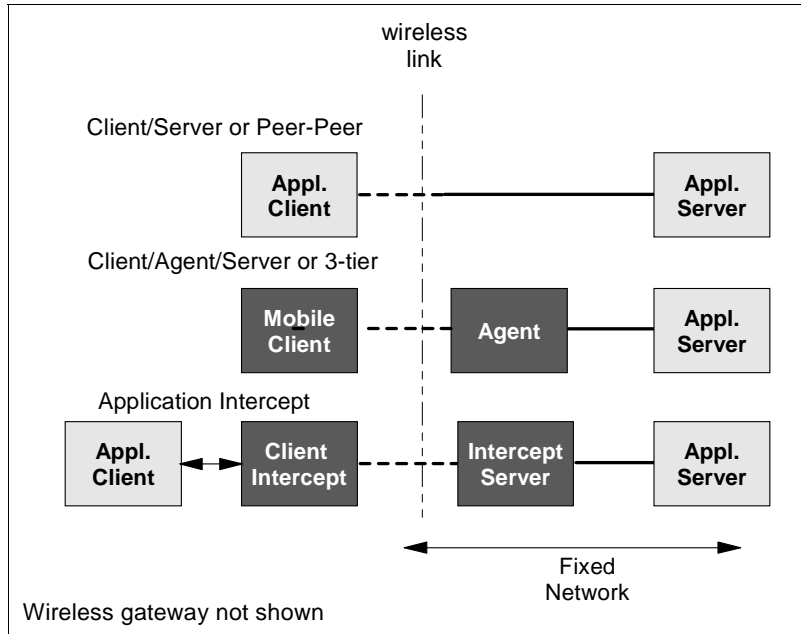


Figure 6. Models to Enable Applications for Wireless Mobile Communication

The second model, the client/agent/server model or 3-tier model, may be best in terms of data reduction but has the considerable disadvantage of being application-specific. In this model, a special mobile client communicates with an agent in the fixed network over the wireless link. The mobile client and the agent have to be implemented specifically for this application. The agent acts as an application client to the application server but transfers the user interface to the mobile client.

The client functionality resides on the agent in most cases. The mobile client acts as some kind of application-specific terminal. In this solution only the information that is absolutely essential to the mobile user must be transferred and all known reduction and caching mechanisms can be implemented. However, a new user interface has to be implemented and this is usually a lot of work. The user has to deal with two different user interfaces when he or she is connected to wireline or wireless networks. Additionally, new features of upcoming versions of the application client require changes to the mobile client and the agent.

The third model, the application intercept model, leaves the application client and server untouched. It is basically a client/proxy/server model where the proxy is in two parts: the intercept client and the intercept server. The intercept client, being located on the mobile device, pretends to be the application server, while the intercept server acts in the role of an application client.

The intercept client and server are specific to a particular application type or protocol. They must fully understand the protocol in order to eliminate unnecessary or redundant data. The same as in the second model, all known compression and caching techniques can be implemented in the communication between the intercept client and server. But the data reduction is limited to a degree, in that the receiving intercept component can fully reconstruct the packet originally sent. That is why with the intercept model data reduction cannot go so far as the 3-tier model. The great advantage, however, is that the application can

be left unmodified. If the application protocol changes in a further version, the intercept components are able to pass-through the packets they cannot interpret. This allows them to continue to support application features they haven't been designed for. Of course some of the optimization techniques will be sacrificed in this case.

Note

Applications heavily using Remote Procedure Call (RPC) usually do not perform very well in low-bandwidth/high latency networks such as wireless networks.

Part 2. eNetwork Wireless Gateway and Client

In this part of the redbook you will find information that is useful for understanding the architecture implemented in eNetwork Wireless Gateway and Client products. A technical overview is presented which includes a description of the wireless mobile network technologies such as DataTAC, Motorola Private Mobile Radio (PMR), Mobitex, Cellular Digital Packet Data (CDPD), PSTN, Analog Cellular Phone Systems (AMPS), GSM (PCS) and Dataradio.

Other chapters provide, in detail, the installation, configuration and management of eNetwork Wireless Gateway and Client products. You will also find a chapter dedicated to problem determination and the last chapter in this part of the redbook explains some performance considerations as well as a few security issues related to wireless networks.

Chapter 2. Technical Basics of Wireless Communication

When you configure the eNetwork Wireless Gateway you will have to know something about the wireless networks the gateway will be attached to. Especially important are the addressing mechanisms and schemes and the way the gateway connects to the wireless network providers, which means the wireline part of the radio network. While the *eNetwork Wireless Technical Overview* (GC31-8630) describes how the wireless networks are constructed, we put the focus on the aspects relevant to the eNetwork Wireless components, the gateway and the client.

Before we go into detail about the wireless technologies, we point out the differences between wireline, mobile, and wireless. After discussing the different wireless networks, we describe the functions of the eNetwork Wireless Gateway and Client and how they work.

2.1 Mobile versus Wireless

What people mean when they talk about mobile computing often differs significantly. In order to have meaningful conversations about mobility as a topic or trend, there are some key distinctions to be established and applied to current and foreseen technologies and equipment. Mobility can be contrasted with stationary. Wired communications can be contrasted with wireless communications. Connected operations can be contrasted with disconnected operations. These six terms are attributes that can be applied to a computer device. Definitions of each term follow to provide a common ground for discussions:

Stationary	As used here means that the device's location is permanent.
Mobile	Means that the device's location may change. It is portable.
Connected	Means that the device is connected to a network or computing system, so that data exchange can take place. This should not be confused with connectionless or connection-oriented transport technologies. Connected in this sense simply means that data exchange can take place at any time. This implies that some kind of session is active.
Disconnected	Means that there is no established connection or session of any type between the device and a network or computing system. No immediate communication is possible.

The following two terms imply that the device is connected:

Wired	Means that the device is connected to the network or a computing system by some type of wired connection, for example a channel, a LAN, or a plain old telephone connection.
Wireless	Means that the device accesses the network or computing system over the air, using a radio transmission technology. Examples are cellular wireless networks. They may use exclusive connections like Global System for Mobile communications (GSM) or shared media access like packet

radio. Other wireless connections are, for example, infrared links and wireless LANs.

These terms span over a three dimensional space, which is depicted in Figure 7 on page 18. In this space, with different combinations of attributes, a device can be located. In many instances a device can occupy different locations at different times.

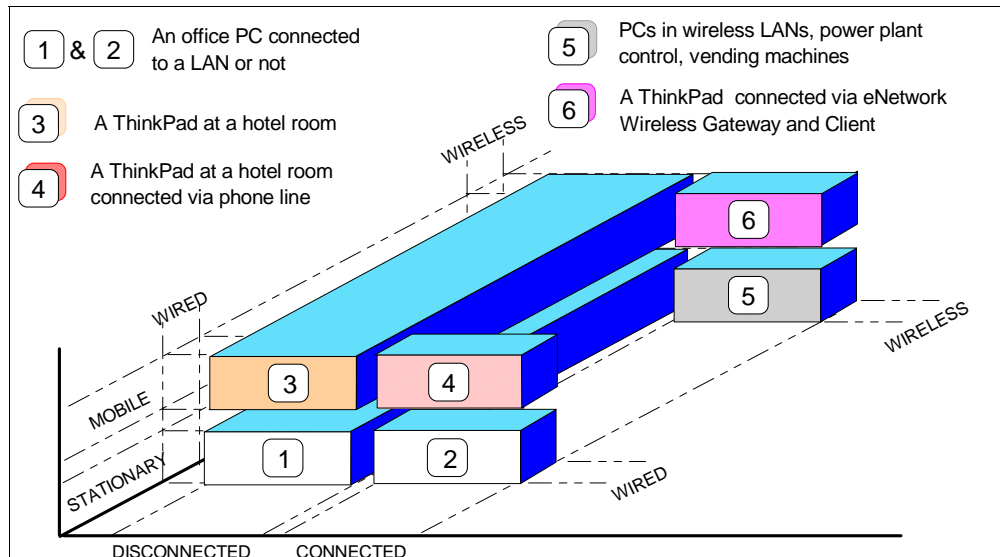


Figure 7. Mobile Versus Wireless

These six locations refer to modes of operation a device can have in this context and, with examples, they can be listed as follows:

1. Stationary and disconnected: In this state, the significance of wired or wireless is meaningless. This is the configuration that spawned the industry: one computer with one co-located user.
2. Stationary, wired and connected: This state includes the traditional 3270 environment, computers on a LAN, etc. The devices are connected by some type of wired connection, and are not moveable or portable. All office PCs belong to this state.
3. Mobile and disconnected: An example for this state is a Lotus Notes user having his or her databases replicated to the local drive of a notebook while connected. Then he or she can sit with his or her notebook and review the data at his or her leisure and convenience. Once the review is complete, he or she may then connect and replicate the changes back to the server (thus leaving the disconnected state). This is an example of a device that can at different times operate in different states.
4. Mobile, wired and connected: One example is the Lotus Notes notebook from the example above dialing in via a PSTN connection from a hotel room to connect to the server for replication. However, another kind of scenario exists, where a notebook connects to a LAN in a foreign location using mobile IP.

Note

Mobile IP is not covered in this redbook.

5. Stationary, wireless and connected: The most important example for this state is a computer connected to the network via a wireless LAN, since the location is restricted to a specific area. Other examples here could be telemetry uses such as power plants, railway yard control, and remotely monitored vending machines. These devices can be everywhere but they don't move.
6. Mobile, wireless and connected: eNetwork Wireless Gateway and Client is actually the solution aimed at this scenario. A notebook connects from anywhere to the network or computer system using a wireless network. The application requires an online connection.

2.2 Wireless Mobile Network Technologies

The basic components of wireless data communication that provide simple peer-to-peer communication are:

- Mobile wireless transmitter and receiver (radio modems)
- A base station

A base station controls the frequency band, which can be divided up into several channels. From the perspective in this book, it doesn't matter whether these channels are in frequency multiplex, time division multiplex, or code division multiplex. The base station transmits with more power and has a more sensitive receiver than the radio modems. Therefore, a modem is able to communicate with a base station from a farther distance than with other radio modems. A radio link protocol must be in place, which prevents the modems from introducing transmission errors due to access collisions on the radio channels. An introduction to the various modulation, multiplex and media access techniques can be found in the redbook *An Introduction to Wireless Technology*, SG24-4465-01.

To build wireless communication networks covering a large geographical area and being capable of allowing access to a huge number of subscribers, one base station isn't sufficient. In cellular radio networks, the area covered by one base station is reduced and other base stations are positioned in a way that there is only a small area where there is coverage by more than one base station. Adjacent cells have to use different frequency ranges but apart from that, the same frequency can be reused. This is shown in Figure 8 on page 20. Since a base station only has a limited number of radio channels available, the more base stations that cover a specific area, the more subscribers can be active in this area.

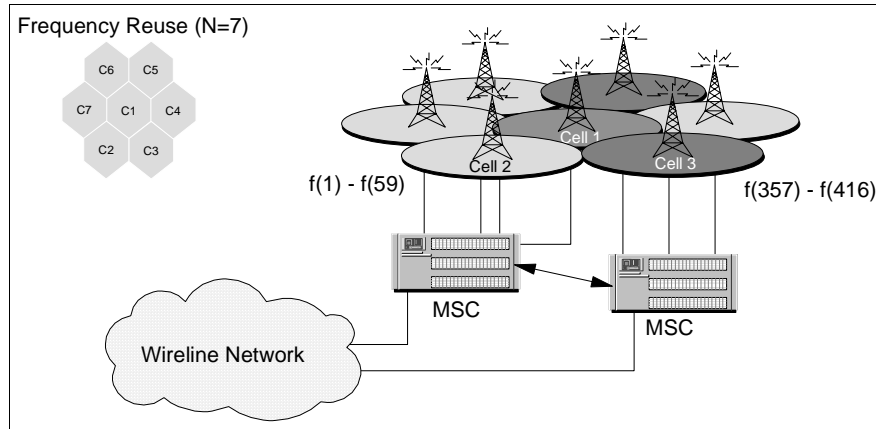


Figure 8. The Principle of Cellular Wireless Networks

The base stations are interconnected via wireline links and mobile switching centers¹ (MSC). The MSCs must also coordinate the frequencies used by the different mobile users and cell transmitters.

Mobile users want to move from one cell to another without interrupting the communication. This takeover process is called a *handoff* and is also handled by the MSC.

When a cellular mobile device is switched on, it will scan a predetermined set of radio channels to find a base station with which it can communicate. If it has found one, the modem is said to be *in coverage*. Now, it checks to which network provider this station belongs, whether it is registered there and whether the network provider grants access. The modem identifies itself with a unique address. In some networks this ID acts as a network address, while in others the network address is assigned by the network provider. When the modem has access to the cellular network, it is said to be *registered* or *signed on*. When a modem is signed on, the network provider knows the cell where it popped up, so all traffic to this device can be directed to the correct cell.

If there are different providers, to which the modem has coverage, the user has to select a provider before the modem can register.

It may happen that a radio modem powers up in a region where there is a wireless network using the same technology, but belongs to a network provider where the device is not registered. It may be that this provider has a contract with the other provider to allow each other access to their network infrastructure. This contract is called a *roaming agreement*. When a radio modem pops up in a wireless network, where there is a roaming agreement, the *hosting network* provider recognizes this and checks with the *homing network* provider whether access may be granted or not. If everything is fine, the radio modem is allowed to sign on and may now exchange data with other devices in the hosting and in the homing network. A message is sent to the homing network, so that if someone directs data to the roaming mobile device, the data is automatically transferred to the hosting network. The roaming contract covers interoperability issues as well as accounting regulations.

¹ The term MSC is taken from the terminology of GSM networks. However, this function exists in any cellular radio network even if it is named differently.

To allow mobile users to communicate with users or applications attached to wireline networks, the wireless network provider has to install some interworking functionality which acts as a transition point between wireless and wireline communication. There are transitions to:

- Analog or digital telephone networks (connection oriented)
- X.25 networks (packet oriented)
- TCP/IP networks (Internet)

Some wireless network providers route data streams directly by converting the protocols and addressing schemes, if necessary. In that case, both, the mobile and the wireline devices may use their native protocols. For example, an X.25 node sends an X.25 packet, which will be received on the mobile side as a message and vice versa. Other wireless networks follow the concept of integrating wireline nodes into their mobile network, making them appear as mobile devices and addressing them as mobile devices. The wireline nodes then have to implement special protocols to allow them to connect to the wireless network.

Radio modems are usually external devices connected to a serial port or have the shape of a PC card (formerly PCMCIA) which can be plugged into a notebook and emulate a serial port to the operating system. The protocols over this serial communication may differ widely. Some radio modems behave as regular Hayes-compatible modems, some come with a driver to act as a networking device such as token-ring or Ethernet card, and others have a totally proprietary interface. If the radio network does not convert the radio transmission protocols to some wireline standard, the protocol, which has to be implemented in the wireline node is also proprietary.

Cellular radio modems or phones are assigned a hardware identification number and a mobile phone number or mobile ID. The hardware identification number is known as the *electronic serial number* (ESN) or *Electronic ID* (EID) and is assigned to the phone at manufacture time. In some cases the mobile ID is on a smart card or SIM card which must be inserted into the modem before powering it on. There are more details about identifying and addressing the different types of radio modems in the following sections.

2.2.1 DataTAC

DataTAC is a radio packet data network technology developed by Motorola. Its network architecture is depicted in Figure 9 on page 23. Public network operators have deployed this technology to offer shared wireless data communications services to a broad base of customers. These services range from fleet management and dispatching for field service organizations to e-mail and database access for mobile professionals.

DataTAC networks offer transmission rates from 4.8 kbps up to 19.2 kbps depending what technology the wireless network provider implements. For example, in the U.S. America Mobile operates the ARDIS network which works with 19.2 kbps channel bit rate, Modacom, which is the DataTAC network in Germany offers 9.6 kbps. DataTAC networks operate at frequencies in the 400 or 800 MHz range, depending on the geography.

Note

Due to the wireless protocol overhead, the effective data rates are lower than the channel bit rates.

There are three variants:

- DataTAC 4000 - Used in the U.S. provided by America Mobile and called ARDIS.
- DataTAC 5000 - Common in the Southeast Asia Pacific area where it is simply called DataTAC.
- DataTAC 6000 - Used in Europe, notably in Germany where it is known as Modacom.

The differences include radio frequency and device compatibility. There are also some slight differences in the lower protocol used between the DataTAC network provider and the station attached via wireline connections. That is why in the eNetwork Wireless Gateway there are different radio network types defined for DataTAC networks, called ARDIS, DataTAC and Modacom.

As in many of the packet radio networks, all DataTAC subscriber units within one radio cell share one communication channel (shared media access). This channel is divided into uplink and a downlink subchannels. In order to send a packet, the radio modem first must get access to the uplink subchannel. The downlink subchannel is entirely controlled by the base station. In DataTAC, the radio link access protocol Radio Data-Link Access Procedure (RD-LAP) specifies how the radio modems communicate with the base station, so that every radio modem is treated fairly. In some cases, the older protocol Mobile Data Communications (MDC) may still be in use.

You may experience that traffic directed to the mobile device is privileged over traffic in the opposite direction. This is because the radio modem has to wait until it receives a token for transmission and the base station will not give this token as long as it has something to send to this device. So be patient when you are using the eNetwork Wireless Client and it is receiving a lot of packets.

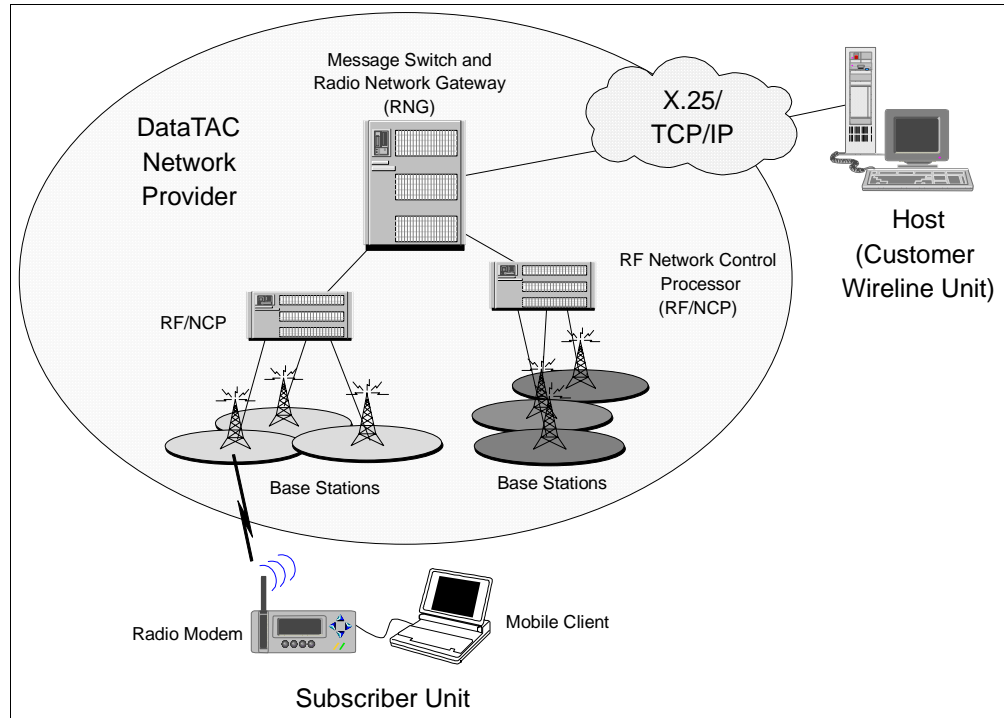


Figure 9. DataTac Network Architecture

DataTAC is a message-oriented wireless network. A message can be up to 2048 bytes. Before it is transmitted over the air this message is fragmented by the sender. Upon receipt the fragments are reassembled by the receiver. Fragmentation and reassembly is handled within the radio modem and the DataTAC network, so none of the applications on either side are affected by this. Messages sent by the subscriber units pass the RF/NCP and are transferred to the message switch where they are stored before they are routed to the corresponding destination. If the destination is not reachable, this message may be stored in the network for quite a long time.

Because the message switch also handles the transfer of messages between the DataTAC network and external applications, this component is also called the radio network gateway (RNG).

The network nodes in the wireline network are called *hosts*. This is because in DataTAC networks, they originally were mainframe computers and may still be in some applications. DataTAC supports a variety of protocols between the RNG and the hosts. They include:

- SNA LU6.2
- SNA3270 terminal emulation and bisynchronous 3270
- X.25
- TCP/IP
- Bisynchronous point-to-pont
- Asynchronous

Note

The protocols mentioned above are only for the communication between the host and the RNG. They allow you to exchange simple messages with a mobile device. Therefore, a middleware platform like eNetwork Wireless is required to provide for Internet access.

Additionally, DataTAC supports the following two routing methods:

- Fixed routing
- Standard context routing (SCR)

The eNetwork Wireless Gateway only supports X.25 and TCP/IP access to the RNG and only standard context routing. We describe these to prepare you for questions that may be asked by your network provider.

With fixed routing some DataTAC providers, namely the German Modacom network, offer services, such as:

- Messaging (mobile-to-mobile only).
- X.25 mobile originated. The subscriber unit is able to establish a connection to an arbitrary X.25 host and therefore, data transfer can then be in both directions.
- X.25 mobile terminated. The subscriber unit listens for a connection to be established by an X.25 host in the wireline network. Data transfer can then be in both directions.

SCR, as the name implies, relies on the context of the data message to determine the destination subscriber unit address. SCR is a specialized protocol designed by Motorola for communications and management control of wireless data subscriber devices. It enables a control of data message delivery characteristics to a high degree. SCR allows a host to address a virtually unlimited number of devices using a single host link, for example, a single X.25 or TCP connection to the RNG. SCR does not support communication between two hosts or between mobile devices. This is why the service based on this routing concept is often called fleet connectivity.

When you request this service type from your DataTAC network provider (which you should do to build an eNetwork Wireless solution over DataTAC), it requires the host to talk to the SCR protocol with the RNG. The eNetwork Wireless Gateway actually does. SCR leaves the subscriber some freedom in specifying whether the network should buffer packets which cannot be delivered immediately or if the network simply should discard them. Note that eNetwork Wireless works best when the radio network does not do any buffering and retransmitting. However, you are able to configure this option at the eNetwork Wireless Gateway.

The eNetwork Wireless Gateway is able to connect to the DataTAC RNG in two ways. The first one is to establish an X.25 connection; the second one is to establish a TCP connection over a TCP/IP network, which may be routed over the (big) Internet.

When connecting via X.25, many countries provide a public packet switched X.25 network, to which both, the eNetwork Wireless Gateway and the DataTAC provider are then attached. Some countries, such as the U.S. do not have these types of networks and there is a leased line where an X.25 modem is placed at both ends instead of an X.25 network. Further details and the differences relevant to the installation and configuration process, are found in 2.3, "Connections via X.25" on page 41. Be sure that you agree with your DataTAC provider to connect via an X.25 Switched Virtual Channel (SVC) and agree on the X.25 addresses you are using or expecting. You should be given an X.25 address.

Your DataTAC provider is listening for incoming calls. If you are connected via a leased line, you are usually free to set your own X.25 address the way you want, but the DataTAC provider may request that you use a specific one for the connection setup.

If you are connecting to the DataTAC network provider via TCP/IP, you usually will have two TCP/IP interfaces configured on your machine. One interface is connected to the company's intranet and the other one to the external Internet. Since IP addresses in public IP networks are controlled by the corresponding Internet Service Providers (ISPs), you should know your own address, and you should ask your provider for the IP address and port number of the DataTAC RNG you wish to communicate with. It is important to understand and realize the risks in the sense of network security in this case. There is some discussion on this topic in 6.4, "Security Issues" on page 164.

In DataTAC, regardless of whether you use X.25 or TCP/IP, connections between a host and the RNG can either be initiated by the RNG or the host. Be sure that you agreed with your network provider that the host has to initiate the connection. DataTAC networks in Europe and in the Asian Pacific area require the hosts to identify themselves with a host ID and a password. Both will be given to you by your DataTAC provider.

In ARDIS, the hosts are connected via leased lines or in the case of TCP connections the originating IP address is registered. There is no other login sequence to go through in order to connect to an ARDIS RNG.

DataTAC uses a logical link identifier (LLI), which is also called a subscriber unit identifier (SUI) to identify and address a radio modem. The LLI is unique to each device and is comparable to an ESN. So, the eNetwork Wireless Gateway has to know the modem LLI in order to transmit data to it. In the opposite direction, the radio modem specifies in each packet which host is intended to receive this packet.

There are two addressing schemes for DataTAC mobile subscribers to address a host:

1. Slot addressing scheme
2. Extended addressing scheme

In a slot addressing scheme, the mobile subscriber identifies a host by a single digit, called *slot number* or simply *slot*. In ARDIS, for example, valid slots are from 1 to 5. The DataTAC provider has to configure the appropriate host for one of these slots in what is called a *Host Table* for that device.

Actually, to start with a DataTAC provider, you go the other way. You request from your DataTAC provider a *fleet* and specify the LLI numbers, you want to be associated to that fleet and optionally the slot number which should be used for this fleet. The provider will come back with a host name, give you the slot number and optionally a host ID and password to login to your gateway, depending on the DataTAC version. The host name begins with a dollar sign and may look something like \$E55. You may also receive the X.25 address to connect to. Having a fleet configured means that only DataTAC radio modems belonging to the corresponding fleet can communicate with this host.

The slot number is preceded by a 7-bit character string, which can be used by the host to identify the type of communication this packet belongs to. This is called a *slot prefix* and eNetwork Wireless usually uses the string *te* for that. It may be, that the DataTAC provider requires you to use a special prefix. Slot prefix and slot number together form the *slot identifier*, which must be configured in the eNetwork Wireless Client.

The slot identifier and LLI are transmitted to the host in every packet. The eNetwork Wireless Gateway only accepts a packet when a registered mobile client with that LLI is found. It ignores the slot identifier but supplies it in the packets it sends to the mobile device.

In the *extended addressing* scheme, things are a bit different. An extended address is differentiated from a slot address at the first byte. It has to have the highest order bit set to 1 in order to become an extended address. In decimal notation the first byte must be greater than or equal to 128. Extended addresses are notated in *dotted decimal notation* (each byte is represented by a decimal number, bytes are separated by dots). Extended addresses may have variable lengths. ARDIS uses 4-byte addressing, making extended addresses look like Internet addresses (for example 157.23.1.0). Extended addresses uniquely define a host. Every DataTAC modem, registered to this DataTAC provider, can talk to a specific host by providing the same extended address. There are, however, some means to prevent a mobile subscriber from addressing a specific host. This is called *negative entitlement*.

Note

Do not confuse extended DataTAC addresses with IP addresses! They are not the same and have nothing in common.

A DataTAC radio modem must be registered by the DataTAC network provider to be able to access the DataTAC network. This can be done by a phone call to the service center. If this DataTAC network uses extended addressing as explained above, and you did not specify the access to your host to be restricted (forming a closed user group), your modem should then be able to contact the eNetwork Wireless Gateway. If there is a restricted access, tell the network provider to include this modem in the access list. In that case you must have your host name available. You find this on the correspondence with your network provider and it will begin with a dollar sign and look something like \$E55.

If, however, the DataTAC network uses slot addressing, tell the network operator that this modem should go to your host over the same slot you are using for your other modems.

When you try to get a brand new DataTAC modem running for the first time, you should pay attention to the following points:

1. If it is an external modem, connected to a serial port, like the Motorola InfoTAC, be sure that the baud rates match. Use 9.600 baud. For example, some time ago the Motorola InfoTAC came preconfigured with a baud rate of 4800 and we had to change it to 9600 baud to be used by the eNetwork Wireless Client. Refer to your hardware documentation and utility programs for permanently switching the baud rate.
2. Most DataTAC modems have two modes, in which they talk over the serial interface. In *Local Command Mode*, the modem emulates a common Hayes AT command set and allows you to communicate using a terminal emulation program. In *Online Mode* or *Native Mode*, the modem uses the *Native Command Language* (NCL) to communicate with the application. Modems may power up in native mode. In that case, you will not be able to issue AT commands. You can, however issue the escape sequence **+++** to switch to local mode. This, however, is only possible when the baud rates match.

To be used by the eNetwork Wireless Client, modems should come up in native mode. Be sure, that the modem powers up in mode 3, which is native mode.
3. When you plug a PC card modem into your notebook, be sure you know which COM port the modem is using. See 4.2.3.2, "Checking Your Modem under Windows" on page 110 and 4.2.3.3, "Checking Your Modem under OS/2" on page 112 if you need more information.

2.2.2 Motorola Private Mobile Radio (PMR)

The Motorola Private Mobile Radio system is a complete solution to build a private wireless radio network. It is used, for example, by US public safety organizations which cannot depend on public data networks.

It is based on the DataTAC technology and can be considered a private DataTAC network. As depicted in Figure 10 on page 28, it consists of base stations, connected via serial lines to a Motorola RNC3000 controller. The RNC3000 controller acts as RNG and is connected to the eNetwork Wireless Gateway. The protocol used is still SCR but all of the DataTAC management operations have to be performed by the eNetwork Wireless Gateway.

The radio modems are pretty much the same as for DataTAC(ARDIS), but they have to use different frequencies. In fact the Motorola InfoTAC (often simply called *brick*) can be programmed to the correct frequencies to act as a PMR modem. However, in PMR networks higher transmission power is usually required, since the cell sizes are much larger. One of these modems is the Motorola VRM 600. The standard eNetwork Wireless Client software can be used for PMR networks by selecting a DataTAC (ARDIS) modem.

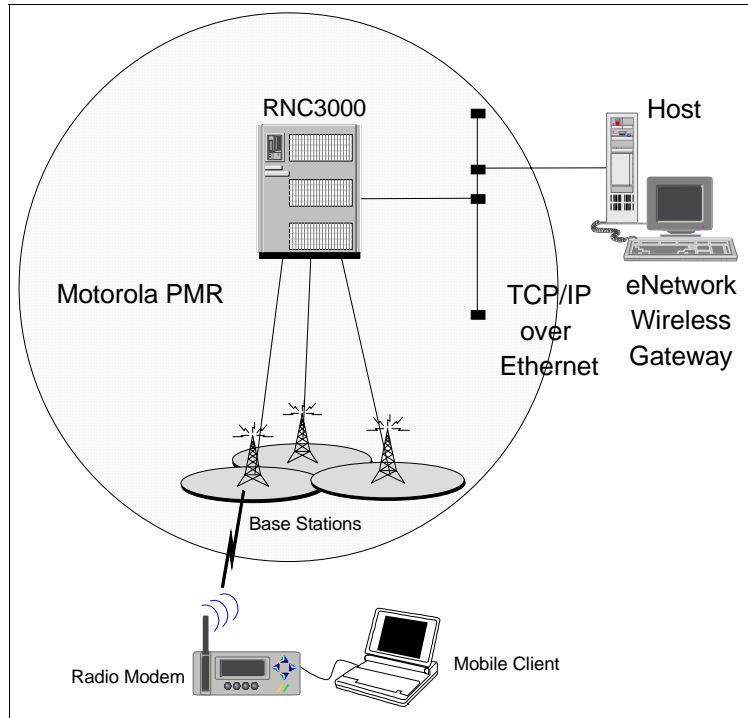


Figure 10. Motorola Private Mobile Radio Architecture

In order to build a PMR network, the customer has to acquire the right to use one or more frequencies to be used by the base stations. Then he or she has to install the base stations and connect them to the RNC3000.

The connection between the RNC3000 and the eNetwork Wireless Gateway is TCP/IP over a local Ethernet LAN. The SCR protocol is encapsulated in the TCP connection using a fixed or variable length message format. This is a bit different than public DataTAC TCP connections, because over this connection the RNC3000 is also configured.

Since the radio modems have to be programmed to the frequency used by the PMR network, there is no slot or extended addressing at the client. This field in the client configuration is meaningless.

The modem LLIs are registered at the RNC3000. The RNC3000 supports several hosts, but one modem can communicate to one host only. Hosts are identified by a CID. Use a CID value of 10, if possible, because this is a reserved ID, which has some extended control functions over the RNC3000 and the eNetwork Wireless Gateway may use them.

The eNetwork Wireless Gateway, does much of the configuration for the RNC3000 controller. Upon startup, the eNetwork Wireless Gateway will register all LLIs belonging to this mobile network interface at the RNC3000. You may flush the table before configuring, to delete all old values, if you have the RNC on your own.

PMR supports broadcasting of messages to all radio modems in coverage transmitting one packet over the air only. This feature can be used to transmit single messages to all of the clients. At the client, these messages may either be

routed to an application or they may be displayed in the status window of the eNetwork Wireless Client. For further details refer to 2.5.7, “Broadcast Messages” on page 52.

2.2.3 Mobitex

Mobitex is a similar technology to DataTAC that developed in Sweden in 1984. The technology is now supplied by Ericsson Mobile Communications AB. It originally started to commercially operate in Sweden, but is spread now over various countries. The Mobitex architecture is depicted in Figure 11 on page 29.

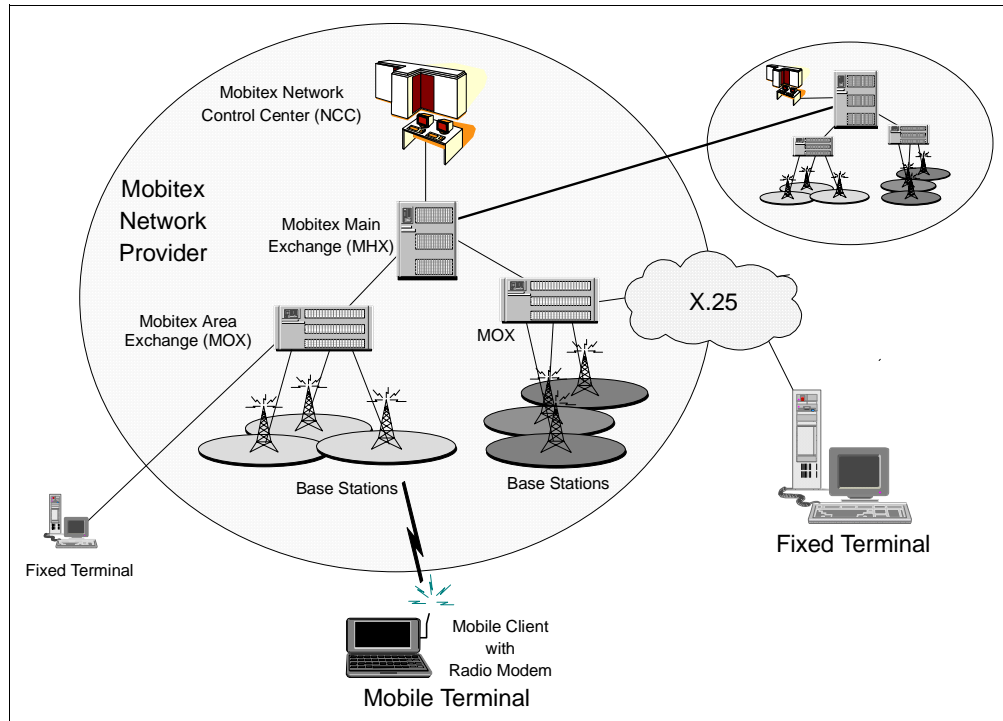


Figure 11. Mobitex Network Architecture

Mobitex operates in the U.S. in the 900 MHz range and in Europe it uses the 400-450 MHz band. Similar to DataTAC, Mobitex uses shared media access within one cell. The data rate of a Mobitex wireless channel is usually 8.0 kbps. The network latency is relatively high and varies significantly. End-to-end transmission rate is usually limited to about 1 kbps. Mobitex provides a maximum message size of 512 octets.

Note

Due to the wireless protocol overhead, the effective data rates are lower than the channel bit rates.

Both, mobile terminals and fixed terminals are treated equally in terms of addressing. Any end system can communicate with every end system in the Mobitex network. It is even possible to address end systems at other network providers if they are interconnected. Mobitex does all the routing necessary for that. So, different Mobitex networks may be interconnected and packets may be

transferred between them, the same way as you would establish international phone calls or between two telephone carriers. This is the big difference compared to DataTAC.

Mobitex mobile and fixed terminals are both identified and addressed by a Mobitex Access Number (MAN), a 24-bit value which is written down in 8-digit decimal notation. Mobitex wireless modem MANs are unique worldwide and are assigned by the modem manufacturer. They act as an ESN, similar to the DataTAC LLI. Every Mobitex network provider has its own address range to assign MANs to fixed terminals. A Mobitex mobile terminal even keeps its MAN when it roams between different network providers.

Mobitex has been designed to be a messaging system, where small amounts of data have to be transmitted at irregular intervals. The transmission characteristics are not well suited for routing IP traffic, so the performance using eNetwork Wireless with Mobitex may be worse than for ARDIS and CDPD, even compared to the same cell bit rate. One problem is the high variance in network latency, because this makes it hard to decide whether a packet should be regarded as lost or just delayed a bit longer.

Access to the Mobitex network from external host systems is provided by a number of different gateways, called MOX. The availability and definition of access methods to these gateways will vary from network to network, but will normally include:

- X.25
- TCP/IP
- SNA/3270

The eNetwork Wireless Gateway only supports connections to the MOX over X.25 links. The gateway will try to set up an X.25 SVC upon startup. When connecting via X.25, many countries provide a public packet switched X.25 network, to which both the eNetwork Wireless Gateway and the Mobitex MOX are then attached. Some countries, such as the U.S. do not have these types of networks and there is a leased line where on both ends an X.25 modem is placed instead of an X.25 network. Further details and the differences relevant to the installation and configuration process are found in 2.3, "Connections via X.25" on page 41.

Be sure that you have agreed with your Mobitex provider to connect via an X.25 Switched Virtual Channel (SVC) and agreed on the X.25 addresses you are using or expecting. In our scenario for this redbook, we were connected to the Mobitex network provider in the U.S. via a leased line. This provider misused the gateway's MAN address as the originating X.25 address he was expecting. This was a bit confusing, but is legal, since on leased line X.25 connections you can choose any X.25 address you want. However, connected to a real X.25 network, the originating X.25 address will be assigned to you by your X.25 network provider and Mobitex has to register this address for incoming connections.

The MOX address you are given is configured at the eNetwork Wireless Gateway mobile network client connection (see 3.4.5.2, "Client Connection over the Mobitex Network" on page 92 for details), and will be used for the destination X.25 address when establishing the X.25 link.

In a Mobitex network the end systems exchange Mobitex packets, called MPAKs. Some MPAKs are exchanged between the terminals and the Mobitex system only. Others flow between the end systems and are routed by the MOX and MHX if they have to leave a MOX domain. The Mobitex radio modem provides a MASC interface to the mobile computer. Similar to the NCL interface in DataTAC, messages called MASC frames are exchanged over a serial link between the PC and the modem. But the MASC protocol is more complex and there are MASC frames exchanged, even if there is no traffic on the wireless link.

A Mobitex radio modem must be registered by the Mobitex network provider to allow access to the Mobitex network. This may be done by a phone call to the service center. Once a modem is registered it can communicate with every device known to that network. Some modem manufacturers provide you with some software that allows you to power up the modem to try to sign on to the network and to check coverage and signal strength without any other application or middleware running. We strongly recommend you install this software before you connect the Mobitex modem for the first time to the mobile device and to sign on without the eNetwork Wireless Client.

For additional security, “closed user groups” may be set up with the network provider.

2.2.4 Cellular Digital Packet Data (CDPD)

Cellular Digital Packet Data (CDPD) is a wireless, packet-switched network technology. It uses the same frequencies as existing AMPS cellular services. Even if analog cellular telephone systems are becoming congested with voice traffic, it is known, that the total information capacity, these networks are able to carry is much greater, because of the “quiet” times during voice conversations. A test conducted on one of the most congested analog networks in the world, New York, revealed that 50% of the network capacity was not being used. While these pauses cannot be utilized by other voice traffic, data packets would fit into these time slots. It has become increasingly common for network operators to dedicate one or more channels to CDPD.

Thus, CDPD is sharing the infrastructure with AMPS networks, which lowers the costs for providing CDPD networks. No separate cellular infrastructure has to be built to provide a packet data service. Like DataTAC and Mobitex networks, CDPD charges are based on the amount of data sent rather than on the duration of the network connection. Because CDPD relies on an AMPS cellular network, it is not available outside North America and some Latin American countries.

CDPD inherently uses Internet Protocol (IP) as the protocol for sending and receiving data. This allows many applications that are used with the eNetwork Wireless Gateway and Client to work without modification using standard CDPD installations.

However, CDPD only gives you access to the Internet. It does nothing to overcome the problems of packet losses and excessive delays when using a wireless packet-oriented network. eNetwork Wireless Gateway and Client provide a number of additional advantages, such as data compression, data encryption, authentication, and IP tunneling. These topics are discussed further in 2.5, “Functions of the eNetwork Wireless Gateway and Client” on page 44.

CDPD networks have a similar architecture as other cellular networks. CDPD Wireless Network Controllers, connected to the base stations, route the packets from the CDPD modems to the Internet and back. They cover the radio protocol, concentrate the traffic of the attached base stations, and manage the hand-off between cells.

Figure 12 on page 32 shows the protocol architecture of a CDPD network without the eNetwork Wireless Gateway and Client. A CDPD modem comes with a network driver enabling the client's IP stack to directly transfer IP packets to the fixed end system. Therefore the CDPD modem is given a fixed IP address from the address space of the CDPD network provider. Keep in mind that with a CDPD modem you can only communicate with fixed end systems, which are visible from the public Internet. Everything behind a firewall is out of reach.

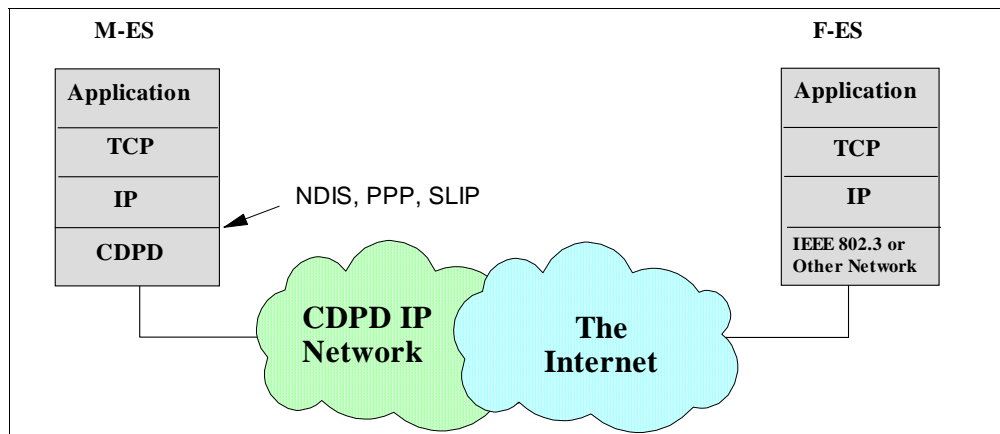


Figure 12. CDPD Protocol Architecture

CDPD radio modems have a burned in EID. Knowing this number, you are able to register this modem at your CDPD network provider. You then get back an IP address, which has to be programmed into the radio modem. Usually you get some utility software to do this. Under this address, everybody in the whole world can reach you, as long as you have your modem turned on.

Note that CDPD is routing its packets over the public Internet, which is very often congested. This is even true when you use the eNetwork Wireless Software. So eNetwork Wireless has to deal with more packet losses than it has to in DataTAC and Mobitex networks. The fact that eNetwork Wireless uses UDP for the transmission protocol between the client and the gateway often leads to the situation that the routers out in the Internet handle this traffic with lower priority than TCP traffic, making the situation even worse.

Note also that connecting to CDPD requires your eNetwork Wireless Gateway to be connected to the (big) Internet, the same way as it has to be for DataTAC/TCP. It is important to understand and realize the risks in the sense of network security in this case. You will find some discussion on this topic in 6.4, "Security Issues" on page 164.

CDPD providers offer to customers a frame relay connection directly from the CDPD IP network to the customer. This will give you much more reliable packet delivery, because you stay within the well-configured CDPD network. But this

doesn't relieve you from the fact that you are still connected to the Internet and are subject to network attacks from the Internet.

2.2.5 PSTN

To most people that have a computer nowadays connecting a computer to a server using an analog modem and establishing a dial-up connection over the PSTN network is very familiar.

By doing this, a peer-to-peer full-duplex connection will be installed, where the bandwidth of this connection is exclusively available to the two peers. In the client/server scenario of eNetwork Wireless, it is important to recognize that on the gateway side there must be as many modems installed as there are users to be able to connect to the gateway concurrently. Figure 13 on page 33 shows the principal architecture. Having this limitation in the number of users being able to connect to the eNetwork Wireless Gateway at the same time is the big disadvantage of dial-up connections with respect to scalability.

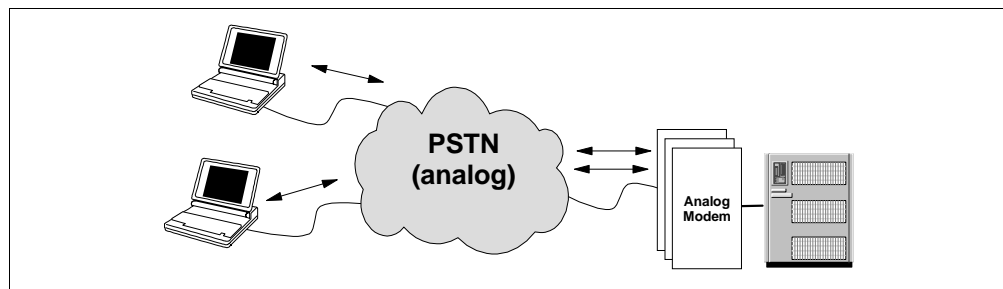


Figure 13. Connections over PSTN Networks

There are special serial adapters available, which allow up to 128 modem devices to be connected and there can be more than one adapter put into a gateway. However, this results in a big number of modems that have to be installed and managed. Each modem has to have an individual connection to the PSTN network and therefore an individual phone number. Each modem can be regarded as a dial-in port.

Usually, there are more mobile users, than there are dial-in ports available. Therefore, it is important to have one number to call for the clients and a PBX to dispatch this number among the modems that are not busy. It is a good idea to configure the PBX in a way that circles the incoming calls in a round-robin manner. So, if a modem should hang, the client will be routed to the next modem on the next call.

The modems on both sides are controlled via standard AT commands. For mobile devices having a PC card slot, PC card modems are available. Analog PSTN systems give the eNetwork Wireless Gateway no opportunity to identify the client, or the phone number from where he or she is calling. The eNetwork Wireless Client has to provide this information when connecting to the gateway. This requires the client to have the calling number configured correctly in order to be accepted by the gateway.

There is only one phone number associated to the client. This number is for identification purposes and to call the client back if the connection has been interrupted. Connection breakdown can be either due to a modem problem or due

to the short-hold feature of eNetwork Wireless (see 2.5, "Functions of the eNetwork Wireless Gateway and Client" on page 44 for details).

Note

Make sure you have the call-back function tested in order to be sure that the modems, at the eNetwork Wireless Gateway and mobile client, have successfully negotiated a common transmission protocol. As described in the sections below, the modems that correspond to dial-up connections from AMPS or GSM networks reside at the wireless network provider.

2.2.6 Analog Cellular Phone Systems (AMPS)

The first cellular systems were developed by Bell Laboratories in the 1970s and experimental operation of the *Advanced Mobile Telephone System (AMPS)* began in 1979 in Chicago. They used analog transmission technology. Today these cellular phone systems are very common in the United States and are offered by several carriers. These networks are coupled with the Public Switched Telephone Network (PSTN). To transfer data over these networks, a special analog modem can be connected to the cellular phone.

Because the wireless analog transmission characteristics are different from wireline networks, special modulation techniques and protocols have been developed to provide a reliable connection over the air. ETC, TX-CEL, MNP-10 and EC are examples of such standards. They achieve data transmission speeds up to 4.8 kbps. However most wireline modems do not support these special standards. In order to still achieve connectivity to the majority of wireline modems, some cellular network providers provide so-called primary access equipment modem pools, such as those depicted in Figure 14 on page 34. In these pools half of the modems support these cellular analog transmission modes and are connected to the cellular network. To each of these modems, a standard wireline modem is attached, which goes over the PSTN to the modem at the final destination.

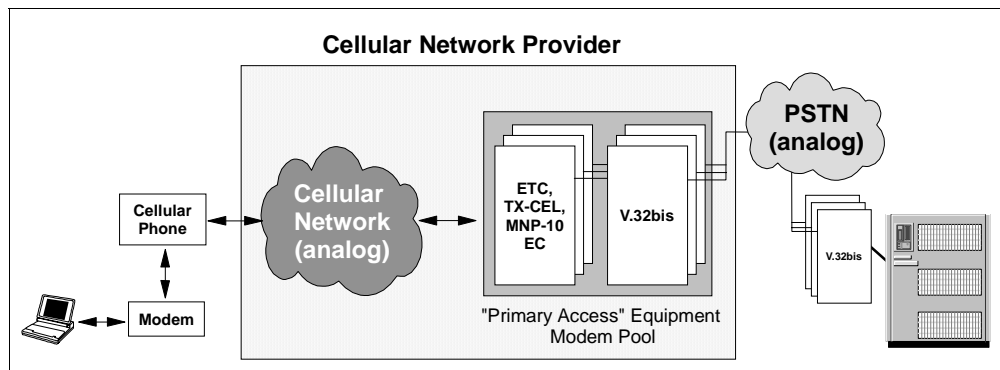


Figure 14. Modem Pools in Analog Cellular Networks

Of course, having four modems involved in a data connection requires some time in the call setup phase until the modems have negotiated all of their parameters. Therefore in an analog cellular network call setup times usually take 20 to 40 seconds but can last up to 90 seconds.

Data connections over AMPS to wireline modems and PSTN dial-up connections are quite similar. The transmission characteristics, transmission speed and error rates are worse over wireless. Connections are very likely to get interrupted, due to coverage problems or other disturbances. Except for these facts, the eNetwork Wireless Gateway and Client software does not recognize any difference. Actually all calls reaching an analog modem on the gateway are handled the same. Therefore, the points mentioned in 2.2.5, "PSTN" on page 33 apply to analog cellular networks, too.

2.2.7 GSM

The Global System for Mobile Communication (GSM) has been standardized by the European Telecommunications Standards Institute (ETSI) for digital cellular telephone and data networks. GSM dominates the European market and is common in the Asian Pacific area. It operates in the 900 MHz band, offers greater signal quality and hence fewer transmission errors, better security through encryption and encoding, and more spectrum giving higher network capacity. More information may be found under the following URL:

<http://www.gsmdata.com>

2.2.7.1 GSM - Networks and Services

GSM networks started with voice telephony and soon added data and fax transmission at variable bit rates. The connection-oriented data service is called Bearer Service and uses the same channels for data transmission that are used for audio communication, giving the user transmission rates up to 9.6 kbps. There are efforts underway to increase speed by combining two or more channels and by applying V.42bis compression.

With GSM phase 2, the Short Message Service (SMS) was added, which provides the ability to do two-way paging using a GSM phone. With the General Packet Radio Service (GPRS), GSM will extend its service portfolio to a relatively high-speed packet-oriented data service, comparable to CDPD, Modacom and Mobitex. The first version of the GPRS standard is complete, while a next version of the standard that adds advanced features such as point-to-multipoint communications is in development. Most GSM vendors such as Alcatel, Ericsson, Lucent, Motorola, Nokia, Nortel, and Siemens have been active in the standards process and many are developing the necessary infrastructure elements. Field trials are expected in 1999 and deployment will begin in the year 2000. Though the GPRS standard specifies support for both X.25 and IP, it is likely that vendors and operators will emphasize IP service.

As an extension to GSM, ETSI developed the Digital Communications System 1800 Standard (DCS1800). It operates in the 1800 MHz band in Europe, uses less power at the mobile phones and has smaller cells sizes. Both standards are functionally similar in terms of voice quality, data facilities, and call handling so the user can hardly tell the difference. DCS1800-based networks are also known as Personal Communications Networks (PCN). GSM technology in the form of DCS1900 is available in North America, and often referred to as Personal Communications Services (PCS) systems.

2.2.7.2 What You Need to Communicate

The eNetwork Wireless Software supports the GSM Bearer Service only. It is very similar to AMPS despite the fact that it is digital over the air. The mobile user has

to have a GSM cellular phone enabled for data transmission. In order to attach most cellular phones to a notebook for data transmission, you need what is called a *DataCard*. And since data transmission is a separate service in GSM, you also have to extend your subscription to include data transmission.

The DataCard usually fits into a PC Card slot and acts as a serial card. There are combo cards available on the market which allow you to connect to a PSTN line and alternatively to a GSM phone. Some manufacturers even put more functions in this card such as attaching to a LAN or to an ISDN network.

There are also GSM phones, which have the DataCard already integrated into the phone. These phones can be directly attached to the notebook serial port or can be linked to the notebook via infrared if both, phone and notebook have a standard infrared transceiver compliant to the IRDA standard integrated. As a third option, some phone manufacturers offer a software solution. The same GSM phone, which may be used in conjunction with a DataCard, may be directly connected to the notebook's serial port using a special cable. You need a special GSM phone driver (mostly available for Win95 only) in order to control the phone and make data calls. You also will need at least a fast Pentium Processor in the notebook to use the software solution. Last but not least, in 1998 more PC Cards became available that have the GSM phone already integrated in it. These types of GSM phones are often referred to as *CardPhones*.

The hardware market in this segment is not an easy one and there is considerable effort to make these devices smaller, less power consuming and more convenient to use.

2.2.7.3 Identifying Mobile Devices and Subscribers

For authentication, the GSM mobile phone has an ESN burned in, which normally is not used by the network provider. However, a GSM provider may blacklist cell phones which are reported to be stolen using the ESN to identify these phones. Every GSM phone has a smartcard in it, called a Subscriber Identity Module (SIM), given to the subscriber by the network provider. The SIM is used to uniquely identify the subscriber, regardless of which cell phone is used. It holds a card number, the telephone number and an encrypted user passcode. On registration, the user must supply the passcode, which must match the encrypted version in the SIM before the mobile phone will register in the network.

Note that GSM distinguishes different services. Voice and data communication are not the same and can be handled differently. A GSM cell phone recognizes the type of incoming call and shows it on the display. The more modern GSM phones may have different strategies for voice and data calls. So, it is possible to configure incoming voice calls to be directly routed to a messaging system while incoming data calls are transferred to the DataCard.

In order to decide whether a call originating from an analog PSTN network is a voice or a data call, a GSM subscription includes three numbers for voice, data and fax.

However, if you call from a digital telephone network, such as ISDN, the type of service (data/voice) is transmitted on the signalling channel which is normally recognized by the GSM providers. In that case, data calls directed to the voice number (which is usually the main number) will be recognized and treated as data calls. As you already probably know, digital telephone networks allow the

signalling of the caller party phone number. Please note that in GSM the caller party number normally is the voice number whether it is a voice or a data call.

2.2.7.4 GSM Bearer Service Types

For the GSM Bearer Service, GSM defines two options to transmit data over the air, referred to as *GSM Bearer Service Types*:

- Transparent
- Non-transparent

Every modern GSM phone and data card should support both Bearer Service Types frequently referred to as modes. The difference between these two modes is that in *transparent* mode the bits from the data card are transmitted over the GSM data channel and the PSTN line as is. In this mode, the DataCard and the modem in the wireline network directly talk to each other and negotiate the transport protocol. The data stream over the air experiences some forward error correction, but all bit errors, that cannot be recovered, will be passed to the PSTN network and must be handled by the DataCard and the wireline modem. If the DataCard supports it, they can negotiate a reliable transport protocol such as V.34.

In *non-transparent* mode, GSM uses an internal error correction protocol over the wireless link. Similar to AMPS, having a Primary Access Equipment Modem Pool, the data link is split into two segments, each having different link protocols to provide reliable transmission. Therefore the modem in the MSC talks to the modem in the wireline network.

We strongly recommend you use the non-transparent mode if possible, since this type of connection has proven to be much more reliable. You should also avoid using a reliability protocol that has not been designed to work over wireless connections.

The GSM Bearer Service Types (transparent/non-transparent mode) are selected by the GSM phone and can be set via special AT commands. For the modems that are supported by the eNetwork Wireless Client this parameter is set correctly. If you have to modify the profile for your GSM device, consult the manual that came with your DataCard, CardPhone, or driver software.

Newer GSM devices should support the standards ETSI GSM 07.07 and ETSI GSM 07.05. They suggest selecting the GSM Bearer Service Type with the following command:

```
AT+CBST=<speed>, <name>, <ce>
```

It has the following parameters:

<speed>:

0autobauding (automatic selection of the speed; this setting is possible in case of 3.1 kHz modem and non-transparent service)

79600 bps (V.32)

719600 bps (V.110 or X.31 flag stuffing)

<name>:

0data circuit asynchronous (UDI or 3.1 kHz modem)

<ce>:

0transparent

1non-transparent

Other values for these parameters are defined, but not included in this description.

To connect to an analog modem via PSTN, you should use:

```
AT+CBST=7,0,1
```

To connect to an eNetwork Wireless Gateway attached to GSM via GSM-ISDN (via UDI) you should use:

```
AT+CBST=71,0,1
```

This selects the V.110 protocol to embed the 9600 bps data stream into a 64 kbps ISDN channel. For details refer to 2.2.7.6, "Connecting to Digital Wireline Networks (ISDN)" on page 39.

To make sure that the settings are correct, go to a simple terminal emulation program configured for your GSM phone, reset it to factory defaults (AT&F), set the options you need and try to dial the eNetwork Wireless Gateway. You receive a CONNECT message if you are successful. If not, you will have to fix the dial string before you proceed with the configuration of the eNetwork Wireless Client.

2.2.7.5 Connecting to Analog Wireline Networks (PSTN)

Having your hardware configuration on the mobile side in place, you should be able to connect to every PSTN modem in the telephone network and vice versa. This leads you to the configuration for eNetwork Wireless as depicted in Figure 15 on page 38. Note that in this case, the gateway only sees a dial-up connection from the PSTN network and the points mentioned in section 2.2.5, "PSTN" on page 33 concerning the Gateway infrastructure apply.

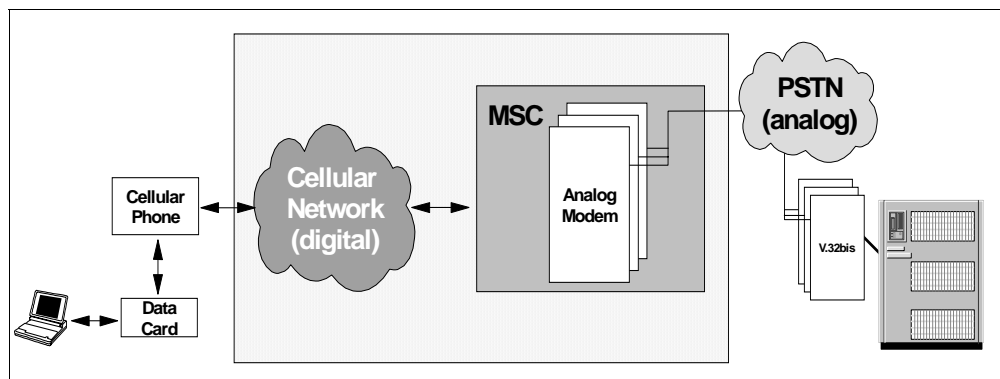


Figure 15. Modem Pools in Digital Cellular Networks

Similar to AMPS, the cellular network provider has to care for the transition to the PSTN network. For this the MSCs are equipped with a modem pool to which the MSC routes the 9600 bps data channels from the GSM network. If a mobile user dials a PSTN number, the following happens:

1. Some user or application dials a number using the AT command ATD.
2. The cellular phone tries to make a data connection.
3. The MSC receives this connection request and assigns it to one free analog modem in the pool.
4. Now that modem dials the destination number over the PSTN network.

5. Then the PSTN modem hooks off and the MSC connects the GSM data call. Now an open data channel exists.
6. Now the modem in the MSC waits for a carrier signal and tries to negotiate a transmission speed. If it succeeds, it signals this to the GSM phone and the DataCard issues the message *CARRIER xxxx*.
7. After that, the two modems have to negotiate a transport protocol. If this succeeds, the user or application receives the message *CONNECTED xxxx*.
8. Now the connection is ready for data transfer.

The whole procedure usually takes about 20 to 30 seconds. Most of the time is spent during steps 6 and 7, for which the customer has to pay the air time.

2.2.7.6 Connecting to Digital Wireline Networks (ISDN)

In countries where both GSM and a digital telephone network using standard Integrated Services Digital Network (ISDN) are available, you may find that your mobile network carrier provides a pure digital transition to the ISDN network, called Unrestricted Digital Information (UDI). Since the transmission speeds between GSM and ISDN differ significantly, the rate adaptation protocol V.110 has been chosen by the mobile carrier to embed the GSM data stream into the 64 kbps B-channel provided by ISDN.

For the transition of GSM data calls to ISDN, the GSM network provider has a pool of ISDN terminal adapters installed in addition to the analog modems used for PSTN access. A GSM data connection via the ISDN wireline network is depicted in Figure 16 on page 39.

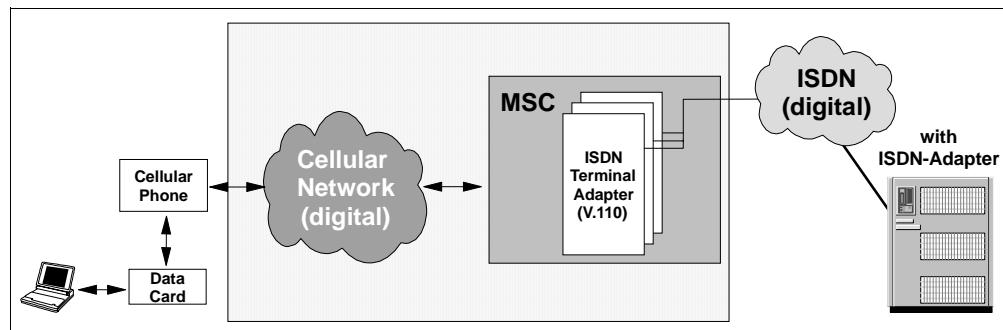


Figure 16. Transition from Digital Cellular Networks to ISDN (Digital) Using UDI

The eNetwork Wireless Gateway hardware infrastructure to support ISDN is a bit different than PSTN access. There is no modem pool like in PSTN. You do not need any serial connections to attach to ISDN.

ISDN multiplexes several channels over a single access line. It distinguishes between the digital user channels (B-channels) available to the user and an independent signalling channel (D-channel). The B-channels are used for a variety of connection-oriented services like voice, data, or fax transmission. Each channel has a transmission rate of 64 kbps. The connection management is totally handled by the D-channel. Only when the called party accepts an incoming call, is a B-channel occupied on both sides and a connection switched through the network. The D-channel protocol also allows the exchange of caller identification and the type of connection that the caller wants to establish, for

example voice, data transparent or data over V.110. Every ISDN access line contains one D-channel that is responsible for all B-channels on this line.

There are two ISDN access types you can order from your providers: one is called *ISDN basic access* (comprised of two B-channels) and *ISDN primary rate access* with 30 B-channels on one line. Therefore, basic access is equivalent to two PSTN lines and primary rate access is equivalent to 30 PSTN lines. There are ISDN adapters for both access types. Keep in mind, however, that the ISDN adapter must support V.110 on all of its ports, to allow as many GSM connections as there are B-channels available. Note also that in ISDN you can even have an analog data connection over a digital B-channel if the ISDN adapter supports this, but a digital connection to an analog port will fail. However the eNetwork Wireless Gateway does not support analog calls over ISDN.

Note

For test installations you can run with an ISDN basic access line, but in a production installation we recommend you use an ISDN primary rate access line.

ISDN adapters widely support the COMMON-ISDN-API (CAPI), which is an application programming interface standard used to access ISDN equipment connected to basic rate interfaces (BRI) and primary rate interfaces (PRI). For more details, look on the Web at:

<http://www.capi.org>

The eNetwork Wireless Gateway uses this interface to communicate with the ISDN adapter. It allows you to specify how many B-channels you want to use for eNetwork Wireless and the protocol you expect incoming calls on (for GSM this is V.110). The ISDN interface does not support analog or voice calls.

The mobile unit has to specify whether it expects the phone number to be an ISDN number capable of accepting V.110 data calls or whether the call should be routed the analog way. This is done during modem initialization with the command specifying the GSM Bearer Service Type (see 2.2.7.4, "GSM Bearer Service Types" on page 37).

2.2.8 Dataradio

Like the Motorola PMR network, Dataradio is a private network technology, where the customer has to acquire the right to use one or several frequencies and to operate over the whole infrastructure.

The simplest Dataradio network consists of some radio modems and a *Base Station Data Link Controller* (BDLC). The eNetwork Wireless Gateway may be connected to the BDLC using a serial line.

Note

Support for the connection to a Dataradio BDLC is not included in the current printed documentation.

With Dataradio technology you can also build a cellular network, where the BDLCs are interconnected via a *Multi-Site Controller (MSC)*. The eNetwork Wireless Gateway is connected to the MSC using TCP/IP over an Ethernet LAN.

The Dataradio modem is an external device connected to the notebook's COM port. The modem has a burned-in address, four to eight characters long, each character in the range from *A* to *P* (all capital letters). These are 16 values representing internally a 4-bit hexadecimal digit, resulting in Dataradio addresses that are two to four octets long (*P* is 0x0, *A* is 0x1, *B* is 0x2,..., *O* is 0xF). The address *P* stands for the device itself (loopback). Addresses from *A* to *GN* are reserved for base stations. *GO* and *HP* have special meanings. *HA* to *OO* are configurable broadcast addresses, and *APP* to *OOO* are MRM addresses. So the first radio modem address is *APPP* going up to *OOOOOOOO* (meaning 0xFFFFFFFF).

Interestingly, radio modem, BDLC, and MSC communicate with a protocol called *Dataradio Multiplex Protocol (DMP)*. Fortunately you will not have to deal with all of this stuff, because the provider of Dataradio networks will help you to set the wireless network up.

Note

For the physical connection between the eNetwork Wireless Gateway and the BDLS no cross-over cable is to be used. That means that the BDLS acts as an RS 232 Data Communication Entity (DCE).

At the eNetwork Wireless Gateway, a serial port has to be used, which is neither used for dial-up connections such as the PSTN mobile network connection type nor by attaching a console for logging in to the gateway. This serial port has to be configured to 9600 baud and full control has to be disabled.

2.3 Connections via X.25

X.25 is an ITU-T standard and networks complying to this standard are usually called X.25 networks. An X.25 network is a packet-oriented data network, consisting of end systems, intermediate systems (packet switches) and transmission lines between them. In many countries public X.25 is installed.

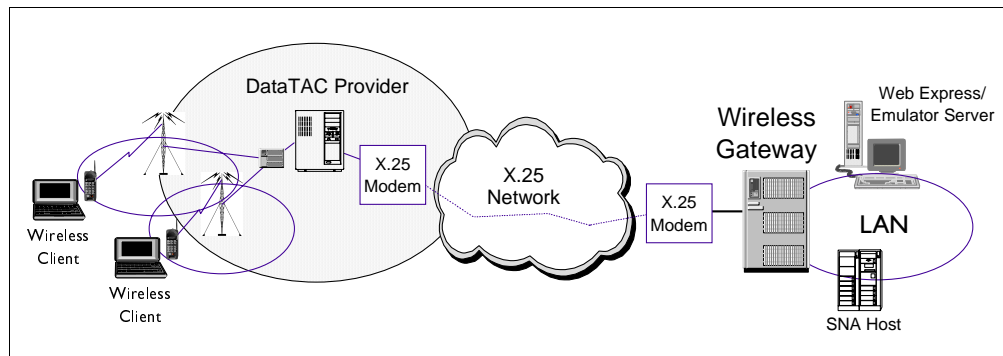


Figure 17. Wireless Gateway Connecting to a DataTAC Provider Using an X.25 Network

X.25 has the concept of virtual connections. If they are permanently set up by the network provider, they are called permanent virtual circuits (PVCs). If they are established dynamically between end systems and logically switched through the network, they are called switched virtual circuits (SVCs). In an X.25 network, every end system has an X.25 address, which can be compared to a telephone number in the telephone network.

Every end system has one physical connection to the device in the X.25 network, called Packet Assembly/Disassembly (PAD) unit. Usually this is a leased line, terminated by an X.25 modem. There may be dial-up connections to the X.25 network and there may be access methods via other data networks. For example, in Europe it is possible to connect to the X.25 network via an ISDN access line, using the X.31 protocol.

Because packet radio networks can be regarded as a natural extension to X.25 networks, some of them provide interfaces to the wireline world via X.25 access as depicted in Figure 17 on page 41. In countries where there is no X.25 network in place, customers connect to the wireless network using leased lines but retain the X.25 protocols between the end systems as shown in Figure 18 on page 42. In that case two X.25 leased line modems terminate the leased line on both sides.

Keep in mind that the X.25 adapter in that case has to be configured to go to a leased line connection.

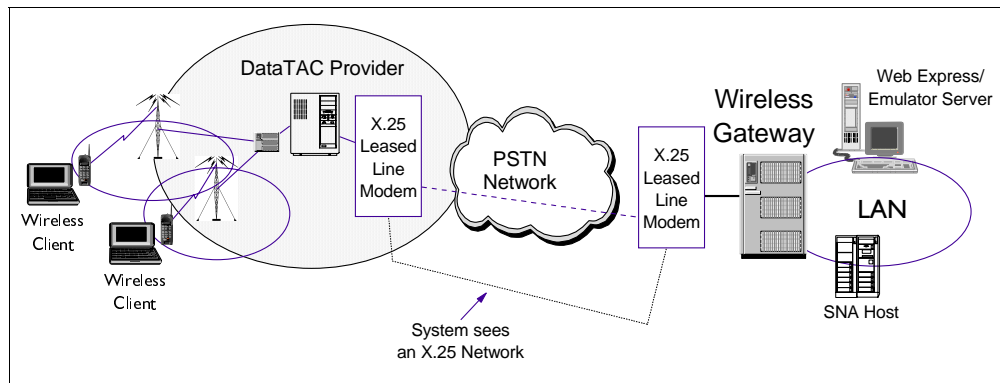


Figure 18. Wireless Gateway Connecting to a DataTAC Provider Using a Leased Line

When you connect to end systems over an X.25 leased line, you are free to assign the X.25 addresses you like. However, there must be an agreement between the two parties, because the end system that initiates a connection has to supply the X.25 address of the other party.

If there is a mismatch, the caller will receive a disconnect indication message by the remote party.

Note

In some limited circumstances, "dial modems" may be used to make a pseudo-leased line X.25 connection for testing and demonstration purposes. In this case, the gateway side should initiate the call to the wireless network.

If there is a need to establish more than one connection to the same wireless network provider, you have two options. If at the network provider the X.25 connections end in the same system, meaning the same X.25 address, you can set up two SVCs. The last two digits in an X.25 address allow you to specify a service access point, which can be used to differentiate the two SVC connections. In this case, you only need one X.25 adapter in your machine.

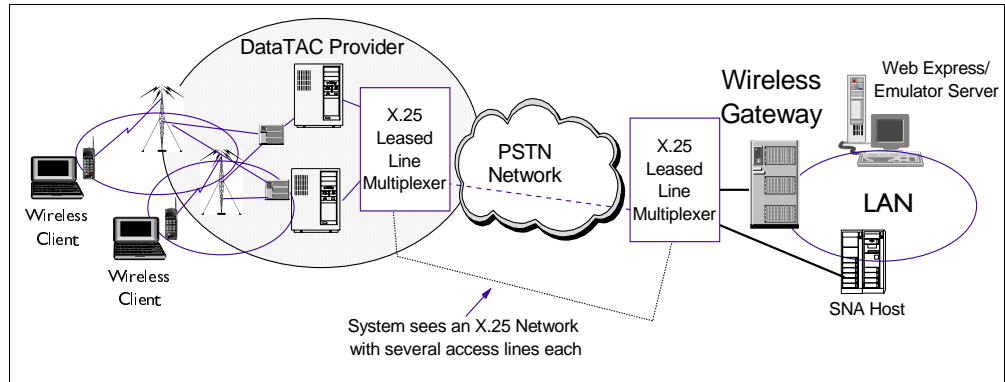


Figure 19. Multiplexing Several X.25 Connections over a Single Leased Line

If, either on your side or on the side of the network provider, the X.25 connections have to end on different machines, you could of course use two leased lines. It is much cheaper, however, to replace the X.25 leased line modems with a multiplexer. This gives you several X.25 ports at each end, which have to be connected to one X.25 adapter each. An example is depicted in Figure 19 on page 43 and shows two DataTAC RNGs where one RNG is connected to a wireless gateway and the other one directly to an SNA host. Both connections are running over the same leased line.

Note

An X.25 adapter in a workstation can only be connected to a single physical link (connection to an X.25 modem). This is not a problem when you connect to a real X.25 network, because then you can set up several SVCs to different wireless network providers. You only have to be sure that the X.25 provider allows you to set up more than one SVC and you have more than one SVC configured for your adapter. However, if you have leased line connections, this will require an X.25 adapter for each connection.

In the U.S. ARDIS can provide a complete service for accessing the DataTAC network, including X.25 ports at the customer location.

2.4 Which Wireless Network Is the Best?

The decision, of which wireless networks to use for an eNetwork Wireless solution has of course to be made before installing the eNetwork Wireless Gateway and Client. There are, however, some general aspects which are useful to remember and they help when discussing with eNetwork Wireless customers or end users.

The first and most important issue is coverage. Deploying a radio network, where coverage is missing at the areas the mobile workforce is likely to use eNetwork Wireless, doesn't make much sense. Even if the eNetwork Wireless Gateway and Client supports a variety of mobile networks, one mobile device usually uses one wireless network only. Companies which cover a larger geographic area and are subdivided into regions, assuming that one mobile worker spends most of his time in one region, you may consider having different wireless networks in the regions, but all of them connected to one eNetwork Wireless Gateway.

In the lucky situation that a specific region is covered by several wireless networks, the choice, of which network to use depends on the type of application. This leads to the decision whether to select a circuit-switched cellular type of network, like AMPS or GSM, or whether a packet radio network, like DataTAC, Mobitex, or CDPD is more appropriate. Figure 20 on page 44 gives you some selection criteria and how common types of applications are positioned in this scale.

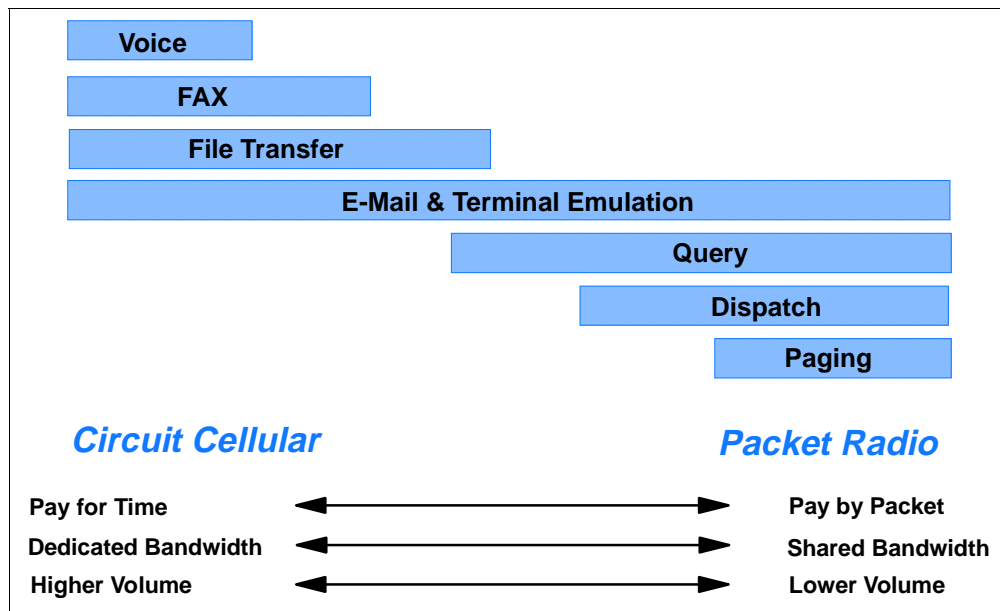


Figure 20. Selection of Wireless Networks

Keep in mind that you may have to trade communication costs for performance, and that bigger customers may be able to negotiate tariffs. For example, you may be able to agree on a monthly fee per client independent from the actual data traffic on a packet radio network.

2.5 Functions of the eNetwork Wireless Gateway and Client

Figure 21 on page 45 depicts the software architecture of the eNetwork Wireless Gateway. The basic functions are already discussed in the *eNetwork Wireless Technical Overview* (GC31-8630) and *eNetwork Wireless Gateway and Client V4R1 Administrator's Guide* (GC31-8633). In the following, some of the concepts used in the gateway are explained in some more detail, in order to give you hints for the configuration of some advanced parameters in the gateway.

2.5.1 eNetwork Wireless Gateway Software Architecture

As you see in Figure 21 on page 45, the eNetwork Wireless Gateway consists of three main blocks: the gateway software itself, the management facility via the SNMP agent and the AIX style management via SMIT. The gateway itself is divided into three layers. The top layer, the *Interface to AIX TCP/IP* contains the IP related functions. The middle layer which may be called *eNetwork Wireless Layer* contains functions which distinguish the eNetwork Wireless Gateway from other remote access routers. The lower layer, the *Mobile Network Connections layer*, contains all the wireless network specific functions. The Mobile Network Connections layer is subdivided into pillars, one pillar for each mobile network connection. At the very bottom are the mobile network devices like TCP or X.25, which provide for access to the wireless radio networks over wireline networks.

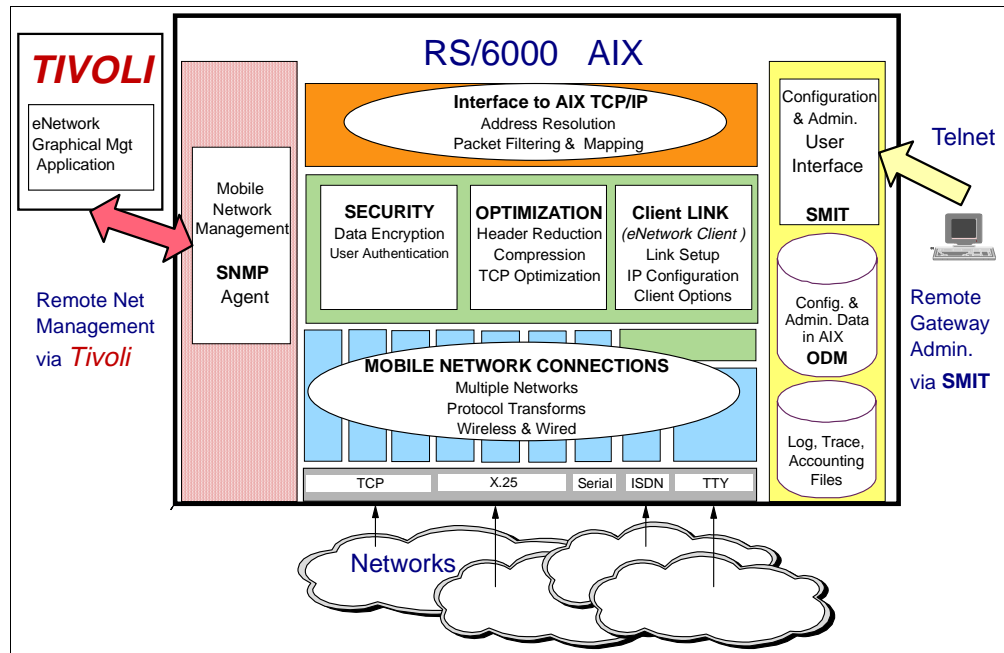


Figure 21. eNetwork Wireless Gateway Architecture

For the eNetwork Wireless Gateway, many configuration parameters exist. They are all stored in an AIX specific configuration database, called ODM where configuration information of other AIX resources are stored, too. The eNetwork Wireless Gateway integrates smoothly into the AIX concepts. So gateway configuration and control is performed for AIX using SMIT, which needs an X-Windows terminal or SMITTY, which can be used over an ASCII session, either via ASCII-console or remotely via a telnet session.

SNMP stands for Simple Network Management Protocol and is the network management protocol used in TCP/IP networks. The SNMP agent allows you to look at the eNetwork Wireless Gateway via a TIVOLI network management console (former NetView/6000) and it is an alternative method to SMIT for configuring and controlling the eNetwork Wireless Gateway. Section 3.6, “eNetwork Wireless Network Management” on page 97 discusses this issue in more detail.

2.5.2 IP Addressing with eNetwork Wireless

After installing the eNetwork Wireless Gateway, you do not see the gateway as a software component. The same way TCP/IP functionality is presented via an IP interface, eNetwork Wireless functionality is presented via a *Mobile Network Interface*. So, you activate the eNetwork Wireless Gateway by creating a *Mobile Network Interface*. Similar to an IP interface, a Mobile Network Interface has a name, for example *mn0* and an IP address, belonging to a *Mobile Subnet*, in which all mobile clients normally reside. An IP interface is normally bound to a single network adapter, a Mobile Network Interface has several *Mobile Devices* defined for this purpose. Over these mobile devices, the *Mobile Clients* are connected. As shown in Figure 22 on page 46, a Mobile Client has only one IP address located in the mobile subnet associated to the mobile network interface of the eNetwork Wireless Gateway. It doesn't matter over which wireless network the Mobile Client is connected to the gateway.

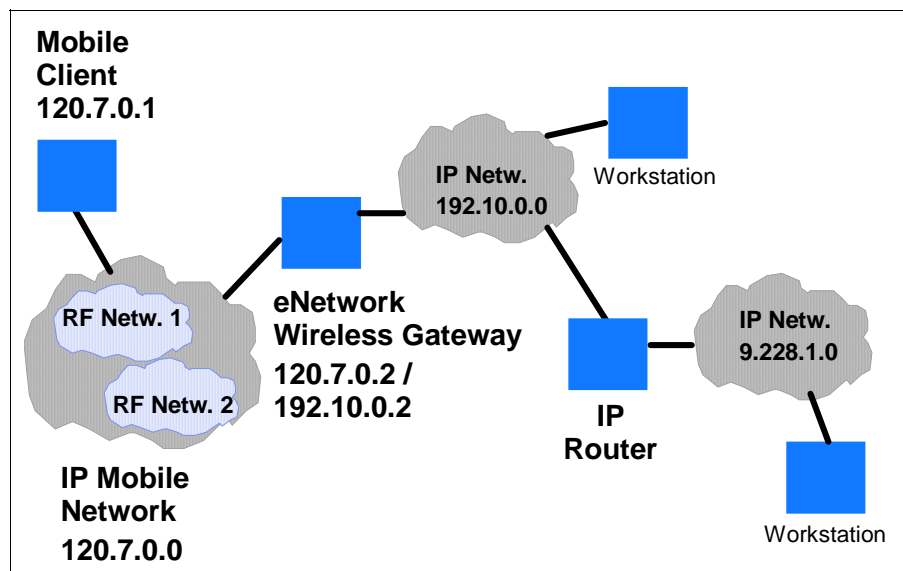


Figure 22. IP Addressing in the eNetwork Wireless Gateway and Client

The Mobile Client IP address is configured in the gateway and will be set in the Mobile Client when it establishes a connection to the eNetwork Wireless Gateway. However, the client IP address is stored locally, because if the Mobile Client already knows its own address, and communicates it to the gateway, two packets less will have to be transmitted.

2.5.3 Data Transmission Techniques

eNetwork Wireless Gateway and Client use an encapsulation technique to transmit IP packets over the different wireless links as depicted in Figure 23 on page 48. eNetwork Wireless takes each IP packet, optionally compresses and encrypts it and encapsulates it into an eNetwork Wireless Protocol packet. The eNetwork Wireless Protocol is also called *ARTour² Link Protocol (ALP)*. The ALP is independent from the radio network over which the packet is to be transmitted. In volume charged networks, this is usually the data the subscriber has to pay for. The ALP data unit is again encapsulated in network-specific Wireless Network

² eNetwork Wireless was formerly named ARTour (*Advanced Radio Communication on Tour*). Therefore in many technical specifications, and within the software itself this name is still found.

Protocol. The structure of the corresponding header is specified by the wireless technology and may differ between client and gateway side.

ALP provides two-side *authentication*, which is outstanding compared to other remote access protocols. This means, that not only does the Gateway know who the user is, by checking its authorization, but the client is also sure that the gateway is the one wanted and is no fake. During the authentication procedure, a *session key* is also exchanged to be used for encryption of the complete IP packets exchanged further on. There is always a new session key exchanged, every time the eNetwork Wireless Client logs on to the gateway. Authentication is an optional feature of eNetwork Wireless Gateway and Client. If it is enabled, the user at the mobile client computer has to key in a password, which is initially set by the eNetwork Wireless Gateway administrator when registering a mobile client. The mobile user is able to change this password at any time while he or she is connected to the gateway.

The transmission of messages exchanged to set a new password is encrypted. Passwords have to follow certain rules which can be set by the gateway administrator to make password guessing hard for potential intruders. Authentication is a prerequisite for the communication between the eNetwork Wireless Gateway and Client to be encrypted.

Note

The eNetwork Wireless Client has the option to save the password in order to keep the user from entering it every time he or she logs into the eNetwork Wireless Gateway. Even if the password is stored in an encrypted form, this is a potential security leak, since everyone who has access to the mobile computer may access the network that eNetwork Wireless allows you to connect to. We strongly discourage you from using this feature and the corresponding checkbox can be hidden via client configuration (refer to 4.2.7, “Advanced Configuration Issues” on page 127 for details).

However, if you should decide to use this feature, make sure that no one else can access your computer, for example by setting BIOS and hard disk passwords.

Data *encryption* helps to prevent inappropriate access to the data exchanged between the eNetwork Wireless Gateway and Client by transforming it into an unintelligible form using the session key exchanged during the authentication process. The original data can only be decrypted by someone who possesses the session key.

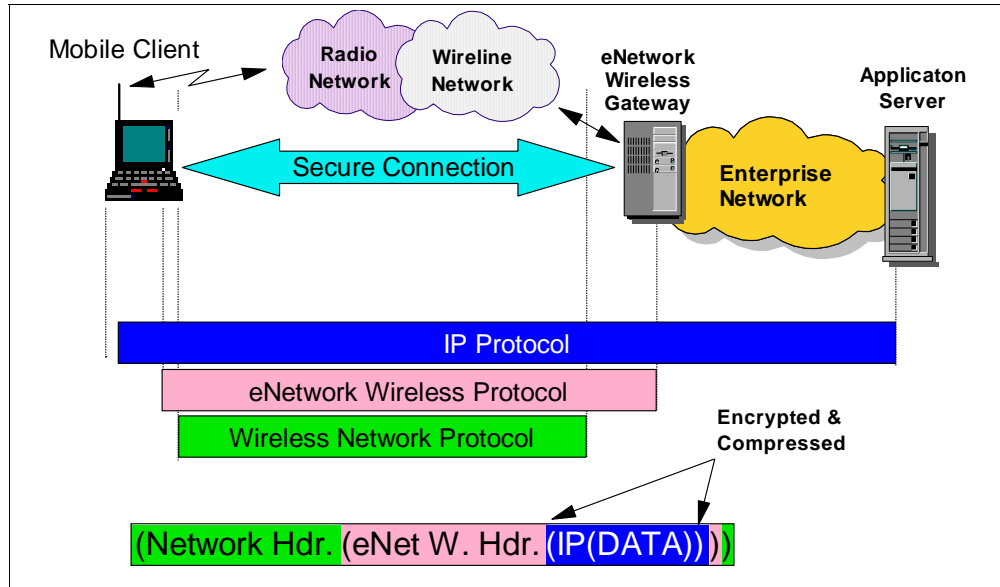


Figure 23. Protocol and Encapsulation Hierarchy of eNetwork Wireless

Since the session key is dynamically created by the eNetwork Wireless Gateway and is transmitted to the mobile client encrypted during the authentication process, this key can be regarded as a secret between the eNetwork Wireless Client and the gateway.

For encryption the Commercial DES Masking Facility (CDMF) algorithm is used. CDMF implements a 40-bit encryption key. If you should need the DES algorithm, which uses a 56-bit wide encryption key, this is also available as an optional feature in the form of a PRPQ. Availability of the PRPQ in specific countries is subject to applicable laws.

If encryption is enabled, the *ARTour Link Protocol* (ALP) can be considered as a *Secure Tunneling Protocol* between the eNetwork Wireless Gateway and Client. It covers both the wireless and the wireline part of the connection. This secure tunneling is also provided when wireless networks are connected over the Internet to the gateway.

2.5.4 Optimization Techniques

Besides providing secure access to the customer's intranet, eNetwork Wireless does a lot to optimize communication over the wireless link. One is *compression*, as already mentioned before. With compression the IP packet is taken individually and its size is reduced in a way that it can completely be restored at the receiver. This is done, without having any knowledge of the content of the IP packet. This increases the effective data rate of the wireless network. It also decreases the amount of data to be transmitted and therefore transmission costs in most cases. Note, when combining compression and encryption techniques compressing the data before encrypting it leads to a higher compression ratio.

Note

Ideally, you would compress data only once to get optimal results. However, since Version 4.1.2 of the eNetwork Wireless Gateway and Client, data is already compressed and not compressed a second time. So we recommend to leave compression always enabled.

If you are running older versions of the product you may not want to enable compression, because the application already has compression built in it, which for example is the case in eNetwork Emulator Express or eNetwork Web Express.

That is the reason why in the older versions the default value for compression has been set to NO, with the exception of dial-up connections.

The second optimization technique works for TCP traffic only and is called *TCP Header Reduction*. It is known that TCP adds a 40-byte header to each packet it transmits. This header is needed to provide reliable communication over IP. Assuming a point-to-point connection between the eNetwork Wireless Gateway and Client, some of the fields in the TCP header are redundant. TCP header reduction takes out this redundancy. For TCP header reduction, the context of each TCP connection has to be saved on both sides, the client and the gateway, and only changes to this context have to be transmitted. This reduces the 40-byte TCP header to an average size of 3-5 bytes. This reduction uses the Van-Jacobson reduction algorithm, which is described in RFC 1144.

Note that reduction means information removed from a packet cannot be restored by looking at the individual packet. Only when the context is stored on both sides can this information be recovered.

eNetwork Wireless has another method to optimize TCP communication, called *Retransmission Optimization*. It has been observed that TCP communication over wireless links often leads to packet retransmissions because of the small bandwidth available or the high latency over the wireless link. The retransmission optimization in the eNetwork Wireless Gateway and Client addresses this problem, as shown in Figure 24 on page 50.

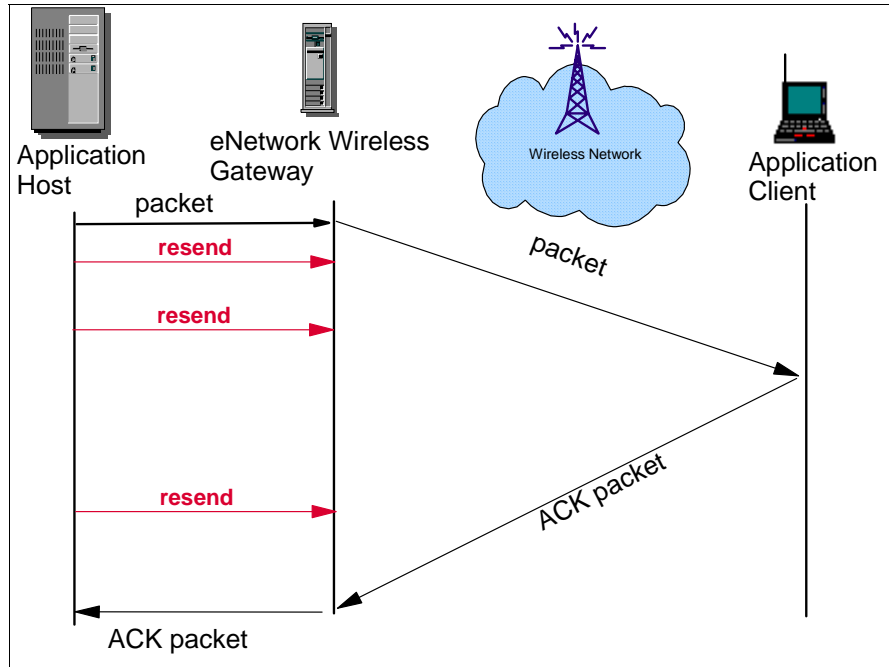


Figure 24. Retransmission Optimization

Last, but not least, there is a mechanism which allows you to reduce air time on connection-oriented wireless networks and PSTN. It is called *Short Hold Mode*. In short-hold mode there is no established physical connection over the mobile network, but client and gateway are in a state, such that they are virtually connected. If the client or gateway is requested by the IP stack to transmit an IP packet, this component will re-establish the physical connection and start the transmission immediately. Short-hold mode is entered when there is no traffic on the line for a certain amount of time. Both, the eNetwork Wireless Gateway and Client have a timer configured after which the short-hold mode will be initiated. To enter the short-hold mode, one party simply hangs up the line.

Short-hold mode is especially useful when the connection setup time is relatively short, as it is in GSM networks connected to the gateway over ISDN (roughly 10 seconds.).

The short-hold mode function is also useful for recovering from connection breakdowns on cellular switched networks. Since none of the parties in a wireless connection can determine if short-hold mode has been entered due to the fact that the opposite party intended to, or the connection was interrupted by the wireless network provider, the connection will automatically recover when one party wants to transmit a packet.

2.5.5 IP Packet Filtering and Mapping

For security purposes and to avoid transmitting packets to a wireless client which shouldn't receive them, the eNetwork Wireless Gateway provides for *packet filtering* mechanisms. Packet filtering reduces the traffic on the wireless link. It allows you to specify, for example, to filter out all ICMP messages, but allow PING messages to be transmitted for test purposes. Also, SNMP requests directly addressed to the mobile client can be blocked since the eNetwork Wireless

Gateway SNMP agent could be used to get information on a specific mobile client.

Packet mapping at the eNetwork Wireless Gateway allows you to change specific Fields in an IP packet, which transits through the gateway. This allows you to perform address translation and other things, which really require you to be a TCP/IP wizard.

eNetwork Wireless filtering mechanisms may also be used to restrict or explicitly permit selected mobile users to access specific IP address ranges.

2.5.6 DataTAC Transmission Parameters for Motorola PMR

DataTAC PMR leaves you the option to select one of two packet delivery modes for outbound messages:

Confirmed Allows host message sizes of up to 4096 bytes sent to the RNC3000 for delivery to a mobile device. The RNC then breaks the (up to) 4096-byte message into (up to eight) 512-byte or shorter message fragments. Each message fragment requires a radio level acknowledgment sent by the receiving mobile device signifying that the message fragment was successfully delivered to the mobile device. If a message fragment is not acknowledged, the RNC3000 will retransmit the message fragment until an acknowledgment is received. When all eight message fragments have been delivered and acknowledged, the host is then allowed to send another message to that particular mobile device. This means that a host message cannot be transmitted to a particular mobile device until all the message fragments of the previous message have been delivered and acknowledged by the mobile device.

Unconfirmed Limits the host message size to be no larger than 512 bytes. No radio level acknowledgment is performed; therefore no retransmission is performed by the RNC3000. In addition, the host is able to send messages as fast as the RNC3000 can handle them. That means the eNetwork Wireless Gateway has to fragment IP packets larger than 512 bytes.

Here is a discussion which helps you to decide whether to use confirmed or unconfirmed mode.

If we consider the connection-oriented TCP protocol, which is based upon IP, this protocol requires each message to be acknowledged by the receiving party. If the acknowledgment is not received within a window of time, the sending TCP entity will retransmit the packet. TCP is usually used by applications to reliably exchange data. In the case of UDP no acknowledgments are required; therefore no retransmissions are performed.

At the application level, there may be acknowledgments, too. This means that application level acknowledgments are sent between the client and server application upon receipt of messages. These acknowledgments are completely independent to both IP and radio network layer acknowledgments. Application level acknowledgments also imply application layer retransmission of messages if they are not acknowledged within a given time window. If the mobile application does not perform application level acknowledgments, then it must rely on the

lower layers, namely the IP layer or radio network layer, to perform reliable message delivery.

To achieve optimal performance and reliable message delivery, it is important to minimize the number of layers performing acknowledgments. If the application performs application level acknowledgments, the recommended choice is UDP type sockets and radio network unconfirmed delivery mode. If the mobile application does *not* perform acknowledgments, the recommended choice is TCP type communication and radio network unconfirmed delivery mode.

From testing and experience, it is possible to stream data to an RNC3000 faster using the unconfirmed mode than using confirmed mode. The faster streaming of data produces better application performance and fewer TCP/IP retransmissions. Reliable message delivery can be handled either by the application layer or by using TCP/IP at the IP layer.

So, we recommend to use unconfirmed delivery in any case. But keep in mind, if you do that, you must set the *RNC3000 Maximum Transmission Unit* parameter to 512 or the communication will fail in certain applications, for example an FTP file transfer of several kilobytes.

2.5.7 Broadcast Messages

Some radio networks support broadcasting of messages to all radio modems in coverage with one packet transmitted. This feature can be used to transmit single messages to all of the clients. These messages will either be routed to an application specially listening for these messages on the client or they can be displayed in the status window of the eNetwork Wireless Client.

The broadcast mechanism is not integrated in the normal routing function of the eNetwork Wireless Gateway. The gateway listens to a specific UDP port for broadcast messages to be transmitted. On the gateway, there exists a command line interface to transmit these messages. However, the programming interface is specified, so that other applications on other computers can easily issue broadcast messages.

Broadcast messages are directed to a UDP port at the client computer. If an application listens on this UDP port on the client, it will get the message. If the broadcast message is sent to port 0, it will pop-up in the eNetwork Wireless Client message window.

Chapter 3. Install, Configure and Manage the Wireless Gateway

In this chapter we describe the installation, configuration and management of the eNetwork Wireless Gateway using AIX SMITTY, the TTY interface of the AIX system management tool. You may also use SMIT which is X-Windows based, because the same menus are also available. We also cover the management of the eNetwork Wireless Gateway using *Tivoli NetView for AIX*.

This chapter also includes sections which describe how to prepare the computer for running the eNetwork Wireless Gateway, such as X.25 adapter and asynchronous serial line configuration, setting up the system to run as a TCP/IP gateway, including LAN adapter configuration.

In this redbook, we assume that the computer on which the eNetwork Wireless Gateway will run has AIX correctly installed. We also assume you that have agreements with providers for the wireless data networks to link the eNetwork Wireless Gateway to their network infrastructure. In the remainder of this chapter we refer to wireless data networks or radio networks as Radio Data Networks (RDN).

To successfully install and run the eNetwork Wireless Gateway software, follow the sequence outlined below:

1. Make sure that your system meets all requirements.
2. Set up the AIX operating system.
3. Prepare the system by configuring the wireline connections to the RDN providers.
4. Install the eNetwork Wireless Gateway software.
5. Create a *mobile network interface* and configure it for all of the RDNs you are connected to.
6. Register the wireless clients and define the *Mobile Connections*.
7. Start the gateway and check if everything comes up correctly.
8. Connect from a registered eNetwork Wireless Client to the gateway.

The following sections help you in these steps in describing how we installed and configured an eNetwork Wireless Gateway. As we did not configure all RDNs the gateway supports, you may refer to the product manuals for networks not described here.

Note

During the installation and configuration process, you must be logged in under the administrator account (**must have root privileges**).

3.1 eNetwork Wireless Gateway Requirements

This section describes the components required (both hardware and software) to successfully install and to configure IBM eNetwork Wireless Gateway.

3.1.1 Hardware Requirements

The following hardware is required to install and run the eNetwork Wireless Gateway software:

- RS/6000 with at least 64 MB memory and at least a 1 GB hard disk.
- A LAN adapter for connection to the enterprise IP network (intranet).

Note

Because the data from a CDPD or DataTAC/IP (ARDIS/TCP) network provider may be routed to the eNetwork Wireless Gateway over the Internet, we encourage you to use a second LAN adapter connected to your Internet service provider or RDN provider. This helps minimize the exposure of your intranet to the Internet. See also 6.4, "Security Issues" on page 164 for a discussion of this topic.

- An IBM X.25 co-processor card - only required if you are connecting the eNetwork Wireless Gateway to DataTAC-SCR (including ARDIS and Modacom-SCR) or Mobitex (RAM)¹ RDNs over an X.25 connection.
 - For MCA-bus RS/6000 machines, use the IBM X.25 Interface Co-Processor/2 card.
 - For ISA-bus RS/6000 machines, use the IBM X.25 Interface Co-Processor/1 card.
- Asynchronous adapter and modems, if you are connecting the eNetwork Wireless Gateway to a circuit-switched network using serial communication over analog lines, for example, PSTN, GSM, or AMPS. For larger installations you may need a modem pool to provide enough dial-in capacity.
- ISDN adapter, if you are connecting the eNetwork Wireless Gateway to GSM (PCS) via ISDN (V.110 protocol).
- To attach a Dataradio PMR network to the eNetwork Wireless Gateway, connect each Multi-Site Controller (MSC) using TCP/IP over Ethernet. Set up and test the network for connectivity to the MSC before configuring eNetwork Wireless Gateway and Client. Refer to other available documentation for configuring a connection to a Dataradio PMR Single Side Controller (SSC).
- To attach a Motorola PMR network to the eNetwork Wireless Gateway, connect each Radio Network Controller (RNC) using TCP/IP over Ethernet. Set up and test the network for connectivity to the RNC before configuring eNetwork Wireless Gateway and Client.

3.1.2 Software Requirements

The following system software is required to use the eNetwork Wireless Gateway (AIX file set names are provided in parentheses):

- AIX V4.1.5 or later (see also Appendix A, "System Requirements" on page 241)
- Base Operating System, level 4.1.5 (or later)

¹ The eNetwork Wireless Gateway SMIT configuration menus do not list RAM as a network provider. When configuring the eNetwork Wireless Gateway to connect to a RAM network, use the procedures and menus defined for Mobitex.

- TCP/IP Server (`bos.net.tcp.server`)
- TCP/IP Client (`bos.net.tcp.client`)
- AIXlink 1.1.3.0 (only needed if using an X.25 adapter):
 - AIXlink/X.25 Runtime Environment (`sx25.rte`)
 - AIXlink/X.25 Server Support (`sx25.server`)
 - AIXlink/X.25 NPI (`sx25.npi`)
 - AIXlink/X.25 Application Development Toolkit - COMIO Support (`sx25.adt.comio`)
 - AIXlink/X.25 COMIO Compatibility Support & Applications (`sx25.comio`)

Note

Both, *AIXlink/X.25 Application Development Toolkit - COMIO Support* and *AIXlink/X.25 COMIO Compatibility Support & Applications* are optional but they allow you to perform X.25 problem determination.

- X.25 adapter software (only needed if using an X.25 adapter):
 - X.25 CoProcessor/1 Adapter Software for ISA Bus Machine
 - X.25 Coprocessor/2 or Multiport/2 Adapter Software for MCA Bus Machine
- Program CD-ROM for the eNetwork Wireless Gateway

To use the eNetwork Wireless Network Management feature of the gateway, you must install Tivoli NetView for AIX Version 3 Release 1.2 on an AIX machine which will be used as the Network Management console. We encourage you to run Tivoli NetView for AIX and the eNetwork Wireless Gateway software on different computers. Note that Tivoli NetView for AIX requires other software components, for example, X-Windows. Refer to your NetView documentation to determine the exact software requirements for NetView.

3.2 Preparing the System

Before you install the eNetwork Wireless Gateway, you should setup the system properly to run the gateway code and set up the connections to the RDN providers.

You will get through the configuration process much quicker when you gather all information you need from other parties in advance (see checklist provided in 3.2.1, “Before You Start” on page 55). Persons to contact are your enterprise network administrator, the providers of connectivity to the RDN providers (X.25 and Internet access provider), and the RDN providers themselves. Additionally you will need information to register an eNetwork Wireless Client.

3.2.1 Before You Start

Here is a checklist listing the information you may want to gather in advance. Note, that if you do not understand all of these parameters, you may first read through the following chapters, where some of them are explained in more detail. Note also that you may only need a subset if you are only dealing with some of

the RDNs supported by the eNetwork Wireless Gateway. Here is the list grouped by connection types and the RDNs:

1. IP settings to access your the enterprise network - get these parameters from your network administrator:
 - Gateway's IP address and subnet mask
 - Default router
 - Network domain
 - List of domain name servers
2. X.25 adapter HW parameters (only if you have ISA X.25 adapters installed) - refer to hardware documentation:
 - Interrupt level
 - I/O address
 - Memory address
3. X.25 parameters (if connected to an X.25 network) - get these values from your X.25 network provider:
 - Local Network User Address (NUA)
 - Number of SVCs configured for this access line (see also note in 3.2.4.3, "Adding Ports to an X.25 Device" on page 63)
4. X.25 parameters (if X.25 over leased line is used) - get these values from your RDN provider:
 - Local Network User Address (NUA), if the RDN provider requires you to have a specific one configured (for example BellSouth for RAM, Mobitex).
5. IP settings to access RDN providers over the Internet - get these values from your Internet access/service provider. Note that the gateway may be directly connected to the RDN provider, for example, using IP over frame relay. In this case ask the RDN provider. In any case, you will need:
 - Gateway's IP address on the Internet and subnet mask
 - Default router
6. Information related to dial-in networks over PSTN - see PSTN access line definitions and hardware manuals:
 - The telephone numbers of your PSTN access lines
 - Information on PSTN-modem to be used including AT command list
 - Exact information about which access line leads over which modem to which serial port on the gateway machine
 - If you are using an ISA serial port adapter card, you will need the hardware settings, like interrupt level, IO address and memory address.
7. Information related to dial-in networks over ISDN - see ISDN access line definitions and hardware manuals:
 - Type of access line (base rate / primary rate access)
 - Telephone numbers assigned to this line

Note

We do not cover ISDN configuration in this version of the redbook.

8. DataTAC RDNs - get these values from your RDN provider:
 - RNG's X.25 address (may not be important over a leased line)
 - Some DataTAC providers use a host ID and password, which the gateway has to provide to access the RNG
 - Extended DataTAC address associated with the eNetwork Wireless Gateway or slot identifier - you will need this information for client configuration
9. Mobitex RDNs - get these values from your RDN provider:
 - X.25 address of the MOX
 - RMAN assigned to the eNetwork Wireless Gateway

The information required to register an eNetwork Wireless Client depends on the RDNs:

- LLIs of the DataTAC radio modems used by the clients
- MANs of the Mobitex radio modems used by the clients
- IP address of CDPD radio modems used by the clients
- Phone number for dial-in networks including country and area code

3.2.2 Setting the Language Environment

To view the SMIT or SMITTY help panels provided with the eNetwork Wireless Gateway, the language environment must be set correctly before installing the Gateway software.

Use the following command to determine the language environment:

```
# echo $LANG
```

To get an English installation this command should return either En_US or en_US. Otherwise make sure that it states the language version you want to have installed on the gateway. You may compare this setting with another AIX machine properly installed for your language or ask your AIX support.

Use the following steps to set the correct language environment:

1. Enter:

```
# smitty chlang
```

2. Choose *Select Set of Cultural Convention, Language, and Keyboard*.
3. Press F4 to view a list.
4. Select the language that applies to your environment and press Enter.
5. Log off and log on to make the changes take effect.

3.2.3 AIX System Resources

The eNetwork Wireless Gateway requires system resources, namely virtual storage and space on the hard drive. The following two sections help you to calculate what may be needed.

3.2.3.1 Determining the Virtual Storage Needed

Virtual storage is the sum of RAM and the paging space on disk storage. A recommended value of 30% to 50% virtual storage should be RAM and the rest may be paging space on the hard drive. The eNetwork Wireless Gateway uses approximately 4 MB of virtual storage regardless of the number of registered mobile clients. In addition, approximately 0.5 KB of virtual storage is required for each active mobile client.

To determine the amount of available paging space available in the system, use the following command:

```
# lspvs -a
```

If the value in the Size field is less than the recommended amount of space, use the following command:

```
# smitty chps
```

If you have several paging spaces configured you may be prompted to select one. Then a data entry panel is displayed as depicted below.

Change / Show Characteristics of a Paging Space

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]			
Paging space name	hd6		
Volume group name	rootvg		
Physical volume name	hdisk0		
NUMBER of additional logical partitions	[]		#
Use this paging space each time the system is RESTARTED?	yes		+

F1=Help	F2=Refresh	F3=Cancel	F4=List
Esc+5=Reset	Esc+6=Command	Esc+7=Edit	Esc+8=Image
Esc+9=Shell	Esc+0=Exit	Enter=Do	

Move the cursor to the NUMBER of additional logical partitions field and enter the number of additional partitions you want to add. Each additional partition increases the paging space by 4 MB. For example, to add 12 MB additional paging space, enter the value 3.

3.2.3.2 Determining the Disk Space Needed

The eNetwork Wireless Gateway uses less than 2 MB of disk space without logging. For each packet transmitted between the eNetwork Wireless Gateway and a mobile client, a 24-byte accounting record can be generated. In field testing, a typical active mobile client produced 250-500 packets per day, resulting in a requirement of 6-12 KB of disk space per mobile client per day. The eNetwork

Wireless Gateway can be configured to produce extended logging of internal events, but this additional logging can consume megabytes of disk space within a few minutes. A standard configuration that logs only errors and warnings might add several kilobytes per week to the log.

3.2.3.3 Determine and Set the Available Space in the /var Directory

The eNetwork Wireless Gateway by default puts all of its log and trace files in the /var directory. This is a very critical directory to the operation of the eNetwork Wireless Gateway which should be closely monitored.

Note

It is very important, that this directory does not reach 100% of its capacity.

Use the following command to determine the amount of free space in the /var directory:

```
df /var
```

The Free column displays the free space. The amount shown is the number of 512-byte blocks available.

Multiply the free value by 512 to determine the total amount of free space.

If the total amount of free space is less than 32 MB, use the following command to increase the free space:

```
# chfs -a size=+number_of_512_byte_blocks /var
```

For example, to increase the free space by 4 MB, enter:

```
# chfs -a size=+8192 /var
```

3.2.4 Configuring X.25 Support

In this section we assume that before configuring X.25 support the X.25 adapter card has been installed in the computer and the required AIX software to support X.25 has been loaded onto the machine. Refer to 3.1.2, “Software Requirements” on page 54 to find out the required software modules and to 3.3.1, “Installing eNetwork Wireless Gateway Product Files” on page 72 for installing AIX software.

X.25 connections will be used to connect the eNetwork Wireless Gateway to the following RDN providers:

- DataTAC-SCR (including ARDIS and Modacom)
- Mobitex

If you are not configuring one of these radio networks, you may skip the rest of this section.

There are several steps that you will need to execute in the correct sequence to successfully connect the gateway machine to an RDN provider over X.25.

It starts with having the hardware configured correctly. If you are using a machine with an ISA bus, be sure to have the interrupt Level, bus I/O address and bus memory address available. See 3.2.4.1, “Add an X.25 Adapter (ISA Bus Only)” on

page 61 for details. Follow the instructions in the manual to install the hardware (should have been done already).

Note

Setting up the eNetwork Wireless Gateway to connect to RDN providers over X.25 is one of the most difficult steps. It rarely works the first time. Note that this is not your fault. Don't hesitate to contact your X.25 network provider in case of problems. They are able to determine whether your X.25 port is active and they may provide further assistance. If you are using a leased line, contact the RDN provider.

The lowest software module that interfaces the X.25 hardware is the *X.25 device driver*, which has to be added for each card. No configuration is needed for this module.

X.25 adapter hardware may contain several physical X.25 ports, meaning you could connect several cables going to different X.25 modems, the same way that you may have several serial ports on a serial adapter card. However, X.25 adapters today only have one port. Since the X.25 device driver supports adapters with several ports, the X.25 interface-to-application software has to be connected to a physical port of the adapter. This is done by adding an X.25 port to the X.25 device. Once this port has been created, X.25 parameters can be configured for it like local X.25 address and data transmission parameters.

The following sections describe this procedure in more detail. They all assume that you are starting from a point, to which the procedure below brings you.

From the AIX command prompt start SMITTY using the following command line:

```
smitty commodev
```

Depending on the machine type you have (ISA or MCA bus) select from the screen that appears for your X.25 adapter. For MCA machines it is:

```
X.25 CoProcessor/2 or Multiport/2 Adapter
```

For ISA bus machines select:

```
X.25 CoProcessor/1 Adapter
```

Press Enter on the appropriate selection. On the screen that appears you select **Adapter** and press Enter. This leads you to the screen below which is the base menu from where all following sections except 3.2.4.1, "Add an X.25 Adapter (ISA Bus Only)" on page 61 start.

Adapter

Move cursor to desired item and press Enter.

List All X.25 CoProcessor/2 or Multiport/2 Adapters
 Manage Device Drivers for X.25 CoProcessor/2 or Multiport/2 Adapters
 Generate Error Report
 Trace an X.25 CoProcessor/2 or Multiport/2 Adapter

F1=Help F2=Refresh F3=Cancel Esc+8=Image
 Esc+9=Shell Esc+0=Exit Enter=Do

3.2.4.1 Add an X.25 Adapter (ISA Bus Only)

For AIX computers having an ISA bus, the interrupt level, I/O address and memory address are set on the card using DIP switches that must match the device driver settings. You may have to open the computer case to verify or change the settings. Note, that if you are using more than one adapter, these settings must differ.

Table 1. X.25 Adapter Hardware Settings

Adapter	1	2
Interrupt	11	7
IO address	0x2a0	0x6a0
Memory address	0xE0000	0xE2000

There are two default settings, one for the first X.25 adapter in the system and one for the second X.25 adapter as shown in Table 1 on page 61, but it is important that you know for sure what the settings are on the adapter card. It is therefore a good idea to record the DIP switch settings before installing the X.25 adapter into the computer.

While for MCA machines the X.25 adapter is automatically recognized by the AIX operating system, you have to do this manually on an ISA machine using SMITTY. To add an X.25 adapter to an ISA bus system, start SMITTY from the AIX command prompt using the following command:

```
smitty commodev
```

Follow the selections below:

```
X.25 CoProcessor/1 Adapter
Add an X.25 Adapter
```

Then a list of available ISA bus card configurations is displayed. Select the one that fits your adapter settings and press Enter to display the data entry panel.

Make sure the values in the hardware settings match exactly (should be the case on default configurations). Otherwise, you will need to make any changes at this time.

Press Enter. If AIX detects an interrupt or address conflict it will warn you. If everything is ok, you may have to re-boot your computer.

3.2.4.2 Add an X.25 Device Driver

This section describes how to add an X.25 device driver for each X.25 adapter which has been successfully added and recognized by the operating system.

1. To make sure that the X.25 adapter for which you are defining a device driver is correctly installed, select:

```
List All X.25 CoProcessor/2 or Multiport/2 Adapters.
```

Note

In the selection above and some to come for both MCA bus and ISA bus machines the same entry is displayed, even if an ISA machine has an X.25 CoProcessor/1 Adapter installed.

For each X.25 adapter installed in the system, you should get a message, stating that the adapter is *Available*. The example below displays two successfully installed X.25 CoProcessor/2 adapters:

```
ampx0 Available 00-02 X.25 CoProcessor/2 Adapter
ampx1 Available 00-03 X.25 CoProcessor/2 Adapter
```

The names of the adapters may vary according to your system. If the adapters you have installed are not available, either the AIX operating system did not recognize these adapters or there may be an interrupt conflict. Check interrupt settings and whether you have installed all X.25 software components. Refer also to the manuals that came with the card.

2. Press F3 to return to the *Adapter* screen, which is the base SMITTY menu for the sections dealing with X.25.
3. Follow the selection sequence below:

```
Manage Device Drivers for X.25 CoProcessor/2 or... Adapter
Manage X.25 LPP Device Driver
Add a Device Driver
```

After pressing Enter, a list of available adapters is displayed. They may have names like *ampx0* or *ampx1*.

4. Select an adapter used by the eNetwork Wireless Gateway and press Enter to add a device driver for this adapter.
5. Repeat these steps for every adapter used by the eNetwork Wireless Gateway.
6. To verify that the X.25 device drivers are configured correctly, choose:

```
Manage Device Drivers for X.25 CoProcessor/2 or... Adapter
Manage X.25 LPP Device Driver
List All Configured Device Drivers to a CoProc... Adapter
```

The response shows that the device drivers have been successfully added (status *Available*):

```
twd0 Available 00-05-00 ARTIC Adapter Driver
twd1 Available 00-06-00 ARTIC Adapter Driver
```

3.2.4.3 Adding Ports to an X.25 Device

In principal an X.25 adapter may have several X.25 ports like a a serial card may have several RS 232 or TTY ports. In that case you would have an *X.25 Multiport/2 Adapter*. Since single-port and multi-port adapters are supported by one device driver, you have to add an X.25 port to an X.25 device driver even if there is only one port.

1. From the base SMITTY menu, follow the selection sequence below:

```
Manage Device Drivers for X.25 CoProcessor/2 or... Adapter
  Manage X.25 LPP Device Driver
    Manage X.25 Ports
      Add Port
```

2. Select the X.25 device driver, for example, **twd0** and press Enter.

You will get the following screen:

Add an X.25 Port

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
Parent Adapter Driver	twd0
* PORT number	[]
* Local network user address (NUA)	[]
* Network identifier	[other public]
Country prefix	[]
PVC - lowest logical channel number	[0]
PVC - Number of logical channels	[0]
Incoming SVC - lowest logical channel number	[0]
Incoming SVC - number of logical channels	[0]
Two-way SVC - lowest logical channel number	[1]
Two-way SVC - number of logical channels	[1]
Outgoing SVC - lowest logical channel number	[0]
Outgoing SVC - number of logical channels	[0]

F1=Help	F2=Refresh	F3=Cancel	F4=List
Esc+5=Reset	Esc+6=Command	Esc+7=Edit	Esc+8=Image
Esc+9=Shell	Esc+0=Exit	Enter=Do	

3. Enter the X.25 port number, which is 0 (zero) for all single-port adapters and enter the *Local Network User Address* (local NUA) assigned to the X.25 access line to which this adapter is physically connected. **Either the X.25 network provider or in case of connections over a leased line, the RDN provider supplies this value.** Check also that the other parameters match the definition of your access line. Look at the request form for these values.

Note

You need at least one two-way SVC configured for each connection to a radio network provider over a real X.25 network. It is useful to have one additional SVC configured for testing X.25 connectivity while the gateway is running.

4. For the field *Network Identifier*, enter the X.25 network you are connected to. Select this from the list by pressing **F4**. If you find your network not to be listed

you may select *other public* or if you are connected over a leased line you may select *other private* as we did. If you have problems in finding the correct value, **contact your X.25 network provider**.

5. If the eNetwork Wireless Gateway is using more than one X.25 adapter, return to the base SMITTY menu and start over from step 1 and repeat this procedure for each installed adapter.
6. To verify that the X.25 device drivers are configured correctly, choose:

```
Manage Device Drivers for X.25 CoProcessor/2 or... Adapter
Manage X.25 LPP Device Driver
Manage X.25 Ports
List All Defined Ports
```

The response may look like this:

```
sx25a0 Available 00-05-00-00 X.25 Port
sx25a1 Available 00-06-00-00 X.25 Port
```

The status should be *Available*.

3.2.4.4 Configuring an X.25 Port

You may want to review or change the configuration of an X.25 port.

Do this by starting from the base SMITTY menu, and following the selection sequence below:

```
Manage Device Drivers for X.25 CoProcessor/2 or... Adapter
Manage X.25 LPP Device Driver
Manage X.25 Ports
Change / Show Characteristics of Port
```

A shortcut from the command line would be:

```
smitty x25str_mp_csp
```

You will get the following selections:

```
Change / Show General Parameters
Change / Show Packet Parameters
Change / Show Frame Parameters
Change / Show Default for Permanent Virtual Circuits
Manage Non-Default Permanent Virtual Circuit
```

The first selection would be the most important one, because it allows you to change the Network User Address (NUA). After selecting the set of parameters you want to edit, select an X.25 port. Figure 25 on page 65 shows how we configured the X.25 port to access our ARDIS provider via a leased line.

For Mobitex, only the following values differed:

Port name	sx25a0
Local network user address (NUA)	[15040522]

Refer to these settings as an example only.


```

Change / Show X.25 General Parameters

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                     [Entry Fields]
Port name                                sx25a1
Local network user address (NUA)         [999999]
COMIO - Address in call request/accept    [allow]
Enable DLPI interface ONLY                [no]
PVC - lowest logical channel number       [0]
PVC - Number of logical channels          [0]
Incoming SVC - lowest logical channel number [0]
Incoming SVC - number of logical channels [0]
Two-way SVC - lowest logical channel number [1]
Two-way SVC - number of logical channels [4]
Outgoing SVC - lowest logical channel number [0]
Outgoing SVC - number of logical channels [0]

X.32 Configuration
*****
Use X.32 XID Exchange                     [no]                +
X.32 XID Identity                         [ ]                  X
X.32 XID Signature                        [ ]                  X

Dial-Up Configuration
*****
Connection Type                           [Direct/Leased]      +
V25bis Call Establishment Method           [Addressed]          +
Phone Number or Address to Call           [ ]
Maximum Connection Delay                  [10]
Enable/Disable DSR Polling                [disable]            +
DSR polling timeout                       [30]                 #
[BOTTOM]

F1=Help          F2=Refresh          F3=Cancel          F4=List
Esc+5=Reset      Esc+6=Command      Esc+7=Edit         Esc+8=Image
Esc+9=Shell      Esc+0=Exit         Enter=Do

```

Figure 25. Configuring NUA to the X.25 Connection Interface

3.2.5 Installing and Configuring Serial Line Support

This section describes procedures for installing and configuring RS-232 asynchronous support for dial-up, namely, serial-line connections to the eNetwork Wireless Gateway. When configuring the eNetwork Wireless Gateway to connect with eNetwork Wireless Clients through the PSTN, AMPS, or GSM connection-oriented networks, use these procedures to configure dial-up support. These procedures do not apply to configuring an ISDN connection to GSM-ISDN.

Note

These procedures describe an example for configuring serial-line support to *Standard I/O Serial Ports 1 & 2 (S1 and S2)*. Your procedures depend on the type of adapter and the number of connections you configure.

3.2.5.1 Configure Defined Asynchronous I/O

When you want to use the standard I/O serial ports to be used by the eNetwork Wireless Gateway you first have to configure AIX for that.

To enable asynchronous I/O support in the AIX operating system follow the steps below:

1. At the command prompt, enter:

```
# smitty
```

2. Follow the selections below:

```
Devices
  Asynchronous I/O
    Change / Show Characteristics of Asynchronous I/O
      Configure Defined Asynchronous I/O
```

3. On the data entry panel, go with the default values and press Enter.

Note

If you are using, for example, a 128-port asynchronous adapter, you may have to go to smitty -> Devices -> Asynchronous Adapter to add the AIX device driver to support this device and configure it. You may refer to your AIX and adapter documentation.

3.2.5.2 Add the AIX TTY Devices Entries for Each Serial Line

Each eNetwork Wireless Client that accesses the eNetwork Wireless Gateway through a dial-up connection interfaces the gateway software through an AIX TTY device. After configuring your asynchronous adapter or the standard async I/O, a TTY device must be added for each physical serial port of the gateway machine. Here is how to add and configure one or more TTY devices:

1. From the SMITTY main menu follow the selections below:

```
Devices
  TTY
    Add a TTY
```

2. Select whether you want to have an RS 232 or RS 422 port. In our case select:

```
TTY rs232 Async Terminal
```

3. Then a list of async parent adapters is displayed which may look like the following:

```
sa3 Available 00-07-21 16-Port RAN EIA-232 for 128-Port Ad...
sa0 Available 00-00-S1 Standard I/O Serial Port 1
sa1 Available 00-00-S2 Standard I/O Serial Port 2
```

4. Select the adapter you wish to create a TTY device for and you will get a screen which may look like this:

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

```

[TOP]                                     [Entry Fields]
TTY type                                   tty
TTY interface                             rs232
Description                               Asynchro...
Parent adapter                             sa0
* PORT number                             []
Enable LOGIN                              disable
BAUD rate                                  [9600]
PARITY                                     [none]
BITS per character                         [8]
Number of STOP BITS                       [1]
TIME before advancing to next port setting [0]
TERMINAL type                             [dumb]
FLOW CONTROL to be used                   [xon]
OPEN DISCIPLINE to be used                [dtropen]
STTY attributes for RUN time               [hupcl,cread,brki>
STTY attributes for LOGIN                 [hupcl,cread,echo>
LOGGER name                               []
STATUS of device at BOOT time             [available]
TRANSMIT buffer count                     [16]
RECEIVE trigger level                     [3]
STREAMS modules to be pushed at OPEN time [ldterm]
INPUT map file                             [none]
OUTPUT map file                           [none]
CODESET map file                           [sbcs]

POSIX special control characters:

INTERRUPT character                       [^c]
QUIT character                            [^\]
ERASE character                            [^h]
KILL character                             [^u]
END OF FILE character                     [^d]
END OF LINE character                     [^@]
2nd END OF LINE character                 [^?]
[MORE...8]

F1=Help           F2=Refresh       F3=Cancel         F4=List
Esc+5=Reset       Esc+6=Command     Esc+7=Edit        Esc+8=Image
Esc+9=Shell       Esc+0=Exit        Enter=Do

```

Use the following guidelines to define the connection characteristics for each TTY:

- Fields marked with an asterisk (*) are required.
- *Port number* defines the serial async adapter port. You may press **F4** to get a list of available port numbers. For a 128-port adapter this may correspond to the number on the extension box starting with a zero.
- Set *Enable Login* to OFF (disable) to disable the getty process.
- Set *BAUD rate* to a value equal to or greater than the maximum line speed of the modem servicing the specified port. See also the modem's manual for a recommended baud rate.
- You can accept the default settings for all other parameters.

5. Finish the configuration of that TTY by pressing Enter.

6. Return to the TTY menu and select Add a TTY for each serial port you need to define.
7. When you finish defining your TTY devices, return to the TTY and select *List all Defined TTYs* to ensure that all the expected device definitions are present. It may look like this:

```
tty0 Available 01-J0-00-00 Asynchronous Terminal
tty1 Available 01-K0-00-00 Asynchronous Terminal
```

3.2.5.3 Configuring PSTN Modem Types

In order to give the eNetwork Wireless Gateway an idea which AT commands to use when communicating with the modem that is attached to the TTY device you assign a *PSTN Modem Type* to each TTY device which will be used by the gateway.

Note

Defining a PSTN modem type and assigning it to a TTY device is a function of the eNetwork Wireless Gateway software. So, configuring PSTN modem types can only be done after the eNetwork Wireless Gateway software is installed on that machine.

To keep things together, this is described here, actually before we describe the installation of the eNetwork Wireless Gateway software. So you read through this section now but do the configuration after installing the software.

eNetwork Wireless Gateway comes pre-configured with a list of modem types. So before you decide to add a new modem type, first check if your modem isn't already supported.

1. Start SMITTY from the command line by entering:

```
# smitty ARTour
```

or

```
# smitty artour
```

This will lead you to the SMITTY eNetwork Wireless main menu.

You can reach this panel also from the SMITTY main menu by choosing:

```
Communications Applications and Services
artour
```

From the eNetwork Wireless main menu follow the selections below:

```
Mobile Network Devices
PSTN Modem Types
```

The fastpath method from the command line would be:

```
smitty inetpstnmARTour
```

2. To list the already defined modem types, select:

```
List all PSTN Modem Types
```

If your modem can be found in the list you are finished with this section. When you configure the eNetwork Wireless Gateway you will assign one of these modem types to a TTY device when you are creating a *PSTN TTY Device* at the gateway.

3. If your modem is not in the list, enter F3 and select:

Add a PSTN Modem Type

The following data entry panel is displayed.

Add a PSTN Modem Type

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
PSTN Modem	[]
Cmd Mode Command	[+++]
Dial Command	[ATDT]
Reset Command	[ATSO=1E0M0Q0]
Hangup Command	[ATH0]
Command Suffix	[OD0A]
Command Timer	[1000]
Carrier Threshold Time	[0]

F1=Help	F2=Refresh	F3=Cancel	F4=List
Esc+5=Reset	Esc+6=Command	Esc+7>Edit	Esc+8=Image
Esc+9=Shell	Esc+0=Exit	Enter=Do	

Figure 26. Adding a PSTN Modem Type

4. Specify the AT commands according to the modem documentation. Since the AT command to reset the modem only uses standard AT commands, you only may have to add commands that are special to your modem to answer calls from your wireless dial-up network. You may want to verify that you can connect to his modem using two PCs, each running a terminal program. One is replacing the eNetwork Wireless Gateway and the other one tries to connect to this modem using the radio data network. **Test both dial directions.**

3.2.6 Configuring TCP/IP

This chapter explains how to configure the AIX TCP/IP component on the eNetwork Wireless Gateway so that this machine will be properly configured to run in the enterprise network (intranet). Since the eNetwork Wireless Gateway may also be connected to RDN providers like CDPD or DataTAC-TCP over the public Internet the configuration of a second IP interface is described.

Section 6.4, "Security Issues" on page 164 outlines how an eNetwork Wireless Gateway may be connected to an enterprise network and the Internet at the same time without creating a security leak problem.

Configuring TCP/IP to access an IP network (intranet or Internet) is done by creating an IP interface for a network adapter like a token-ring adapter or an Ethernet adapter. This, however, presumes that you already have a network adapter physically installed in the machine and this adapter is recognized by the operating system. Additionally you need the configuration parameters like an IP address, subnet mask, default router and domain name server information from your network administrator.

In our installation we used the following parameters:

- Host name: artdevgw5
- IP address: 9.67.131.119
- Network mask: 255.255.248.0
- Domain name server IP address: 9.67.128.3
- Host domain name: raleigh.ibm.com
- Default “gateway” address (default router for the intranet): 9.67.128.1
- Network interface (Ethernet, IEEE 802.3, or token ring): tr0
- Additional network interface parameters, which in our case was the ring speed of 16 Mbit/s for our token-ring LAN.

To configure the IP interface to the enterprise network, perform the following operations:

1. Collect IP and network information for the eNetwork Wireless Gateway (see above).
2. Start SMITTY. From the main menu make the following selections:

```

Communications Applications and Services
TCP/IP
Minimum Configuration & Startup

```

Alternatively you can also use the following command line:

```
# smitty mktcpip
```

3. Select the network interface (LAN adapter).
4. Configure the IP interface. An example may be our configuration which is shown below:

```

HOSTNAME                               [artdevgw5]
Internet ADDRESS (dotted decimal)     [9.67.131.119]
Network MASK (dotted decimal)         [255.255.248.0]
Network INTERFACE                       tr0
NAMESERVER
Internet ADDRESS (dotted decimal)     [9.67.128.3]
DOMAIN Name                             [raleigh.ibm.com]
Default GATEWAY Address                 [9.67.128.1]

```

Note

Specify all portions of the network mask a.b.c.d (for example, 255.255.255.0 is a valid address, 255.255.255 is not).

5. Enter **yes** in the field *START Now*.
6. Press Enter to finish the configuration. The IP interface should now be successfully started or modified.
7. Test the IP interface by using the *ping* command. Use a known IP address (numeric values) in the same subnetwork first, then try a machine which is located outside of the subnetwork and then check the name server by entering host names in the same domain and in other domains.

Configuring the second IP interface to access the Internet is very similar to the first one. Below you find an example of how we configured our second interface to connect to the CDPD network provider:

```

HOSTNAME                                [artdevgw5]
Internet ADDRESS (dotted decimal)      [32.97.<a>.<b>]
Network MASK (dotted decimal)         [255.255.255.224]
Network INTERFACE                       tr1
NAMESERVER
    Internet ADDRESS (dotted decimal)  []
    DOMAIN Name                         []
Default GATEWAY Address                 [32.97.<a>.<c>]
(dotted decimal or symbolic name)
RING Speed                              [16]
START Now                               no

```

Notes

A TCP/IP host normally has a single Domain Name Server list. The fields defining the local domain and domain name servers may be left blank on the configuration of an IP interface used to connect to RDN providers. This assumes you have properly configured these parameters on the intranet IP interface.

In our example we put <a>, , and <c> instead of the real numbers because these addresses are real IP addresses visible on the Internet.

Again, test the IP interface by issuing *ping* commands to known IP hosts on the Internet including the RDN provider. Check with your RDN provider whether the machine the eNetwork Wireless Gateway connects to is configured to answer ping requests.

3.2.7 Enabling the Portmap Daemon for Automatic Startup

The eNetwork Wireless Gateway software uses RPC communication mechanisms which require a portmap daemon to run. The portmap daemon allows an application program to register for incoming traffic on a specific IP port. It listens for incoming IP connections or UDP packets and routes them to the appropriate application program.

The port mapper must be running when the eNetwork Wireless Gateway is started for the gateway to operate correctly. The best way to achieve this is to automatically start the portmap daemon at system boot time. You must configure this manually following the procedure below:

1. Load the file */etc/rc.tcpip* into the *vi* editor by typing at the command line:

```
vi /etc/rc.tcpip
```

You must have root permissions to do this. We strongly encourage you to use *vi* even if this editor is not a very user friendly one. However, other editors may add extra control characters to the file or may break file links.

2. Locate the portmap entry by entering.

```
/portmap
```

This should place the cursor on a line that looks like this:

```
# start /usr/sbin/portmap
```

3. Remove the “#” from the beginning of the portmap entry. (The # in column 1 indicates that the line entry is only a comment and is not to be executed.)

In command mode move the cursor to the # character and press the **x** key to delete the # character (press Esc to toggle between text-entry mode and command mode).

4. Save and close the file. Toggle to command mode and type “:wq”.

After doing this, you may start the portmap daemon from the command line:

```
# startsrc -s portmap
```

and proceed with the installation of the eNetwork Wireless Gateway. Otherwise you will have to re-boot the machine to get the portmap daemon started.

Note

It is imperative for the proper operation of the eNetwork Wireless Gateway that the portmap daemon is running.

3.3 Installing and Removing eNetwork Wireless Gateway Product Files

This section describes how to install and remove IBM eNetwork Wireless Gateway software.

3.3.1 Installing eNetwork Wireless Gateway Product Files

The eNetwork Wireless Gateway software package is built using the program *installp* and may be installed using SMIT installation menus. The IBM eNetwork Wireless product files contain the eNetwork Wireless Gateway including message support, and the eNetwork Wireless Network Management software. The program images are organized as follows:

- eNetwork Wireless Gateway program code (artgw).

This category contains all program code including the code support for all radio data networks supported by the eNetwork Wireless Gateway.

- eNetwork Wireless Gateway SMIT menu text and help (artgw.msg.En_US and artgw.msg.en_US and other languages).

This category contains all the SMIT panel and help text included with and used by the eNetwork Wireless Gateway program code.

Note

The message files include information critical to configuring the eNetwork Wireless Gateway. Because this information is NOT described in this book, install the entire category of message files.

- eNetwork Wireless Network Management (artnwm)

This category contains all the program files required to enable network management support for the eNetwork Wireless Gateway.

eNetwork Wireless Network Management is an extension of Tivoli NetView. To install eNetwork Wireless Network Management, you need root access to the Network Management console where Tivoli NetView is installed. Exit the NetView user interface before you execute the install program.

Note

Do not install this component on the machine running the eNetwork Wireless Gateway. Install this module on your Network Management console running Tivoli NetView for AIX.

You can install the eNetwork Wireless Gateway program files selectively or all at once. To reduce the number of parameters in the SMITTY configuration menus, install only the files for the RDNs that you expect to use. This also saves installation time and avoids potential operational confusion. If you lack experience for installing products on AIX, you may install all components.

The following procedure shows how to install the eNetwork Wireless Gateway software:

1. Make sure that you are logged in under the *root* account.
2. Insert the product media (CD ROM) in the appropriate drive.
3. Start SMITTY using the following command line:

```
# smitty install
```

Follow the selections below:

```
Install and Update Software
  Install/Update Selectable Software
    Install Software Products at Latest Level
      Install New Software Products at Latest Level
```

4. In the dialog panel, press **F4** to choose the device type from which you are installing the eNetwork Wireless Gateway, which normally is the CD ROM drive.
5. In the next dialog panel, move the cursor to the field *SOFTWARE to install* and press **F4** to view the list of program files on the device.
6. Use **F7** to choose the entries you need in each category (artgw*.*)). Select your language for the message support category (for US English you would select artgw.msg.En_US and artgw.msg.en_US). In most cases you would not want to install the artnwm component (eNetwork Wireless Network Management) on the gateway machine.
7. To start the installation process press Enter.

For the eNetwork Wireless Gateway, the install program allocates the directories and subdirectories and copies the program files to the directories.

When you install eNetwork Wireless Network Management (usually on the Network Management console machine), the install program does the following:

- Copies the following files to the /usr/OV/bin directory:

artourmgr

The executable file that provides the radio network topology.

artour_devinfo

The file for retrieving and setting device information.

artour_devsearch

The file for searching devices and their connections.

- Copies the following registration and configuration files to various directories:
 - artourmgr.reg
 - > /usr/OV/registration/C (application registration)
 - artourmgr.symbols
 - >/usr/OV/symbols/C (symbol definitions)
 - artourmgr.fields
 - > /usr/OV/fields/C (database fields)
 - bitmaps/*
 - > /usr/OV/bitmaps/C (symbol icon bitmaps)
- Copies the artour.gateways file to the /usr/OV/conf directory, if it is not already there.
- Installs all trap formats contained in the trapd.conf.inst file.
- Loads MIB definitions from ARTourMIB.my into the NetView MIB database.
- Starts the NetView database daemon ovwdb.
- Installs the new database fields.
- Compiles the symbol icon bitmaps.

3.3.2 Installing CSDs

CSDs which are updates to a specific version of the eNetwork Wireless Software are currently shipped as a full blown installation CD ROM. This makes no difference in installing a CSD on eNetwork Wireless Gateway or upgrading to a new version. You may follow normal installation procedures. The configuration information will be retained.

Note

Stop the eNetwork Wireless Gateway before upgrading it.

3.3.3 Removing eNetwork Wireless Gateway Product Files

eNetwork Wireless Gateway product files should only be removed using SMIT or SMITTY. Use the following procedure to remove the eNetwork Wireless Gateway software:

1. Make sure that you are logged in under the *root* account.
2. Start SMITTY using the following command line:

```
# smitty install
```

Follow the selections below:

```
Maintain Installed Software
Remove Software Products
```

Use the dialog panel to specify the software components to remove.

3. To remove all eNetwork Wireless Gateway software, SMIT menus, and customized mobile network interfaces, specify **artgw** in the field *SOFTWARE name*.

To selectively remove eNetwork Wireless Gateway components:

- Press **F4** to view a list of installed software products.
 - Scroll to the eNetwork Wireless Gateway components prefixed with the letters “artgw” and use **F7** to select the individual components you want to remove.
 - Press Enter and the selected components are displayed in the *SOFTWARE name* field.
4. Specify **no** in the field *PREVIEW only* and press Enter.

3.3.4 Upgrading from Earlier Versions

In principle the eNetwork Wireless Gateway software allows you to upgrade from previous versions and migrates the old configuration into the newer one. Please note, that up to version 2.x, which had the name *ARTour Version 2.x*, all configuration data has been stored in a flat file */etc/ARTour.route*, while the newer version places this information in the AIX ODM database. When you are upgrading from a 2.x version, the install program takes the information from the *ARTour.route* file and puts it into the ODM database. However, when you are downgrading, configuration information is not converted to the older one. Therefore, de-install the eNetwork Wireless Gateway before installing an older version on the same machine. In this case you will lose all configuration information.

Note

Make a system backup before upgrading a previous version of the eNetwork Wireless Gateway. This allows you to go back to the previous version quickly in case of problems.

Overwriting the eNetwork Wireless Gateway software with a previous version may eventually lead to a complete loss of configuration information.

On Version 2.x it is also a good idea to save the *ARTour.route* file.

3.4 Configuring the eNetwork Wireless Gateway

In this section we describe how to create a mobile network interface and understand the overall procedures used to configure connections to the RDN provider and to register mobile clients and mobile client connections.

To allow users with different application needs (for instance, for transmission costs, coverage, or devices) to select the best suited radio data network for each, the eNetwork Wireless Gateway and Client integrates access to different RDNs through a single mobile network interface.

The mobile network interface is the interface through which the IP layer communicates with all supported RDNs. IP forwards all packets with IP

addresses belonging to mobile units over this network interface. It is similar to an IP LAN interface, but although a single physically existing LAN is the basis for an IP LAN interface, the mobile network interface abstraction hides a set of different RDNs. To logically separate different user groups inside the eNetwork Wireless Gateway, more than one mobile network interface can be set up.

In this section we will describe the configuration of an eNetwork Wireless mobile network interface connected to ARDIS, Mobitex, PSTN and CDPD as we did for a test installation. We changed the mobile network interface configuration parameter and added a mobile client connection for each type of RDN.

Before you start to create a mobile network interface, look at a parameter common to all connections to RDN providers over X.25. This is the *Reset Delay Timer Interval* and the next section explains how this parameter should be set.

3.4.1 Defining X.25 Reset Delay Timer Interval

The X.25 Reset Delay Timer is a timer within the eNetwork Wireless Gateway that is used when terminating an X.25 connection to the RDN provider. Termination of an X.25 connection happens for example when the gateway goes down.

The X.25 Reset Delay Timer controls the interval between the time at which the gateway sends an X.25 packet over an SVC to the mobile clients, for example a “GW down” message, and the time at which it terminates the X.25 SVC by sending an X.25 close packet. Having connection termination delayed allows the X.25 network to successfully deliver the last eNetwork Wireless Gateway message to the RDN provider.

The default delay is 100 milliseconds which might be sufficient for your operating environment. However, if network monitoring reveals that one or more mobile devices indicate a connected state after a shutdown is issued, increase the interval to allow sufficient time for data to clear and for the mobile devices to receive the proper shutdown notification.

Since the X.25 Reset Delay Timer is a parameter within the eNetwork Wireless Gateway and refers to a mobile network interface, it only can be changed after the Gateway software has been installed and a mobile network interface has been created.

To display the current value of the X.25 reset delay timer interval, enter:

```
lsattr -E -l mmi -a x25resetdelay
```

where `mmi` is the mobile network interface (for example, `mn0`) using the X.25 SVC connections. This command may result in the following output:

```
x25resetdelay 100 X.25 Reset Delay True
```

The sample output shows the value “100”, indicating that the value is set to 100 milliseconds.

To change the current value of the reset delay timer interval, enter:

```
chdev -l mmi -a x25resetdelay=interval_value
```

where:

mni is the mobile network interface (for example, mn0) using the X.25 SVC connections.

interval_value is the number of milliseconds that the eNetwork Wireless Gateway waits before resetting and clearing an SVC connection. Specify a value ranging 0-1000 milliseconds. The default value is 100 milliseconds.

For example, to set the delay timer to 120 milliseconds enter:

```
chdev -l mn0 -a x25resetdelay=120
```

3.4.2 Creating Mobile Network Interface

From an IP addressing point of view eNetwork Wireless Clients reside in a mobile network. When they connect to the eNetwork Wireless Gateway they establish a point-to-point connection, called a mobile client connection to the gateway's mobile network interface. All IP packets the client sends are routed to the IP address associated with the mobile network interface. This is regardless of the underlying RDN the client uses. For each RDN the eNetwork Wireless Gateway supports, it has to maintain a connection to that provider.

This section describes how to create a mobile network interface on an eNetwork Wireless Gateway machine. Section 3.4.3, "Configuring the Mobile Network Interface for the Desired Networks" on page 79 explains how to configure the connections to the RDN providers.

You may create several mobile network interfaces on one eNetwork Wireless Gateway, thus creating several IP address ranges (subnetworks). The eNetwork Wireless Gateway routes IP packets between the mobile networks and the enterprise network.

Note

If you want to enable wireless clients to access an enterprise network you normally want to create a single mobile network interface and configure connections to all radio network providers you want to support.

However, if you create several mobile network interfaces you will have to create one connection to a radio network provider for each mobile network interface. Radio network providers may charge you for every connection to them. For dial-in connections, you need distinct modem pools, since one serial port is dedicated to a specific mobile network interface.

A mobile network interface is identified by its IP address and a subnet mask for the mobile network. The company must legally own the IP network or subnetwork used for the mobile network and the routers in the enterprise network must have a route definition pointing the eNetwork Wireless Gateway for IP addresses belonging to the mobile network.

To prevent assigning the IP address of the mobile network interface to an eNetwork Wireless Client, assign the first IP address of the subnet to the mobile network interface. If you have a mobile network 9.68.150.0 with subnet mask 255.255.255.0 assign the value 9.68.150.1 to the mobile network interface.

To create a mobile network interface and configure common parameters not specific to RDN connections, follow the procedure below:

1. Start smitty by entering the following on a command line:

```
# smitty artour
```

and choose:

```
Mobile Network Interfaces
```

You may also use the following fastpath by entering:

```
# smitty inetARTour
```

For other alternatives to access eNetwork Wireless smitty menus refer to step 1 in 3.2.5.3, "Configuring PSTN Modem Types" on page 68.

2. Choose:

```
Add a Mobile Network Interface
```

A dialog panel is displayed showing default values for all types of RDNs the eNetwork Wireless Gateway supports. This this panel may depend on how you installed the gateway.

3. Enter a value in each field marked by an asterisk (*) in the left-hand margin. The values you supply in the other fields depend on which RDNs the eNetwork Wireless Gateway is connecting to and are described in 3.4.3, "Configuring the Mobile Network Interface for the Desired Networks" on page 79.

You may create the mobile network interface first without any connection to an RDN provider and later add the RDNs you need one by one. In that case fill in the mandatory fields only as shown in the example below.

```
Network Interface Name          mn0
INTERNET ADDRESS (dotted decimal) [10.10.1.1]
Network MASK (hexadecimal or dotted decimal) [255.255.255.0]
Maximum IP Packet Size          [4096]

PSTN Country Code                [1]
ISDN Country Code                 [1]
```

The field *INTERNET ADDRESS* specifies the gateway's IP address in the mobile network. This address, together with the *Network MASK* field, defines the mobile network.

Note that if the gateway supports dial-in networks, the Country Code fields are mandatory. Set the correct country codes now.

4. Press Enter to confirm the creation of the mobile network interface.

Note

In the example above, the IP address 10.10.1.1, an *unroutable* address, may be used in a test environment. Operational systems are normally configured with an IP address and subnet mask forming the mobile network domain (subnetwork or IP network).

Be aware that the eNetwork Wireless Gateway acts as a router between the mobile network and the enterprise network (intranet).

For proper operation, your enterprise IP routers must be configured to route IP packets, addressed to hosts located in the mobile network (the subnetwork defined by the mobile network interface) to the eNetwork Wireless Gateway intranet IP interface.

This is because responses to packets sent by mobile clients to intranet hosts need to be routed to the eNetwork Wireless Gateway to reach the client.

3.4.3 Configuring the Mobile Network Interface for the Desired Networks

You may configure the mobile network interface for all RDNs you want to support in one pass. An alternative is to configure one network at a time and test it immediately by creating a mobile client with a client connection over that RDN. You may select the corresponding section in 3.4.5, “Configuring Mobile Client Connections” on page 91 for information how to configure the corresponding mobile client connection information for the RDNs described below.

When you finish the creation of a mobile network interface, you may then change the RDN-specific default values by starting smitty with the following command:

```
smitty artour
```

and following the selections below:

```
Mobile Network Interfaces
Change / Show a Mobile Network Interface
```

You can also use the following fastpath command:

```
smitty chinetARTour
```

The following panel appears:

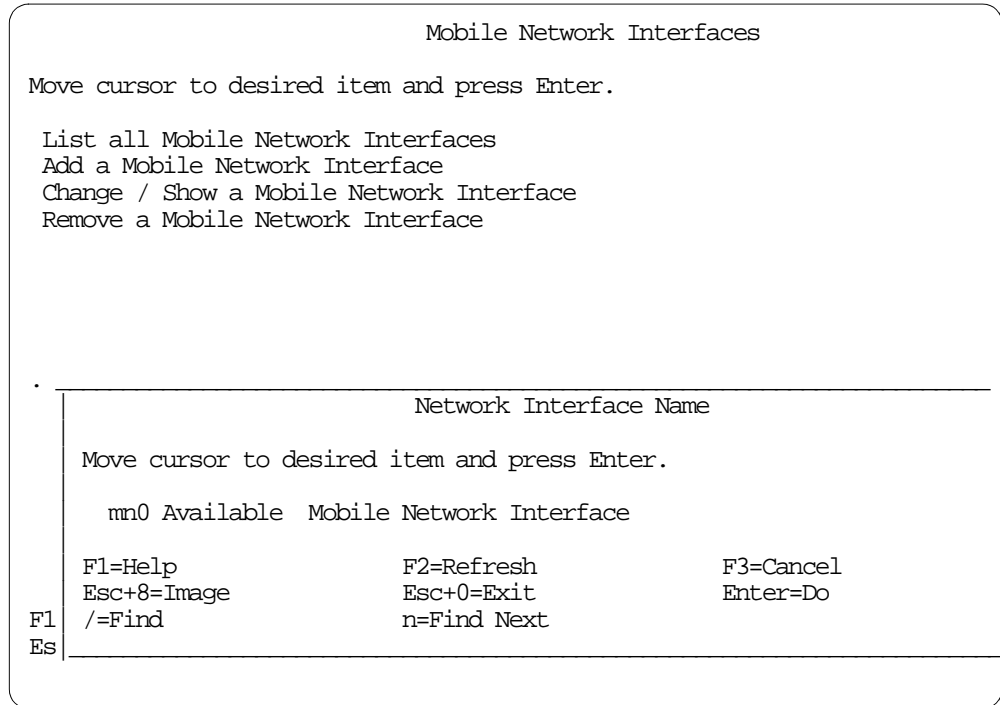


Figure 27. SMITTY Wireless Gateway and Client Mobile Network Interface Panel

Select the mobile network interface you want to change (for example *mn0*) and configure the connections to the RDN providers by changing the parameters prefixed by the RDN type. The following sections describe the RDNs we configured. To configure other RDNs refer to the manual.

Global connection parameters that apply to all RDNs are defined using the General ARTour Configuration menu.

In the following sections we assume that you have the *Change / Show a Mobile Network Interface* panel displayed for the mobile network interface you want to configure.

3.4.3.1 Configuring ARDIS Connection

In this section we will discuss how to configure an eNetwork Wireless Gateway through an ARDIS connection. You need to configure the connection between the X.25 adapter card to the ARDIS Radio Network Gateway (RNG).

This section assumes that the X.25 parameters are already configured including your own X.25 address as described in 3.2.4.4, “Configuring an X.25 Port” on page 64.

Note

The X.25 address of the ARDIS (or DataTAC) RNG is configured at the mobile client connection. This may be confusing, but it helps if you remember how the eNetwork Wireless Gateway works.

The mobile network interface defines the mobile (IP) network and associated hardware components. Connections to RDN providers for DataTAC and Mobitex networks are under the scope of a mobile client connection. As a consequence, an X.25 connection to the RDN provider is established only when there is at least one mobile client configured for that RDN.

To configure an eNetwork Wireless Gateway with an ARDIS connection, follow the procedure below:

1. Locate the ARDIS section on the *Change / Show a Mobile Network Interface* panel.
2. Select the X.25 adapter connected to your ARDIS provider. Press F4 to view a list of X.25 adapters from which you can choose. The adapter must already be installed in an “available” state and configured for connecting to your ARDIS provider. See 3.2.4, “Configuring X.25 Support” on page 59 for details on X.25 adapter configuration.
3. If you are using an X.25 network you may want to set the parameter *Ardis Reverse Charging* to **Yes** if agreed with your provider on that.
4. Try to go with the default values for any parameter which you are not sure how to set. In case of problems contact an X.25 specialist.

We used the adapter **sx25a1** to connect to America Mobile, our ARDIS provider over a leased line. Figure 28 on page 82 shows our configuration panel for the ARDIS mobile network interface.

```

Change / Show a Mobile Network Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...9]                                     [Entry Fields]
Ardis X.25 Adapter                             sx25a1
Ardis Fragment Time To Live (Seconds)         [120]
Ardis TCP Retransmit Interval (msec)          [30000]
Ardis Delivery Priority                         Medium High
Ardis Acknowledgment Indicator                Ack not required
Ardis Congestion Timer                        [120]
Ardis Hold Timer                              [120]
Ardis Maximum Transmission Unit                [2048]

Optional X.25 Facilities for Call Setup
Ardis Reverse Charging                         no
Ardis Packet Size for Received Data           []
Ardis Packet Size for Transmit Data          []
[MORE...204]

F1=Help           F2=Refresh           F3=Cancel           F4=List
Esc+5=Reset       Esc+6=Command       Esc+7=Edit         Esc+8=Image
Esc+9=Shell       Esc+0=Exit           Enter=Do

```

Figure 28. Configuring ARDIS X.25 Adapter Interface

3.4.3.2 Configuring a Mobitex Connection

To connect the eNetwork Wireless Gateway with the Mobitex network provider, you need a configured X.25 adapter card to connect to the Mobitex MOX.

Note

The X.25 address of the Mobitex MOX as well as the gateway's MAN address are configured at the mobile client connection. This may be confusing, but it helps if you remember how the eNetwork Wireless Gateway works.

The mobile network interface defines the mobile (IP) network and associated hardware components. Connections to RDN providers for DataTAC and Mobitex networks are under the scope of a mobile client connection. As a consequence, an X.25 connection to the RDN provider is established only when there is at least one mobile client configured for that RDN.

To configure an eNetwork Wireless Gateway with a Mobitex connection, follow the procedure below:

1. Select the X.25 adapter connected to your Mobitex provider. Press F4 to view a list of X.25 adapters from which you can choose. The adapter must already be installed in an "available" state and configured for connecting to your Mobitex provider. See 3.2.4, "Configuring X.25 Support" on page 59 for details on X.25 adapter configuration.
2. If you are using an X.25 network you may want to check the parameter *Mobitex Reverse Charging*. Common for Mobitex Networks is **No**.

3. Try to go with the default values for any parameter which you are not sure how to set. In case of problems contact an X.25 specialist.

We used the adapter **sx25a0** to connect to America Mobile, our ARDIS provider over a leased line. Figure 29 on page 83 shows the configuration panel of the Mobitex mobile network interface.

```

Change / Show a Mobile Network Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...106]                                     [Entry Fields]
Mobitex X.25 Adapter                             sx25a0
Mobitex Fragment Time To Live                    [120]
Mobitex Sequencing Fragment Time to Live         [5]
Mobitex TCP Retransmit Interval (msec)           [30000]
Mobitex Delivery Option                          Send once and quit
Mobitex Congestion Timer                         [120]
Mobitex Hold Timer                               [120]
Mobitex Keep Alive Timer                         [0]
Mobitex Maximum Transmission Unit                [512]

Optional X.25 Facilities for Call Setup
  Mobitex Reverse Charging                        no
  Mobitex Packet Size for Received Data          []
[MORE...107]

F1=Help      F2=Refresh      F3=Cancel      F4=List
Esc+5=Reset  Esc+6=Command  Esc+7=Edit    Esc+8=Image
Esc+9=Shell  Esc+0=Exit     Enter=Do

```

Figure 29. Configuring Mobitex X.25 Adapter Interface

3.4.3.3 Configuring eNetwork Wireless Gateway with PSTN Connection

In this section we discuss configuring PSTN connections on the eNetwork Wireless Gateway. Before you start, be sure that you have a modem type configured which suits your modems. You also need the PSTN phone number under which these modems can be reached.

Note

We encourage you to connect your modems to a PBX (Private Branch Exchange) and configure one phone number for the whole modem bank. The PBX should route incoming calls to the modems in a round robin manner and skip busy modems. Doing this, all clients share the modem pool because all of them dial the same number. Additionally, if one modem hangs and does not answer calls the next call will be routed to another modem.

The eNetwork Wireless Gateway divides a PSTN phone number into four fields:

- Country code
- Area code
- Company code
- Personal code

These fields refer to the ISO numbering scheme which many countries follow in Europe and Asia Pacific. However in the US a company code is normally not

known. In the following we briefly discuss these numbering schemes. This may help US readers to get the key to company codes and all of you to fill in the fields correctly.

In the US, all phone numbers have the same number of digits. The country code is 1 (one). They are written down in the following format:

+1-aaa-ppp-pppp

The area code (<aaa> in our example) has three digits. On a normal phone line you always have to dial the personal code (<ppp-pppp> in our example). When you reside in the same area as the party you wish to call you may omit the area code. If you are making a long distance call, you indicate that you are dialing an area code by preceding the area code with the digit "1". In eNetwork Wireless terminology this is called *PSTN Area Prefix*. To make an international call, you have to enter "011" then the country code, area code, and the rest. The digits to indicate an international call are called *PSTN Country Prefix*.

It is a coincidence in the US, that the digit "1" to mark a long distance call is also the country code in the US.

In Germany, for example, things are a bit different. The country code is "49". The number of digits on German phone numbers may vary. They are written down in the following format:

+49-aaaa-ccc-pppp

for a company on a PBX and

+49-aaaa-pppppp

for a private number.

Area codes (<aaaa> in our example, but may vary from 2 to 4 digits) have the same meaning as in the US. You don't have to dial them if you reside in the same area as the called party. Company codes are used when there is a PBX at the end of a public PSTN (or ISDN) line. Having a PBX, the personal code is assigned under the authority of the PBX while the company code is given by the telco company. For a private number, the telco company assigns the whole number following the area code.

If you are dialing a number within the same company you only have to dial the personal code (<pppp> in our example). To dial outside the company mechanisms differ. In many cases you have to dial a 0 (zero) to get a public line. The digits to dial to get a public line from within a company are called the *PSTN General Prefix*. Having access to a public line you either dial <ccc-pppp> to connect to another company or <pppppp> to get a private number. To make a long distance call in Germany you have to dial a 0 (zero) for the PSTN Area Prefix. To make an international call, the Country Prefix is "00" to indicate an international call then dial the country code, area code, and the rest. From within a company you may have to dial three zeros, one to get a public line (General Prefix), another two zeros (Country Prefix) to indicate an international call.

To configure PSTN connections to the eNetwork Wireless Gateway, you must have your TTY devices and modem types defined as described in 3.2.5, "Installing and Configuring Serial Line Support" on page 65.

The mobile network interface has several sections for dial-in connections:

- PSTN
- AMPS
- PCS
- GSM
- And maybe others

If your modems support calls from all dial-in networks you may configure one dial-in network only (for example PSTN as we did). If, however, you need different modems for example to accept calls from AMPS and PCS, you have to assign both network types to the corresponding TTY devices, thus resulting in two modem pools. In that case you also need to assign different PSTN numbers to each of the modem pools.

For each dial-in network you want to configure, in the mobile network interface definition you have to set the TTY devices and the PSTN country code, area code and optionally the company code. TTY devices may be selected from a list at the parameter *Serial Line Interfaces*. Then you have to set for each TTY device assigned to this dial-in network type a modem type and a local PSTN address, which is the personal code part of the PSTN phone number.

Now, here is the procedure to configure dial-in connections to the eNetwork Wireless Gateway:

1. Locate the PSTN line parameter block and configure the prefix values and the common phone number parts of your PSTN access lines. (In the US, always leave company code field empty.) An example is shown below:

```
Change / Show a Mobile Network Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...70]                                     [Entry Fields]

-----

PSTN General Prefix                             [9]
PSTN Country Prefix                             [011]
PSTN Area Prefix                                [1]
* PSTN Country Code                             [1]
PSTN Area Code                                  [919]
PSTN Company Code                              []

-----
```

These parameters have to be set for PSTN independently to which dial-in network you use. Don't be confused by having the term *PSTN* used twice, once for the PSTN access lines and second for the PSTN dial-in RDN.

2. Now, locate the parameter block for your dial-in connection network (they are functionally all the same, so you may choose the one you like).

It starts with a *Serial Line Interfaces* parameter for that type of network. Set this parameter to include a list of all TTY devices you want to assign to this RDN. Press F4 to view a list of TTY devices from which you can choose. The serial adapter must already be installed and must have the status "available".

In the example shown in Figure 30 on page 86, we entered **tty0** as the only serial device for this network.

```

Change / Show a Mobile Network Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...191]                                     [Entry Fields]

PSTN Serial Line Interfaces                       tty0
PSTN Allow Dial Out                               yes
PSTN Connect Timeout                             [0]
PSTN Min Redial Delay                             [1]
PSTN Max Redial Delay                             [15]
PSTN Min Time Idle                               [30]
PSTN Max Time Idle                               [60]

-----

AMPS Serial Line Interfaces
AMPS Allow Dial Out                               yes
[MORE...22]

F1=Help      F2=Refresh      F3=Cancel      F4=List
Esc+5=Reset  Esc+6=Command  Esc+7=Edit    Esc+8=Image
Esc+9=Shell  Esc+0=Exit    Enter=Do

```

Figure 30. Configuring PSTN Parameters on the Mobile Network Interface

1. You may allow or prevent the gateway from dialing eNetwork Wireless Clients by itself by setting the parameter *Allow Dial Out* accordingly.
2. Press Enter to finish the definition of the mobile network interface and return to the SMITTY artour main menu.
3. Now from the SMITTY artour main menu follow the selections below:

```

Mobile Network Devices
  PSTN TTY Devices
    Change/Show a PSTN TTY Device

```

A list of defined TTY devices is displayed.

4. Select the TTY device you want to configure by pressing F7 and then press Enter. The following panel appears:

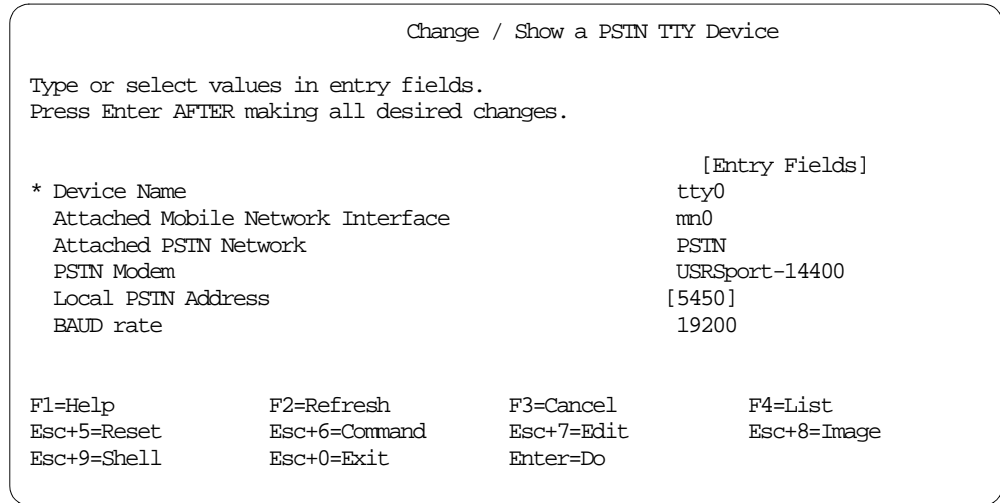


Figure 31. Applying Modem and Configuring Local PSTN Address

For a description of a specific parameter, move the cursor to the parameter and press F1 (Help).

5. Select the modem type from the list you get by pressing F4.
6. Set the *Local PSTN address* parameter to the individual phone number assigned to the PSTN line. If you are using a PBX having one number for the whole modem pool, don't use the common number, but the number which always gets you to that specific modem.
7. Check that the baud rate is set correctly.
8. Repeat this step for every TTY device used for the eNetwork Wireless Gateway.

Note

The panels for configuring the mobile network interface for dial-in networks and for configuring PSTN TTY devices allows you to set the same parameter using different methods. We encourage you to select the TTY devices at the mobile network interface definition and add the parameters *Modem Type*, *Local PSTN Address* and *BAUD rate* at the panel *Change / Show PSTN TTY Device* as described above. Note that in the latter panel, mobile network interface name and PSTN network type are also displayed and may be changed.

3.4.3.4 Configuring a CDPD Connection

In this section we will discuss how to configure CDPD parameters of the eNetwork Wireless Gateway's mobile network interface. You should have IP connectivity between the wireless gateway to the CDPD network (probably via the Internet) by configuring a second IP interface.

Note

For CDPD networks there is no Radio Network Gateway like in DataTAC or Mobitex networks. The eNetwork Wireless Clients are already visible on the Internet. eNetwork Wireless Gateway and Client have some sort of IP tunnel to provide secure and reliable access to enterprise networks.

To configure the eNetwork Wireless Gateway with a CDPD connection, follow this procedure:

1. Make sure that your TCP/IP interface connecting the gateway to the CDPD provider is configured correctly. See 3.2.6, "Configuring TCP/IP" on page 69 for details. You should be able to ping IP hosts (not eNetwork Wireless Clients) on the CDPD network from the gateway.
2. Make sure that you are on the smitty panel:
Change / Show a Mobile Network Interface
and locate the CDPD section.
3. Normally you do not have to change anything. Check that the parameters CDPD gateway UDP port and CDPD client UDP port to have the predefined values shown below. These names actually refer to UDP port numbers defined in the file `/etc/services`. See 3.4.6, "Advanced Configuration" on page 94 if you think you will have to change these settings.

```
Change / Show a Mobile Network Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...39]                                     [Entry Fields]

-----

CDPD GW UDP Port                               [ARTourCDPD-S]
CDPD Client UDP Port                           [ARTourCDPD-C]
CDPD Fragment Time To Live (sec)               [10]
CDPD TCP Retransmit Interval (msec)            [10000]
CDPD Maximum Transmission Unit                 [576]

-----

[MORE...67]

F1=Help           F2=Refresh           F3=Cancel           F4=List
Esc+5=Reset       Esc+6=Command       Esc+7=Edit         Esc+8=Image
Esc+9=Shell       Esc+0=Exit          Enter=Do
```

Figure 32. CDPD Mobile Network Interface Configuration Panel

3.4.4 Registering eNetwork Wireless Client

Only registered eNetwork Wireless Clients can use the eNetwork Wireless Gateway. That is, the eNetwork Wireless Gateway must know in advance which eNetwork Wireless Clients may connect. This section describes how to register

eNetwork Wireless Clients (mobile clients) to use the eNetwork Wireless Gateway.

This includes defining an IP address within the mobile network address space and assigning a host name for the eNetwork Wireless Client to be registered. The client's host name should be added to the gateway's hosts file in the *etc* sub-directory. This allows you to address the eNetwork Wireless Client by its name instead of entering the numeric IP address.

Note

If you want to enable IP hosts in the enterprise network to access eNetwork Wireless Clients by their host names instead of numeric IP addresses, someone has to register these names at the enterprise domain name server. This is normally done by your network administrator.

Additionally you have to specify if a password should be required for the client to log into the eNetwork Wireless Gateway (which we encourage you to do for every client), set the initial password and set the password parameters according to the security guidelines of your enterprise. Ask your network administrator if you need information about your enterprise's network security guidelines concerning password change periods, number of failed logins before an account is locked and password restrictions.

The definitions concerning the radio data networks, over which the eNetwork Wireless Client is allowed to connect to the gateway are performed by configuring a mobile client connection which is described in 3.4.5, "Configuring Mobile Client Connections" on page 91.

Before you add mobile clients you have to decide how to register the IP names in the */etc/hosts* file. There are two options:

1. Let the eNetwork Wireless Gateway configuration add the names to the hosts file in the *etc* sub-directory. This is the option we chose in our example.
2. Edit the hosts file manually by entering names and IP addresses of all mobile clients in one step and create new mobile clients at the gateway without specifying IP addresses. In that case the parameter *Add to /etc/hosts file?* must be set to **no**.

Note

To enhance gateway performance, use the local */etc/hosts* file for mobile client lookups. To achieve this, configure TCP/IP on the eNetwork Wireless Gateway to use the hosts file prior to asking the domain name server.

To add a new mobile client using option 1 as described above, follow the procedure below:

1. Start SMITTY by entering the command:

```
# smitty artour
```

and choose:

```
Mobile Client Configuration
```

Add a Mobile Client

2. Enter the name (IP host name) of the eNetwork Wireless Client. This is the only required parameter.
3. Enter the IP address of the mobile client in dotted decimal notation.
4. Set the parameter `Add to /etc/hosts file?` to **yes**.
5. Set the field `Password Required` to **yes** and set an initial password. This password is displayed on the panel. Communicate this password to the mobile user. The mobile user has to change the password when he or she logs into the gateway for the first time.

When creating an initial password, follow the current password rules to avoid giving a user an unusable password.

6. Check that the parameter `Is this ACCOUNT LOCKED?` is set to **false**. You may set this to **true** to prevent eNetwork Wireless Clients from connecting to the Gateway without removing them totally from the system.

Note

If a mobile user has entered a wrong password too often, you have to unlock the account **and** reset the failed login counter manually.

The Lock / Unlock parameter in the Change / Show a Mobile Client panel cannot be used for that purpose. Use the panels:

`Reset Mobile Client's Failed Login Count`

and

`Lock / Unlock a Mobile Client Account`

7. The other parameters deal with login security. You may modify the login security values for this client individually by changing them on this panel. To change the default security values, select Change / Show Security Defaults from the Mobile Client Configuration panel.
8. For information on a specific field, move the cursor to that field and press F1 to view help.

Below you find an example where we named the eNetwork Wireless Client to be **ARTTest** with IP address of **10.10.1.10**.

Note

Do **not** use the password displayed here! Everyone who reads this redbook will be able to guess this password.

```

                                Add a Mobile Client

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                [Entry Fields]
* Mobile Client                       [ARTTest]
  Internet ADDRESS (dotted decimal)   [10.10.1.10]
  Add to /etc/hosts file?              yes
  Data Tracing                          no
  Password Required                     yes
  Password                             [set214test]
  Is this ACCOUNT LOCKED?              false
  EXPIRATION Date (MDDdhmmyy)         []
  Number of FAILED LOGINS before       [5]
    user account is locked
  Number of PASSWORDS before reuse     [0]
  Password MAX AGE (days)             [0]
  Password MIN AGE (days)            [0]
  Password MIN LENGTH                  [6]
  Password MIN ALPHA characters        [2]
  Password MIN OTHER characters        [2]
  Password MAX REPEATED characters     [8]
  Password MIN DIFFERENT characters    [0]
  Password can CONTAIN USERID         true
  NUMERIC FIRST / LAST characters     true
[BOTTOM]

F1=Help           F2=Refresh           F3=Cancel           F4=List
Esc+5=Reset       Esc+6=Command       Esc+7=Edit         Esc+8=Image
Esc+9=Shell       Esc+0=Exit         Enter=Do

```

Figure 33. Add a Mobile Client Panel

When you change a mobile client definition you may set the parameter Administrative Change to **true** to force the client to change the password at the next login attempt. If the eNetwork Wireless Client is currently logged in, specifying true forces the client to log off the gateway.

3.4.5 Configuring Mobile Client Connections

Do not confuse adding an eNetwork Wireless Client with adding a connection to an eNetwork Wireless Client. Although you add an eNetwork Wireless Client only once, you can define multiple connections to multiple RDNs for a single eNetwork Wireless Client.

To add a connection for an existing eNetwork Wireless Client:

1. Start SMITTY by entering the command:

```
# smitty artour
```

and choose:

```
Mobile Client Configuration
  Manage Mobile Client Connections
```

2. Select:

```
Add a Mobile Client Connection.
```

3. Move the cursor to the RDN for which you want to define a connection and press Enter. A list of existing eNetwork Wireless Client names is displayed.

4. Move the cursor to the eNetwork Wireless Client for which you want to define a connection and press Enter. A dialog panel corresponding to the RDN you chose is displayed with the name of the eNetwork Wireless Client you chose in the mobile client field.
5. In this redbook we describe how to configure connections to ARDIS (but all DataTAC networks are very similar), Mobitex, PSTN and CDPD. Go to the corresponding section below to continue. To configure RDNs not covered here, refer to the manuals.

3.4.5.1 Client Connection over the ARDIS Network

When you select

```
ardis          (Standard Context Routing)
```

for the RDN and mobile client ARTTest, you see the following panel:

Add an Ardis Connection

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

	[Entry Fields]
* Mobile Client	ARTTest
* Ardis Gateway	[34525]
* Subscriber Unit Identifier	[EE811845]

F1=Help	F2=Refresh	F3=Cancel	F4=List
Esc+5=Reset	Esc+6=Command	Esc+7=Edit	Esc+8=Image
Esc+9=Shell	Esc+0=Exit	Enter=Do	

Figure 34. Configuring ARDIS Gateway and SUI

Enter the following parameters:

ARDIS Gateway This specifies the X.25 address of the DataTAC RNG.

Subscriber Unit Identifier Corresponds to the client's ARDIS modem identifier also referred as LLI.

3.4.5.2 Client Connection over the Mobitex Network

When you select

```
mobitex       (Mobitex International Standard)
```

for the RDN and mobile client ARTTest, you see the following panel:

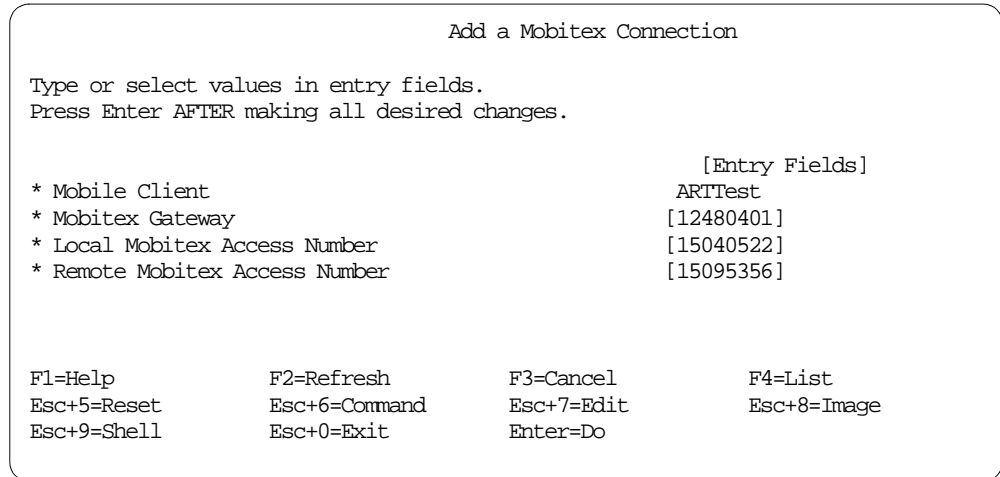


Figure 35. Configuring Mobitex Gateway, Local MAN and Remote MAN

Enter the following parameters:

- Mobitex gateway** This is the MOX X.25 address.
- Local MAN** This is the MAN address of the eNetwork Wireless Gateway (sometimes also the local X.25 address when you are connected over a leased line to the Mobitex provider).
- Remote MAN** This is the MAN number you find on the Mobitex modem.

3.4.5.3 Client Connection over the PSTN Network

When you select

PSTN (Public Switched Telephone Network)

for the RDN and mobile client ARTTest, you see the following panel:

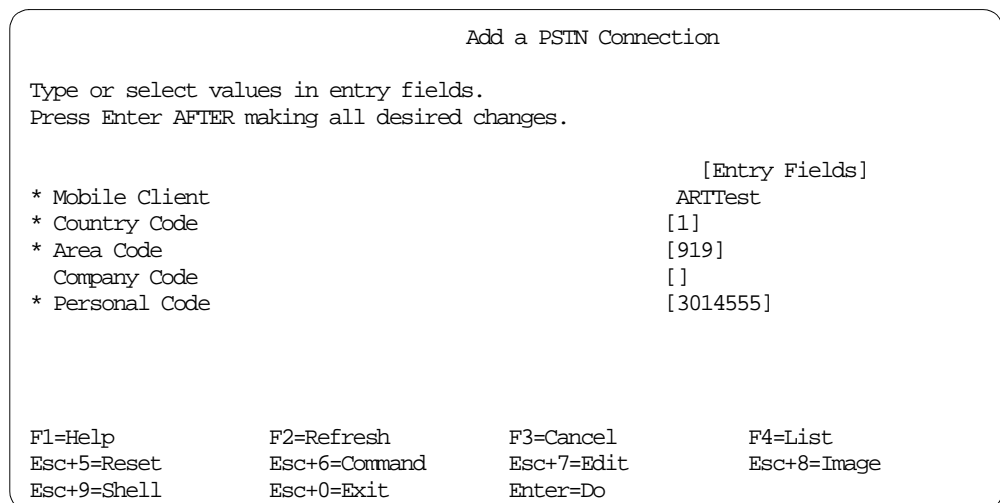


Figure 36. Configuring PSTN Mobile Network Connection

Enter the parameters for Country Code, Area Code, Company Code and Personal Code of the eNetwork Wireless Client's mobile phone number. See 3.4.3.3, "Configuring eNetwork Wireless Gateway with PSTN Connection" on page 83 for a description of these parameters.

3.4.5.4 Client Connection over CDPD Network

When you select

`cdpd` (Cellular Digital Packet Data)

for the RDN and mobile client ARTTest, you see the following panel:

Add a CDPD Connection

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* Mobile Client	[Entry Fields]
* CDPD IP-Address	art0m051 [9.167.23.44]

F1=Help	F2=Refresh	F3=Cancel	F4=List
Esc+5=Reset	Esc+6=Command	Esc+7=Edit	Esc+8=Image
Esc+9=Shell	Esc+0=Exit	Enter=Do	

Figure 37. Configuring CDPD Client IP Address

Simply enter the IP address of the CDPD modem used by the eNetwork Wireless Client.

3.4.6 Advanced Configuration

There is a huge number of parameters to be configured on the eNetwork Wireless Gateway. Aside from the parameters mentioned in the above sections, you may go with the default parameters. You may get more information about these parameters by pressing the help key or button when you are in the appropriate SMITTY screen.

There is, however, a special case which may be important to you.

As shipped, the UDP ports 8888 and 8889 are used by the eNetwork Wireless Gateway and Client software. Therefore applications running on the client or the gateway host should not use these ports.

If your application requires one of these ports, eNetwork Wireless allows you to configure these ports to avoid conflicts. Be sure to change these parameters consistently with all of the eNetwork Wireless Clients connecting to this gateway.

UDP port 8888 is used for password changes. Changes to this port number can be made in the General Configuration smitty panel. Be aware that a change on this port number will affect all clients for all configured mobile network interfaces.

UDP port 8889 is used for CDPD network connections. You can modify this parameter by changing the mobile network interface. To find the actual port number assigned to the port names, which may be configured in the SMITTY menu, you may check the file `/etc/services` on your machine.

Changing these values in the `/etc/services` file may be another method of changing UDP port numbers. This, however may easily confuse others checking your gateway configuration.

3.5 Starting/Stopping eNetwork Wireless Gateway

The eNetwork Wireless Gateway cannot be started or stopped as an application program. The gateway is present in its mobile network interfaces. You have to start and stop the mobile network interfaces in order to control the eNetwork Wireless Gateway software.

3.5.1 Starting a Mobile Network Interface

The current state field from the eNetwork Wireless Gateway SMITTY configuration menus controls the starting and stopping of each mobile network interface.

To start a mobile network interface, go to the SMITTY menu `Change / Show a Mobile Network Interface` for the specific MNI, set the current state field to up, and press Enter.

You may access this menu by entering the following command:

```
# smitty chinetARTour
```

and selecting the interface you want to start (we selected `mn0`).

As an alternative you may start smitty by entering:

```
# smitty ARTour
```

and select

```
Mobile Network interfaces
Change / Show a Mobile Network Interface
```

```

Change / Show a Mobile Network Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                [Entry Fields]
* Network Interface Name              mn0
* INTERNET ADDRESS (dotted decimal)   [9.67.140.1]
Network MASK (hexadecimal or dotted decimal) [255.255.255.0]
Maximum IP Packet Size                [4096]
Accounting                            all
Current State                          up

-----

Ardis X.25 Adapter                    sx25a1
Ardis Fragment Time To Live (Seconds)   [120]
Ardis TCP Retransmit Interval (msec)    [30000]
Ardis Delivery Priority                Medium High
[MORE...106]

F1=Help          F2=Refresh          F3=Cancel          F4=List
Esc+5=Reset      Esc+6=Command      Esc+7=Edit        Esc+8=Image
Esc+9=Shell      Esc+0=Exit        Enter=Do

```

Figure 38. Changing Current State Field to Start/Stop Mobile Network Interface

On re-booting the gateway machine, eNetwork Wireless remembers the state of its mobile network interfaces and therefore in order for a mobile network interface to start automatically at boot time, simply set the value of the field Current State to **up** for that mobile network interface.

After starting a mobile network interface, check that the eNetwork Wireless Gateway software starts up correctly.

You should receive a network management trap at Network Management console (running Tivoli NetView for AIX). On the gateway machine, see if the following processes are active:

- if_MNU-drive
- if_MNU-drive
- if_MNU-drive.SmuxD (only when SMUX daemon is enabled)
- if_MNU-drive.Acct
- if_MNU-drive.Trace
- if_MNU-drive.Log
- if_MNU-drive.ChPw
- if_MNU-drive.CfgMgr
- if_MNU-drive.Rcv.IO

In addition, depending on the configuration, these processes might also be active:

- if_MNU_drive.Snd.GSM.tty0
- if_MNU-drive.BcMc

You may also check the `artour.log` file for warning and error messages. Be sure to have the appropriate log file settings.

To check the actual status of a mobile client in eNetwork Wireless Gateway enter the following from the command line:

```
# lsARTour -devstatus
```

This shows you the connection status for each mobile client and if a client is connected, you may see what has been negotiated at the eNetwork Wireless protocol level.

3.5.2 Stopping a Mobile Network Interface

To stop a mobile network interface, go to the SMITTY menu *Change / Show a Mobile Network Interface* for the specific MNI, set the Current State field to **down**, and press Enter.

You may access this menu by entering the following command:

```
# smitty chinetARTour
```

See 3.5.1, “Starting a Mobile Network Interface” on page 95 for alternate methods to find this smitty panel.

You have to select the mobile network interface you want to stop before the panel comes up.

When the eNetwork Wireless Gateway is stopped, a trap is sent to the Network Management console (running Tivoli NetView).

Note

When you stop a mobile network interface of the eNetwork Wireless Gateway, all mobile users logged to that mobile network are disconnected. The gateway will try to inform the mobile users if possible.

This may result in errors on the application the mobile user is currently using. Check for logged in clients and try to inform them before shutting down a mobile network interface.

3.6 eNetwork Wireless Network Management

In this section we will describe how to configure eNetwork Wireless network management. We will also show how to monitor an eNetwork Wireless Gateway and its client connections using Tivoli NetView for AIX.

To use eNetwork Wireless network management, you must install Tivoli NetView for AIX Version 3 Release 1.2 on an AIX computer acting as a network management console, not in the machine running eNetwork Wireless Gateway software.

Although it is theoretically possible to run both, the eNetwork Wireless Gateway and Tivoli NetView on one computer, we recommend this for testing purposes

only. In a production environment the eNetwork Wireless Gateway software should run on a computer dedicated for this purpose, while the Network Management console would manage the whole enterprise network including the eNetwork Wireless Gateway and its client connections.

3.6.1 Configuring eNetwork Wireless Network Management

To configure eNetwork Wireless network management, go to the SMITTY menu General Configuration on the eNetwork Wireless Gateway and enable the generation of SNMP traps by starting the SMUX daemon. You will also have to specify one or several network management stations to which these traps will be sent. Finally you have to specify a log level for the trap generation because this is different from the log level used for file logging. Figure 39 on page 98 shows how we filled out this panel.

```

                                General Configuration

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                [Entry Fields]
Network Management Stations           [nwst45]
Start SMUX Daemon                     yes
Log Level for Trap Generation         err,warn

Log File                              [/var/adm/ARTour.log]
Log Level                             err,warn,log,trcart

Accounting File                       [/var/adm/ARTour.acct]

Trace File                            [/var/adm/ARTour.trace]

UDP Port for Password Update Service  [ARTourChPw]

[MORE...12]

F1=Help          F2=Refresh          F3=Cancel          F4=List
Esc+5=Reset      Esc+6=Command      Esc+7=Edit        Esc+8=Image
Esc+9=Shell      Esc+0=Exit        Enter=Do

```

Figure 39. eNetwork Wireless General Configuration

Here is a description of the parameters relevant for eNetwork Wireless network management:

1. Network Management Stations:

This field specifies a list of network nodes which the gateway takes as Network Management consoles. SNMP traps are forwarded to these IP addresses when eNetwork Wireless Gateway detects a message type that matches the type(s) specified in the Log Level for Trap Generation field. From these nodes SNMP query and configuration requests concerning the eNetwork Wireless Gateway are accepted.

This field is ignored if the Start SMUX Daemon field is set to “no”, which is the default.

2. Start SMUX Daemon:

A value of **yes** in this field starts the SMUX daemon, which allows the SNMP agent, which is part of AIX TCP/IP to access variables residing in the Management Information Base (MIB) belonging to the eNetwork Wireless Gateway. This daemon must run in order to use eNetwork Wireless network management.

3. Log Level for Trap Generation:

This field specifies the type of message for which IBM eNetwork Wireless Gateway will generate and forward an SNMP trap. Valid values are:

- none** Do not generate traps.
- err** Generate a trap when an error message occurs.
- warn** Generate a trap when a warning message occurs.
- log** Generate a trap when normal logging events occur.

If you are running Tivoli NetView on a network management console and want the traps from the eNetwork Wireless Gateway to be reported, you must define the IP name of the network management console and start the SMUX daemon on the gateway.

To activate the new NetView configuration file after installing eNetwork Wireless network management on the network management console, stop and restart Tivoli NetView.

To stop the NetView application, go to the menu bar of the network management console and select **File -> Exit**.

To start Tivoli NetView from the command line, enter:

```
nv6000
```

The network management console comes up with a *home submap*, showing your network configuration.

If you want Tivoli NetView to show the eNetwork Wireless Gateway and the wireless network (this is what a mobile network is called in NetView terminology) in the IP submap at startup, follow the steps below:

1. Locate and activate the Tivoli NetView Window IP Internet, which is depicted in Figure 40 on page 100.
2. Select Options from the upper menu bar.
3. Select Set Home Submaps from the shown list.
4. Select the desired submap with the mouse and click on Set as Home.

We recommend setting the submap IP Internet as the Home Submap, as depicted in Figure 40 on page 100.

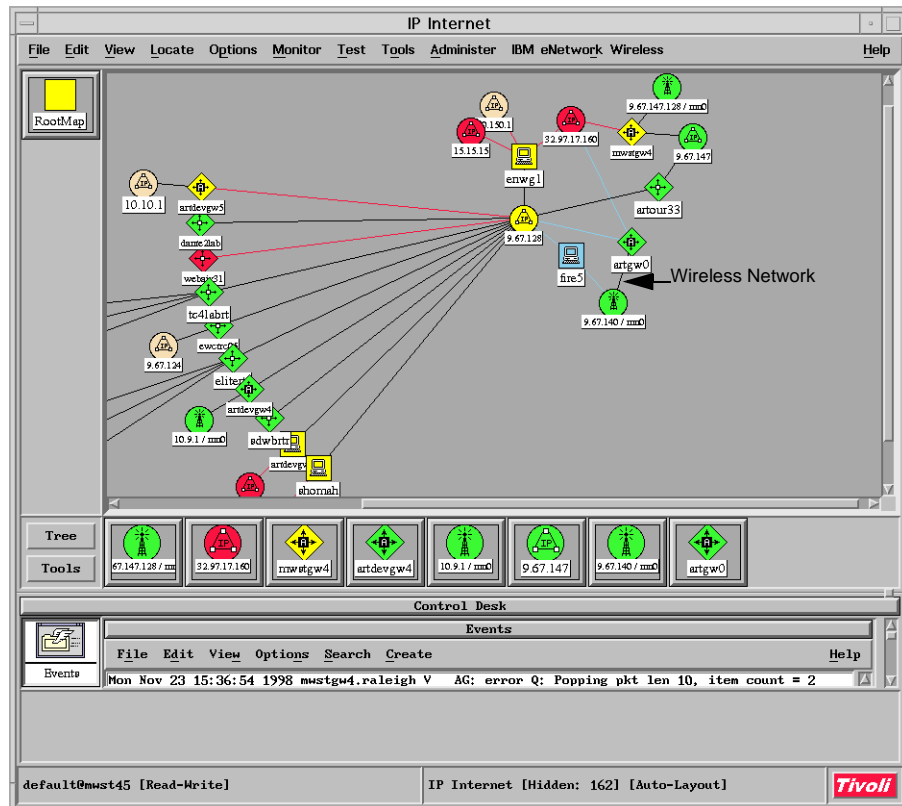


Figure 40. The Submap IP Internet

You can use the automatic layout supplied by the system or customize the layout by hand. To deactivate automatic layout and move objects where you want them in the submap:

1. Select View from the upper menu bar.
2. Select Automatic Layout from the shown list.
3. Select For This Submap from the shown list.
4. Select Off for This Submap.

Then, by pressing **Ctrl** and the middle mouse key simultaneously, you may change object positions on the map. New objects come up in the New Object Holding Area in the lower part of the map. You can then drag the new objects to any position on the map.

3.6.2 Monitoring eNetwork Wireless Configuration

IBM eNetwork Wireless network management uses Tivoli NetView to represent the wireless gateway and network and to display status information for the network and individual components at various levels. Mobile devices are objects displayed as standard computer symbols (rectangles) with a laptop computer symbol inside. They are displayed within a NetView hierarchy used specifically for radio networks.

Note

Mobile devices in the context of network management are the same as mobile clients in the context of eNetwork Wireless Gateway.

In the IP Internet map the eNetwork Wireless Gateway is shown as a router icon with an “A” in it with *Wireless Networks* defined by the mobile network interfaces (for example *mn0*) attached to them. Note that a wireless network may contain different radio networks, which correspond to mobile client connection types, like ARDIS, Mobitex, GSM, etc.

In Tivoli NetView a wireless network is similar to an IP subnet in that it can be zoomed in to see more details. If you look into a wireless network, you see the mobile network interface of the Gateway and the radio networks it supports, as shown in Figure 41 on page 102. Since a mobile device may have several mobile client connections, its connections may reside in different radio networks.

A radio data network (ARDIS, GSM, and so forth) displays a symbol for each mobile device connected to it. Therefore, the same mobile device can be represented many times, once for each mobile client connection in the corresponding radio network.

Five colors show the connection status of the device to a network (see Table 2 on page 101).

Table 2. Status of Mobile Devices

Color	Status	Meaning
Red	Closed	Totally disconnected from the gateway.
Yellow	Open	Connected via another radio network.
Green	Connected	Connected via this radio network.
Purple	Hold ^a	Connected via this radio network, but the gateway temporarily lost connection to the RDN provider.
Pink	Short hold ^b	Connected via this radio network, but client is temporarily in short hold mode.

a. For packet radio networks connected to the gateway via X.25 only.

b. For dial networks only.

Status information for a mobile device connection is sent up to parent objects and affects their status. A parent object (a network, user segment, and so forth) displays colors as shown in Table 3 on page 101.

Table 3. Parent Object Status

Parent	Children
Green	No child device connection is critical (all are in open, connected, or short-hold device status).
Yellow	Some, but not all, child device connections are critical (some are in closed or hold state).
Red	All child device connections are in a critical state (closed or hold).

3.6.2.1 Viewing and Setting Device Information

To see the status of the mobile network interface click on the mobile network interface icon (for example 9.67.140/mn0), and you will see the window as shown in Figure 41 on page 102. This window shows all radio networks connected to the eNetwork Wireless Gateway (in our case artgw0) with the status of each component coded in the icon's color according to Table 3 on page 101, since all of these items are parent objects

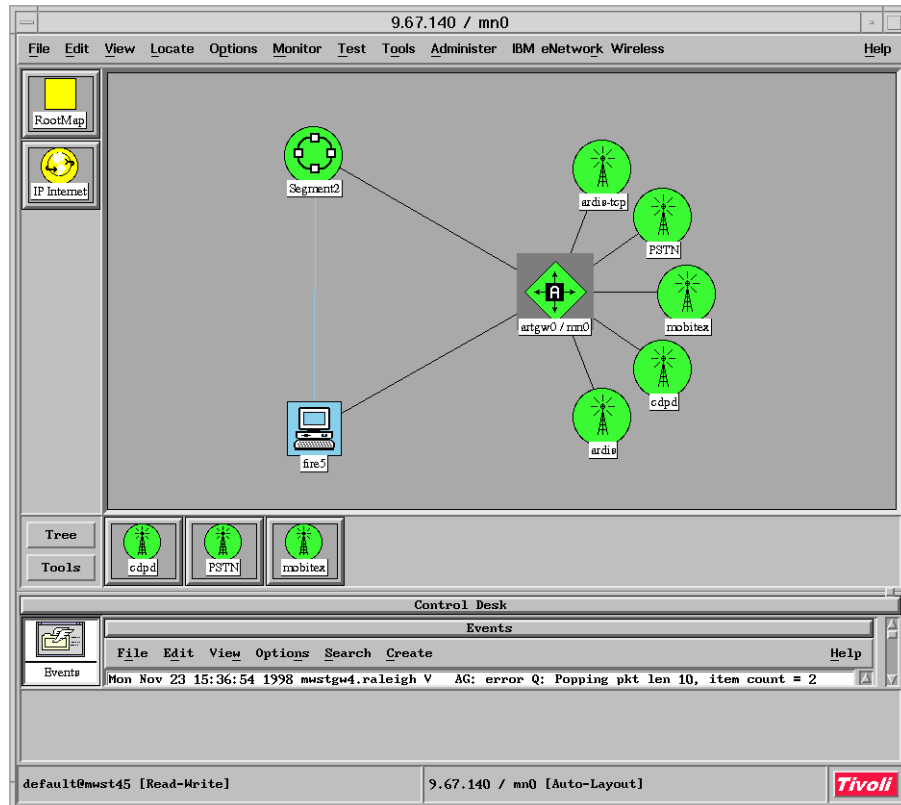


Figure 41. Mobile Network Interface Status

If you double-click on the icon of a radio network (in our case we selected the Mobitex network), you will see all mobile devices that have a connection configured for this radio network. The color of the mobile device icon represents the connection status as coded in Table 2 on page 101. An example is shown in Figure 42 on page 103.

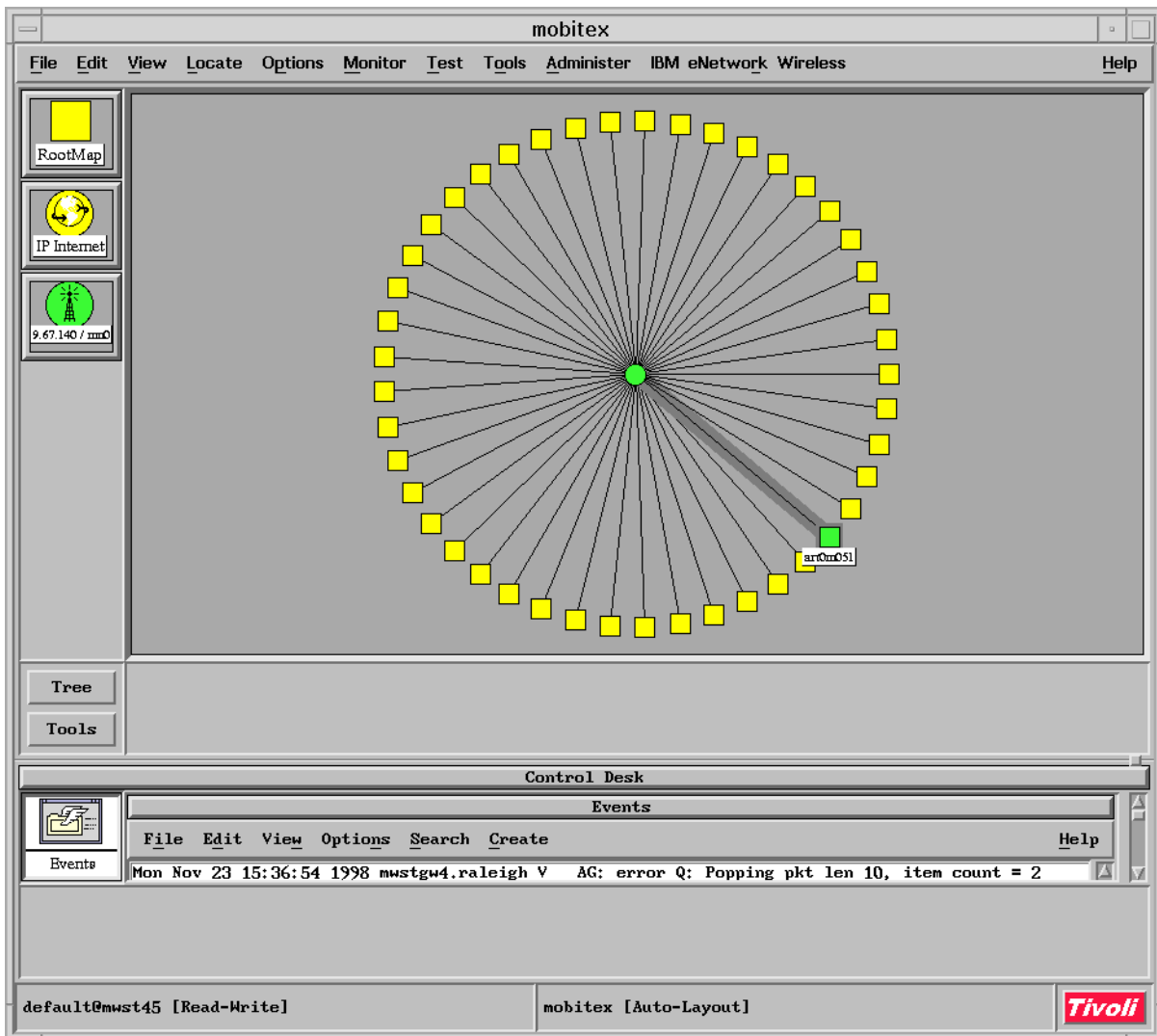


Figure 42. Mobitex Mobile Network Interface Screen Panel

If you click on one of the mobile device icons and choose **Device Info** from the *IBM eNetwork Wireless* menu, you will get the Device Information panel as depicted in Figure 43 on page 104, which gives you an option to set specific information about mobile devices).

The top of the Device Information panel shows general information that applies to the mobile device itself and is the same under all mobile client connections. The lower part displays radio network specific information. To view information about a different network connection, you may use the connection pop-up button that displays the actual mobile client connection type and radio network.

You can change the following information associated with the mobile device:

- Password
- Password expired flag (Set to “yes” when a password needs to be changed or when a new password is assigned.)
- Authentication required flag

- Trace flag
- Connect status



Figure 43. Mobitex Device Information Panel

Use pop-ups or select buttons to make changes. When all changes are complete, select **Apply** to send changes to the eNetwork Wireless Gateway.

To view a network connection for a different mobile device, change the IP address at the top of the display and press Enter or select **Restart**.

To end the dialog without updating the network connection, select **Close**. Selecting **OK** ends the dialog and also updates the network connection

3.6.2.2 Locating Devices and Connections

The /IBM eNetwork Wireless menu provides an easy way to locate mobile client connections for a mobile device. When you select **Search**, from the IBM eNetwork Wireless menu bar item, you can enter a regular expression and a pop-up connection status. If you leave the input field blank, all devices are searched.

Note

The asterisk (*) does not act as a wildcard character as it does for UNIX file names.

The regular expression is compared with information that relates to any of the following fields:

- IP address
- Device name
- Connection name
- Fleet name (if applicable)
- Specific information, such as LLI, MAN, and phone number

Press Enter or select **Search** to display a list of all mobile client connections that match the search condition.

To further restrict the search, specify a connection status in the pop-up window. Then only mobile devices that match the search criteria and have a particular status are searched. You can also display all mobile devices of a particular status by leaving the input field blank and selecting a status.

3.6.2.3 Checking Connections

When a user turns off a mobile device without properly terminating the eNetwork Wireless Client, the eNetwork Wireless Gateway is not informed. Therefore, connections might appear to be established when actually they are not.

To verify the connection status of one or more mobile devices, select them on the Tivoli NetView window that shows the radio network and choose Check Connection from the IBM eNetwork Wireless menu item. This results in an SNMP query to the eNetwork Wireless Gateway which then reports the last known status of this connection.

As an alternative, you can also check a connection to a mobile device by selecting the device and choosing Check Connection->Ping, as you would with any device in the LAN. This selection results in the Network Management console sending out a ping request to test the connection to the mobile device.

If you suspect that a mobile device has been disconnected without properly terminating the connection to the eNetwork Wireless Gateway, the ping selection may help to clarify the situation. Be aware, however, that filtering mechanisms in the eNetwork Wireless Gateway may prevent any network node in the LAN, including the Network Management console, from pinging mobile devices.

Note

Do not use ping to routinely monitor mobile devices, because it generates traffic over the wireless data networks.

To verify all the connections on the eNetwork Wireless Gateway, select Check Connection->All Connections on the eNetwork Wireless Gateway symbol. This global verification is an easy way to update all status information in the eNetwork Wireless Gateway display.

3.6.2.4 Listing All Mobile Devices in a Structure

To list all devices and network connections within a radio network, choose Contained Devices from the IBM eNetwork Wireless menu.

3.6.2.5 Changing Device Labels

To change the label of selected devices, choose from the IBM eNetwork Wireless menu Device Label->Show XXX where XXX=IP address, device name or specific data.

This allows you to change labels for a single device, multiple devices, or all devices contained within any eNetwork Wireless network structure.

3.6.2.6 Grouping Mobile Devices

To customize a group of devices, choose from the IBM eNetwork Wireless menu User Segments->Create Segment.

To create a new group, select all device connections, which is how mobile client connections are referred to in Tivoli NetView terminology, that should belong to this group before choosing to create the segment. A new symbol for a user segment appears and all selected devices disappear from the display as they move to that new segment. Give the new user segment a meaningful name. You can repeat these steps to further regroup device connections within one or more levels in the hierarchy.

To move device connections to an existing user segment, select the connections you want to move and also select the segment where you want to move them. When you choose Create Segment, all selected device connections are moved into the user segment.

To delete a user segment, select it and choose from the IBM eNetwork Wireless menu User Segments->Delete Segment. When a segment is deleted, the device connections that it contained are moved up to the submap on which the user segment was displayed.

3.6.2.7 Synchronizing Tivoli NetView and the Wireless Gateway

During normal operation, the Network Management console reflects the current state of the gateway. However, bursts of network traffic or system irregularities can interfere with status updates. If you suspect inaccurate status, you can re-synchronize the Network Management console and the eNetwork Wireless Gateway by choosing Synchronize from the IBM eNetwork Wireless menu. Tivoli NetView then updates all available information for the gateway.

3.6.2.8 Renaming Structures

Change symbol labels from the Tivoli NetView standard object context menu by choosing Edit->Modify/Describe->Symbol.

The title of a corresponding submap can also be changed by choosing Edit->Modify/Describe->Submap from the menu bar of a displayed submap.

Change the labels for an eNetwork Wireless network structure and the title of the corresponding submap in one step by choosing Edit->Modify/Describe->Object. In the list that appears, choose ARTour. In the resulting dialog, enter the new name in the Common Label field. Select **Verify** to ensure the label does not already exist, then select **OK** to confirm your input.

Chapter 4. Wireless Client

This chapter gives you an introduction to the eNetwork Wireless Client and describes the installation and configuration procedures including updating and removing the software. Finally it gives you some hints on running the client software.

4.1 Introduction

The eNetwork Wireless Client allows a mobile computer with a wireless modem to run TCP/IP applications over a wireless network. To access intranet and Internet applications, the client computer connects to an eNetwork Wireless Gateway. eNetwork Wireless Gateway and Client extend Internet Protocol (IP) connectivity across a diverse set of wireless and dial-up networks to seamlessly enable TCP/IP applications to access the enterprise network.

One of the major benefits of using eNetwork Wireless Gateway and Clients is that the mobile client is virtually part of the enterprise network. Other benefits include client and server authentication, data stream encryption, compression, and reduction. eNetwork Wireless Gateway and Client only supports IP traffic.

Figure 44 illustrates the general eNetwork Wireless Gateway and Client configuration.

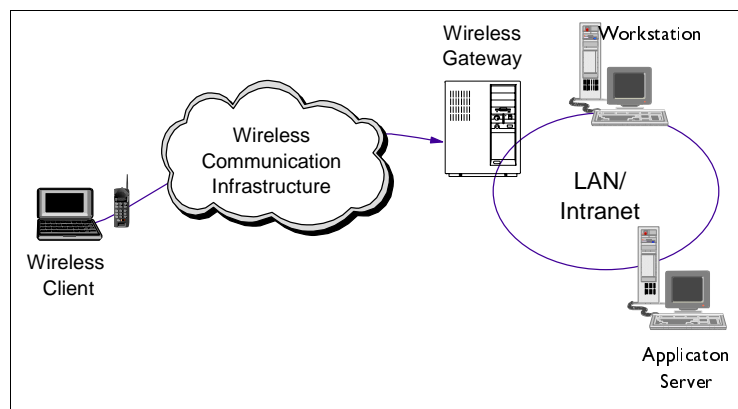


Figure 44. eNetwork Wireless Gateway and Client Configuration

eNetwork Wireless Gateway and Client has many features which distinguish this product from other products allowing you to access the Internet or intranets. For a detailed discussion of the eNetwork Wireless functions refer to 2.5, "Functions of the eNetwork Wireless Gateway and Client" on page 44.

The eNetwork Wireless Client software is middleware which can be located below the TCP/IP protocol stack. To TCP/IP it shows up as a network adapter. Thus every application using TCP/IP sockets may communicate over eNetwork Wireless. Figure 45 on page 108 depicts the software components involved in an eNetwork Wireless solution.

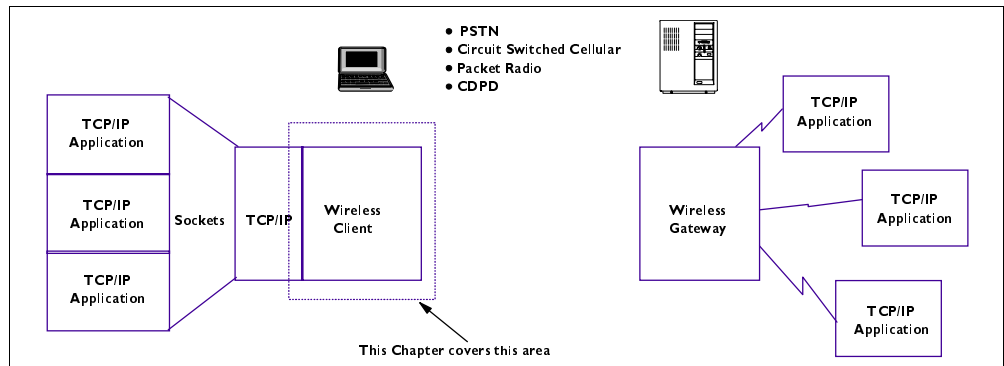


Figure 45. An Architectural View of the Wireless Client and Gateway Components

eNetwork Wireless Client supports the following wireless networks:

- DataTAC (including Motorola PMR)
- Mobitex
- CDPD
- Dial connections
 - AMPS
 - GSM/ PCS
 - PSTN
- Dataradio

For more information about of these technologies refer to 2.2, “Wireless Mobile Network Technologies” on page 19.

4.2 Installation and Configuration

The following section will discuss installation and configuration procedures for Windows 95, Windows NT and OS/2. Windows 3.x is not covered in this book. Refer to the manuals if you have to install the client under Windows 3.1 and 3.11.

Refer to Appendix A, “System Requirements” on page 241 for information about the system requirements.

Note

You may use Windows 98, but it is not officially supported in the current release.

For this redbook we performed installations on Windows 95, Windows NT and OS/ 2 using the DataTAC, Mobitex, CDPD and PSTN wireless networks. For install procedures of other wireless networks, please refer to the manuals.

4.2.1 Checklist

Here is a checklist for installing the eNetwork Wireless Client:

- Get the required hardware and software.
- Make sure that your wireless modem is registered at the network provider.
- Get the required information from your eNetwork Wireless Gateway administrator.
- Install the modem on the mobile computer including driver and support software, if available and make sure that everything works.
- Install the eNetwork Wireless Client.
- Set up the connection to the eNetwork Wireless Gateway.
- You may create an icon to start a connection directly from the desktop.
- You may customize the client to auto-start a user application.

4.2.2 Setting Up the installation Environment

For our testing, we used the following hardware:

- IBM ThinkPad as the eNetwork Wireless Client platform
- IBM Wireless Modem for ARDIS network
- IBM Wireless Modem for Mobitex network
- IBM Wireless Modem for CDPD network
- IBM Data/Fax Modem for Dial PSTN connections

The ThinkPad was running Windows 95, Windows NT 4.0 Workstation and OS/2 Warp 4.

Note

- Using Windows NT, log on to your computer under an administrator account, to have enough privileges to access and modify the operating system features.
- An IBM ThinkPad requires the ThinkPad utilities to be installed, which gives you the ability to monitor, enable or disable the ThinkPad's features. You will have to use this to avoid interrupt conflicts between the PC card modems and the infrared port.

The software you need to have installed prior to installing the eNetwork Wireless Client includes:

- eNetwork Wireless Client software which comes on the CD-ROM labeled *eNetwork Wireless Gateway for AIX*. You can put this on two diskettes prior to installing the eNetwork Wireless Client if your notebook only has a floppy drive.
- Operating system install media (for Windows 95 you will need the CD-ROM or the CAB files on the hard drive).
- Driver and utility software from the modem manufacturer, if available.

4.2.3 Setting Up the Wireless Modems

Before you start configuring the eNetwork Wireless Client software, you have to make sure that your wireless modem is registered at the network provider and is installed correctly on your computer. You also must know the COM port your modem uses. To determine the COM port number, refer to "Installing a Modem on the Mobile Computer" in the *eNetwork Wireless Gateway and Client Administrator's Guide* (SC31-8633).

The following two sections give you some additional hints and information.

4.2.3.1 Registering the Wireless Modems at the Network Provider

Before your modem can communicate in your area, it must be registered to a network provider. The information you need to have for this varies between the wireless networks. Table 4 on page 110 lists the parameters required for and supplied by the network providers. The meaning of these parameters is explained in 2.2, "Wireless Mobile Network Technologies" on page 19.

Table 4. Important Information to Register a Wireless Modem

Network Provider	Requires from You	Supplies to You
CDPD	Equipment ID (EID)	1. Internet IP address ¹ 2. Network side, either A or B ²
DataTAC (ARDIS)	1. Modem ID (LLI or SUJ) 2. Host port connection ³	1. Slot number or extended address
Mobitex (RAM)	Modem ID (MAN) ⁴	N/A
Private Mobile Radio / Dataradio	Private network, customer has to acquire the right to use certain frequencies and then operate the network by himself.	Hardware manufacturers help the customer to set up the network infrastructure correctly.
Dial	N/A	Telephone number

Additional notes:

- ¹ Use this IP address to configure your CDPD modem (using the configuration utility supplied with your modem).
- ² The eNetwork Wireless Client configuration defaults to network side A. If you use network side B, use the eNetwork Wireless Client Configuration Wizard to change the CDPD modem configuration to side B.
- ³ The host port connection is available from your eNetwork Wireless Gateway administrator.
- ⁴ The MAN of the eNetwork Wireless Gateway is required by the network provider if your modems and the gateway should build a closed user group.

4.2.3.2 Checking Your Modem under Windows

The most probable failure in connecting to the gateway is having modem problems. To avoid these problems in advance, check the installation of your wireless modem and the network connection before installing the eNetwork Wireless Client.

Very common modem problems are that the computer cannot recognize a PC card modem correctly or Windows assigns a COM port different from what you expected or there is a conflict situation in the interrupt settings.

When you insert the PC card into a computer running Windows 95 or Windows 98 with plug-and-play capability, Windows may recognize the modem as a new card, but it may not have a corresponding driver in its Windows's database. To avoid this problem, you should install the driver given to you by the modem manufacturer properly before you insert the modem for the first time.

Note that if you plug in a PC card which is unknown to the operating system, it may offer to use a standard modem driver. If you accept this, an entry in the modem list is generated and you may have problems installing the correct modem driver. In that case, remove the standard modem entry before you install the wireless modem driver.

In some cases, the wireless modem comes with some utility software, which gives you the ability to perform diagnostics, monitor the modem, or update the microcode. It may also allow you to configure the modem, for example, read and change the IP address of a CDPD modem. Refer to the modem documentation and README files for these subjects.

Note that some IBM ThinkPad models, for example type 76x series have a built-in infrared serial port, an external serial port and other features that use hardware interrupts usually reserved for COM ports. Run your ThinkPad utility software and disable any built-in devices you do not need, then shut down, power off and reboot the computer before you install the wireless modem. This frees your interrupts for the wireless modem. Note also that the eNetwork Wireless Client only supports the serial ports COM1 to COM4 and that the interrupt used by the wireless modem may not be used otherwise.

As an example we describe the installation of an IBM Mobitex modem with its support software under Windows 95:

- Be sure to have your IBM Mobitex modem removed from the PC card slot.
- Install the software from the two diskettes.
- When the installation is finished you should see a folder with three applications and one README file. The applications are, Hardware Diagnostics, Mobitex Modem Configuration, and Support Panel.

The Mobitex Modem Configuration application will also be put in the Control Panel. This application is useful for running your connection with a Mobitex modem.

- Reboot your computer.
- Now, insert the modem, and start the Mobitex Modem Configuration program.

If the modem is recognized, you can start the eNetwork Wireless Client software after installing it. Otherwise you should check your configuration for interrupt conflicts or try to release the modem from the PC card slot, re-insert it, and re-run the Modem Configuration.

Note

In our tests, our NT machine did not recognize the Mobitex modem. This may happen with other modems too, which do not supply Windows NT drivers. In our case, we inserted the modem and booted the computer. The computer then recognized the PC card as a standard modem and assigned a COM port for it. We got the COM port number out of the modem panel and used it to successfully configure and run the eNetwork Wireless Client.

Note that Windows NT does not have the plug-and-play feature like Windows 95, so the wireless modem has to be inserted at boot time. There is, however, some third party PC card utility software available, which allows you to insert and pull-out PC cards while NT is up, but we didn't test this software to run with the eNetwork Wireless Client.

4.2.3.3 Checking Your Modem under OS/2

When you install OS/2 on a ThinkPad, you should have the PC Card Director application installed too by default. You can use this application to check if the modem is recognized correctly. Figure 46 on page 112 depicts a properly recognized modem.

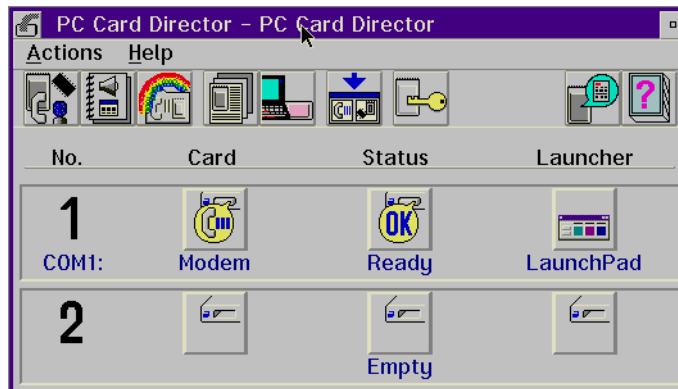


Figure 46. PC Card Status Information

The PC Card Director says that there is a modem recognized on socket 1 which is assigned to COM1 and its status is Ready.

Sometimes the modem will not be assigned to a COM port. In that case, may have to edit your CONFIG.SYS file manually. Refer to the OS/2 help files or try the following:

- In the CONFIG.SYS file, find the following line:

```
DEVICE=C:\OS2\BOOT\COM.SYS
```

- Assign specific I/O ports and interrupts for each of the COM ports needed. The following example would enable all of the ports supported by the eNetwork Wireless Client:

```
DEVICE=C:\OS2\BOOT\COM.SYS (1,3f8,3) (2,2f8,4) (3,3e8,5) (4,2e8,10)
```

You must make sure the I/O ports and interrupts specified are available for use.

4.2.4 Registering a Mobile Client at eNetwork Wireless Gateway

To connect to the eNetwork Wireless Gateway your client will have to be registered at the eNetwork Wireless Gateway. To register a wireless modem at the gateway, the gateway administrator needs the information provided by the wireless network operator together with the modem identification parameters.

To configure the eNetwork Wireless Client correctly, you need the following information from the gateway administrator, depending on the wireless networks you are using. Here is a list of the required information for the different wireless networks:

- Information whether a gateway password is required and if it is, the initial password assigned to your client by the eNetwork Wireless Gateway administrator. We strongly recommend to use the authentication feature. Note that the password is case sensitive. This is common to all wireless networks.
- Although data compression and encryption can be negotiated by the client, it is a good idea to follow the company rules, which you get from the gateway administrator.
- CDPD: The eNetwork Wireless Gateway IP address on the Internet. If you are connected to a CDPD network provider over a direct connection, this IP address may be in the address range of the CDPD network provider. Otherwise it is in the range of your Internet service provider.
- Mobitex: MAN number of the eNetwork Wireless Gateway (eight-digit decimal number).
- DataTAC: Depending on the addressing scheme you either need a slot identifier (for example, TE3) associated with the eNetwork Wireless Gateway or its extended address. Note that for Motorola PMR the slot identifier field is ignored but you still have to type something in.
- Dataradio: You need to know whether the Dataradio network is set up for the CARMA-M or DBA protocol. You need this to properly select the Dataradio modem device.
- Dial-up connections. These include PSTN, GSM, and so on. You need the area code and the telephone number of the eNetwork Wireless Gateway.

4.2.5 Wireless Client Installation and Removal

In this section we assume that the operating system has been installed on your computer and the latest fix-packs applied. We also assume that TCP/IP has been installed.

The eNetwork Wireless Client for Windows installs on Windows 3.1/3.11, Windows 95 and Windows NT. For OS/2 there is a separate disk set.

eNetwork Wireless Client for Windows uses InstallShield commonly used for many Windows applications. For OS/2, the IBM Software Installer is used, so the installation process is straightforward.

4.2.5.1 Client on Windows 95

To install from CD-ROM, go to the CD-ROM drive, open the **Clients** folder, choose **En** for English Version or any language you prefer, then **Win** for Windows, **Install** until you find the folder **Disk1**.

From this directory, run **setup.exe**.

If you are installing from diskettes, you will find this program on Disk 1.

Note

The InstallShield recognizes which Windows version you are running and will install the appropriate code.

The program then asks you to see the READ.ME file. We strongly encourage you to carefully read through the material, since it may contain important information. When you exit the editor, the installation continues.

If you have a previously installed version, you will receive a warning message stating that all program files will be overwritten including any previously defined connections. If you choose to continue you won't get the opportunity to install into a new directory. If you wish to change the installation path, you are required to first uninstall the client.

In order to migrate connections from a previous version, print out the previous file `artour.ini` from the installation directory, install the new version and configure your client connections manually. Be warned, that when you overwrite the `artour.ini` file with a previous version, you may end up with an invalid configuration.

If you are installing the eNetwork Wireless client for the first time, you will be asked for a destination directory. If this directory doesn't exist, it will be created by the InstallShield.

During the installation process, the NDIS Version 3.0 device driver for Windows 95 is installed. You may be prompted for Windows 95 system files. If you have the Windows 95 CAB files on your hard disk, you may change the path to the corresponding directory. Otherwise you have to insert the Windows 95 Operating System CD-ROM.

If during device driver installation you get a message box stating that you are about to overwrite a file with an older version, be sure to keep the newer version.

Note

If you don't have the Windows CD-ROM at hand and quit the device driver installation, you have to perform an adapter device install manually before you start the eNetwork Wireless Client.

Go to the Control Panel and start the Network program. Then select the tab **Configuration** and push the button **Add**. Select **Adapter**, click **Add**, click **Have Disk** and point it to Disk 2 which may reside in your A-drive or on the eNetwork Wireless Install CD-ROM.

After the install of the adapter called *IBM eNetwork Wireless Client for Windows 95*, go to the Configuration tab of the network program and look for all protocols bound to the adapter just installed and remove every protocol except TCP/IP.

After installation is finished, you will be prompted to reboot the computer. Do it now.

To uninstall the eNetwork Wireless Client use the standard method selecting Add/Remove Programs from the Control Panel. This removes the eNetwork Wireless NDIS device driver as well.

4.2.5.2 Client on Windows NT

To install the eNetwork Wireless Client under Windows NT, follow the instructions in 4.2.5.1, "Client on Windows 95" on page 113.

The only difference under Windows NT is that the NDIS driver for eNetwork Wireless is not automatically installed. You have to do this manually using the following procedure:

1. From the NT task bar, click **Start->Settings->Control Panel**.
2. Double click **Network** Icon, then click the **Adapter** tab.
3. Select **Add** and then **Have Disk**
4. Insert the eNetwork Wireless Client for Windows Disk 2 in the drive and select **OK**.
5. Select IBM eNetwork Wireless Interface for Windows NT then click **OK**.
6. Select **Binding**.
7. Select **TCP/IP protocol** from Protocol tab.
8. Click **Properties**
9. Choose **eNetwork Wireless Interface** from the Adapter option
10. Select the Obtain an IP Address from DHCP server radio-button.
11. Click **Yes** on the question to enable DHCP, click **OK** and **Close**.
12. Reboot your computer.

To uninstall the eNetwork Wireless Client use the standard method selecting **Add/Remove Programs** from the Control Panel. Note that once you have

installed the NDIS driver, it will not be removed automatically with the client software. You will have to do this manually.

So, if you want to do a proper and clean reinstall of the eNetwork Wireless Client Software, you should uninstall the client and remove the adapter called IBM eNetwork Wireless Interface.

4.2.5.3 Client on OS/2

You must have a LAN Adapter Support (LAPS) or Multi Protocol Transport Services (MPTS) installed and the TCP/IP protocol added in your computer as a prerequisite to install the eNetwork Wireless Client for OS/2.

So be sure to have the following lines included in the CONFIG.SYS file:

```
DEVICE=C:\TCPIP\BIN\INET.SYS  
DEVICE=C:\TCPIP\BIN\FNDISNL.SYS
```

To install from CD-ROM, go to the CD-ROM drive, open the Clients folder, choose **En** for English Version or any language you prefer, then **OS2, Install** until you find the folder Disk1.

From this directory, run Install.exe.

If you are installing from diskettes, you will find this program on Disk 1.

The eNetwork Wireless Client install window displays the README.ART file. After reading this file, click **Continue**. Note that the installation program changes the CONFIG.SYS file.

After you finish installation, reboot your computer.

To remove the OS/2 eNetwork Wireless Client, start the install program from your install medium using the following command line:

```
a:\install /a:d
```

When the instruction panel appears, press **Continue** and select **Delete** to delete the eNetwork Wireless Client program.

4.2.6 Configuring the eNetwork Wireless Client

The configuration of the eNetwork Wireless Client is the same under all Windows platforms. Under OS/2 it is also very similar. Therefore, for a detailed configuration description we use the Windows platform. In 4.2.5.3, "Client on OS/2" on page 116 we show the differences under OS/2.

In most cases, configuring the eNetwork Wireless Client means creating a connection to the eNetwork Wireless Gateway, selecting the radio modem from a list and entering the required parameters. When you create a connection to the eNetwork Wireless Gateway you are prompted for the essential connection parameters only. If the connection you have created does not work the first time, you may have to edit your connection profile as described in 4.2.8.3, "Modifying a Connection Profile" on page 131. By modifying a connection profile, you have (for some network types) the ability to set parameters which you could not access during the creation of that connection.

Since creating a connection to the eNetwork Wireless Gateway is in many stages similar for all networks, we only describe the full process in the next section. The other sections show how to fill in the network-specific configuration panels. Therefore read through the configuration of a PSTN connection even if you are about to configure another wireless network.

Note

As shipped, the UDP ports 8888 and 8889 are used by the eNetwork Wireless Gateway and Client software. Therefore applications running on the client or the gateway host should not use these ports.

If your application requires the use of one of these ports, eNetwork Wireless allows you to configure these ports to avoid conflicts. To change these ports at the client, refer to 4.2.7.6, “Changing UDP Ports Used by the eNetwork Wireless Client” on page 130.

4.2.6.1 Configuring the eNetwork Wireless Client for a PSTN Network

eNetwork Wireless Gateway and Client supports PSTN connections normally in conjunction with cellular phones. You may, however, use eNetwork Wireless to access an enterprise network over a wireline PSTN connection, thus benefiting from the security and optimization features of the product.

To start configuring a wireless client connection, run the eNetwork Wireless Client software from the Start button following the path below:

Start->Programs->eNetwork Wireless Client->Client

You see the eNetwork Wireless Client Connect window.

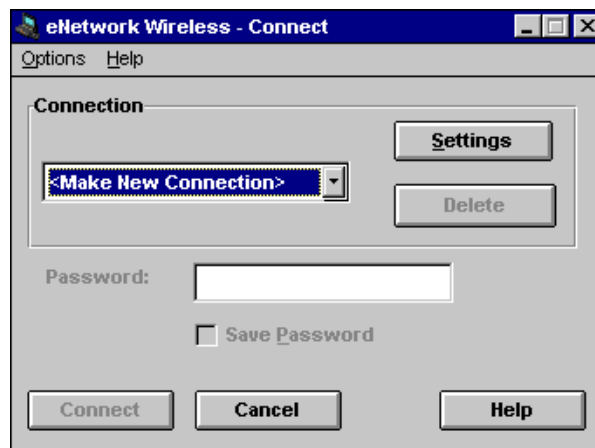


Figure 47. The eNetwork Wireless Client Connect Window

Click **Settings...** to create a *New Connection profile*.

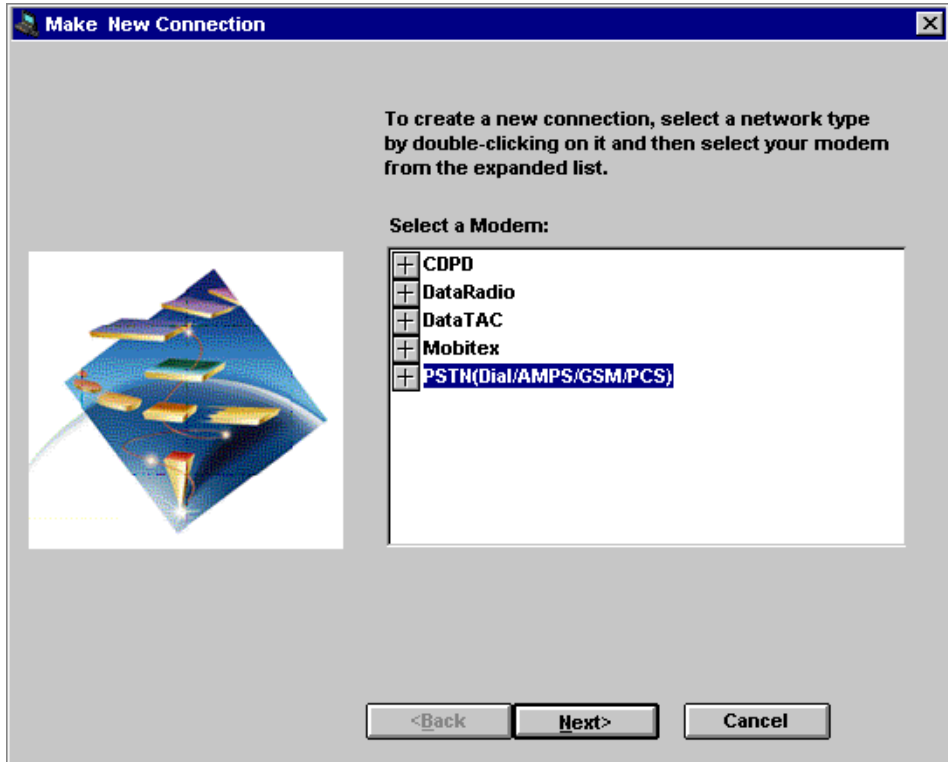


Figure 48. General Modem Selection

To configure a PSTN connection, double click on **PSTN(Dial/AMPS/GSM/PCS)** to expand the PSTN modem list. You may also click on the button with the plus sign in it.

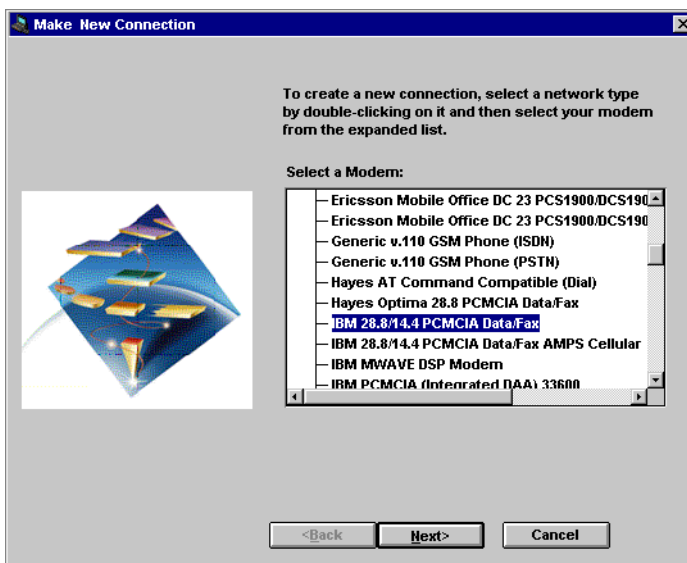


Figure 49. Selection of Dial Modems

Now choose the modem you are using in your computer. We selected the *IBM 28.8/14.4 PCMCIA Data/Fax*.

Note

If you have a modem that is not listed here, you may select the following modem:

HAYES AT Command Compatible (Dial)

You will probably have to modify the AT command string settings after creating the connection as described in 4.2.8.3, "Modifying a Connection Profile" on page 131.

Now click **Next**.

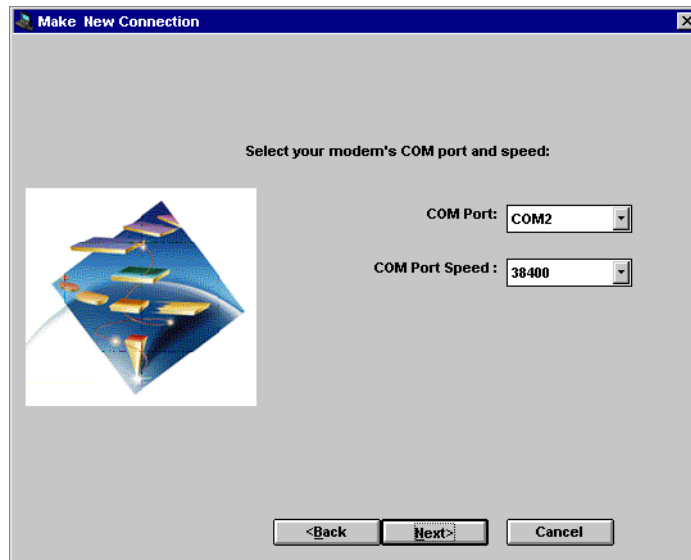


Figure 50. COM Port and Speed Selection

Choose the COM port and speed to be used. COM2 is frequently used by serial PC cards. The COM port speed typically defaults to what the modem manufacturer recommends, so you may go with this value.

Note

The eNetwork Wireless Client is not able to access ports higher than COM4.

If you are not sure which port your modem uses, select one and check later whether the system has changed it to a different port. You may then modify the eNetwork Wireless Client configuration to the new COM port. COM port changes due to the Windows plug-and-play feature may also happen to other wireless modems, such as CDPD, Mobitex or ARDIS.

Then click **Next**.

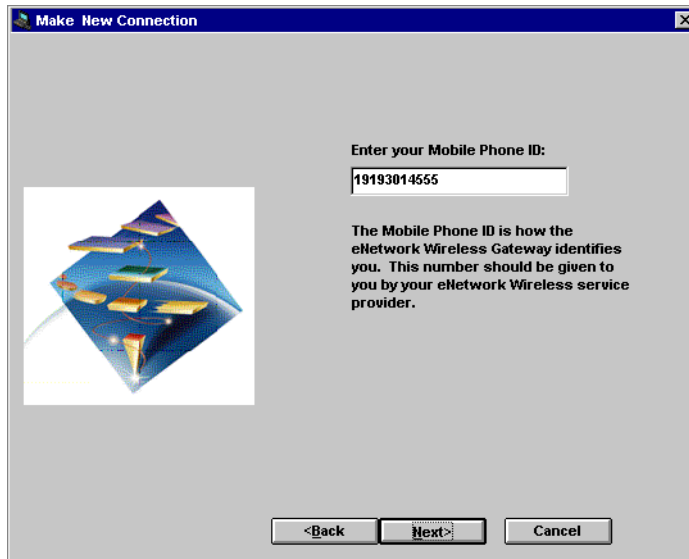


Figure 51. User's Mobile Phone ID Input Field

Enter your *Mobile Phone ID*.

This is the telephone number which is registered with your client at the gateway. If the gateway call-back feature is enabled, it has to match your actual number; otherwise the gateway will not be able to reach the client during the call-back operation.

Then you click **Next** to enter the destination phone number, which is the eNetwork Wireless Gateway telephone number (the number to be dialed).

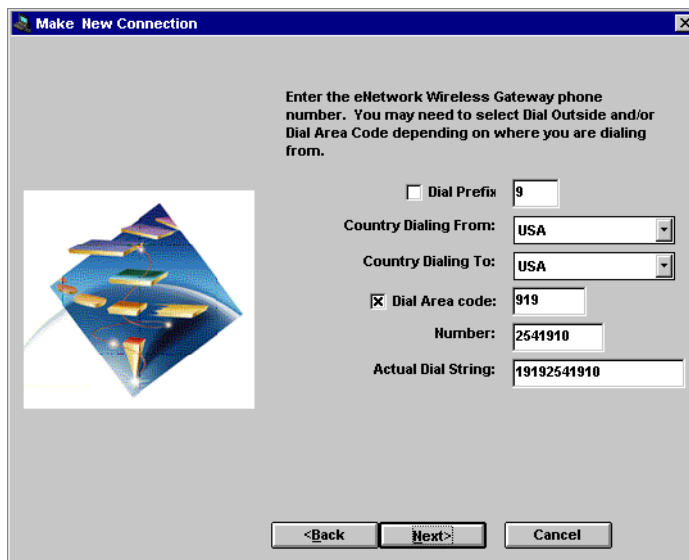


Figure 52. Entering the Wireless Gateway Phone Number

If you are dialing from your office over a PBX line you should specify the prefix number to dial outside. You also need to include the area code to dial and the destination phone number.

Click **Next** to get more options regarding data compression, authentication and encryption.

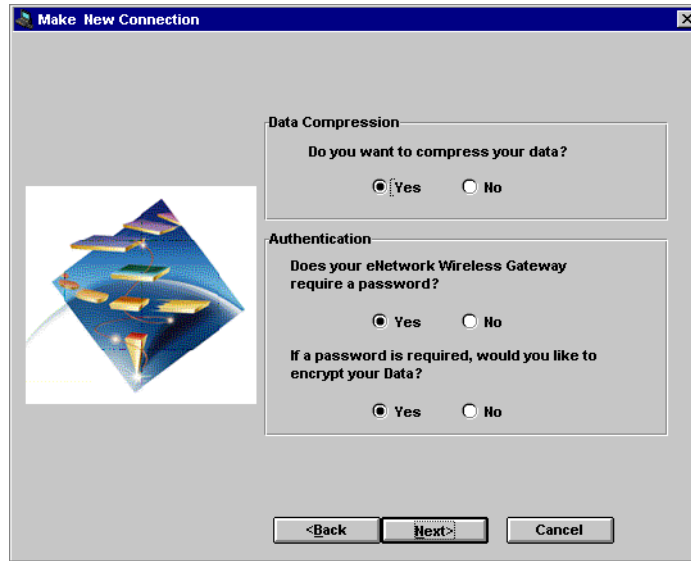


Figure 53. Data Compression and Authentication Options

These are default options. Change these settings according to the information the gateway administrator provided. For an explanation of these options refer to 2.5.3, "Data Transmission Techniques" on page 46 and 2.5.4, "Optimization Techniques" on page 48.

Then click **Next**.

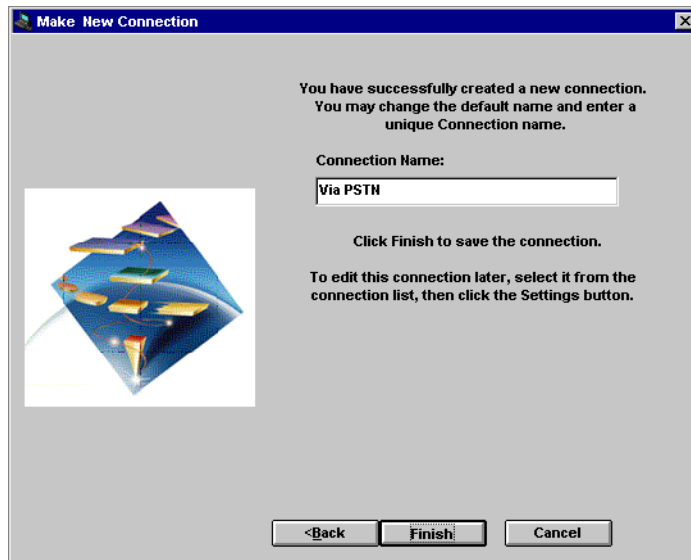


Figure 54. Profile Name Field

Now, enter a name for this configuration (Profile Name), we used *Via PSTN* to indicate that this profile will use a PSTN link.

Finally, click **Finish**.

You should get the last panel, which also appears when you start the eNetwork Wireless Client again.

You have now finished the configuration of a PSTN connection to the eNetwork Wireless Gateway. This connection is stored in the client's configuration file (artour.ini in the client install directory). You may want to edit this file for advanced configuration as described in 4.2.7, "Advanced Configuration Issues" on page 127.

Note

Please remember that your current definition is for PSTN and uses a PC Card modem. If you want to use another modem to access the same or other gateways, you should create a new profile.

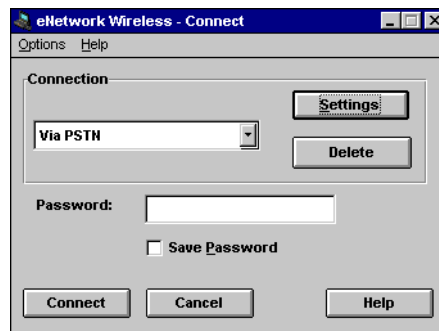


Figure 55. eNetwork Wireless Client Startup Window

You may now key in the password you received from the gateway administrator and you are ready to make a connection by clicking the **Connect** button. Again, we discourage you from checking the **save** option to preserve the password in your computer. To run the eNetwork Wireless Client refer to 4.2.9, "Preparing and Running the eNetwork Wireless Client" on page 133.

If you have problems connecting to the eNetwork Wireless Gateway you may modify the configuration as described in 4.2.8.3, "Modifying a Connection Profile" on page 131. Note that upon the creation of a connection not all options are accessible.

4.2.6.2 What's Different for DataTAC Networks

Configuring a connection to the eNetwork Wireless Gateway over a DataTAC is pretty much the same as configuring a PSTN connection, which was described in the previous section. You have to create a new connection profile but instead of selecting the *Dial* option, click on one of the DataTAC modems.

The panels following the radio modem selection are specific to the network type the modem belongs to. The configuration for DataTAC modems, which differs from the other networks, is described below.

Start configuring the wireless client, by selecting **<Make New Connection>** and clicking on the **Settings...** button as described for PSTN network connections.

Double click on the DataTAC section to expand the modem list and choose your modem type.

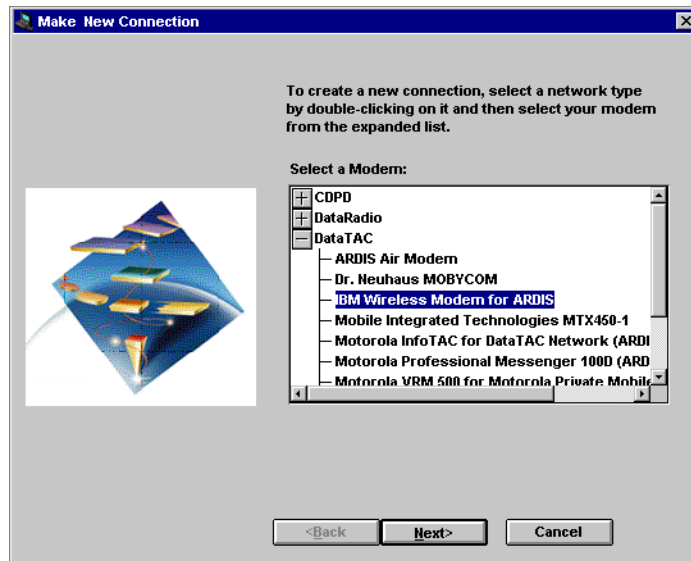


Figure 56. Modem Selection for DataTAC Networks

We used *IBM Wireless Modem for ARDIS*. Then click **Next**.

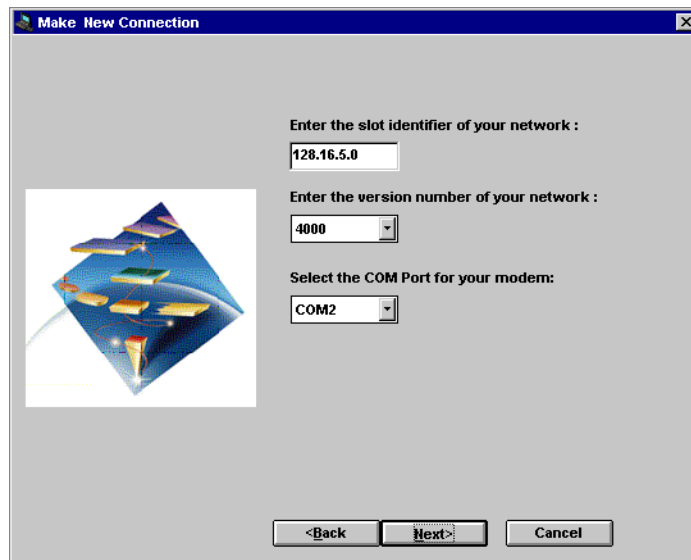


Figure 57. DataTAC Specific Settings

In the panel that shows up next, enter the DataTAC slot identifier or extended address provided by the DataTAC network provider or the gateway administrator. Then choose the DataTAC network version according to your geography and enter the COM port.

In our installation, we used an extended address of 128.16.5.0 to reach our eNetwork Wireless Gateway and the network version of 4000 for USA. The default value for the COM port is COM2, which was fine for us.

Then click **Next** to get to the panel to set Data Compression and Authentication parameters, which was shown in Figure 53 on page 121. The rest of the configuration is common to all wireless network types.

4.2.6.3 What's Different for Mobitex Networks

Configuring a connection to the eNetwork Wireless Gateway over Mobitex is again very similar to the configuration of a PSTN connection as described in 4.2.6.1, "Configuring the eNetwork Wireless Client for a PSTN Network" on page 117. That means you have to create a new connection profile but instead of selecting the *Dial* option, click on one of the Mobitex modems.

The panels following the radio modem selection are specific to the network type the modem belongs to. The configuration for Mobitex modems which differs from the other networks is described below.

Start configuring the Wireless Client by selecting **<Make New Connection>** and clicking on the **Settings...** button as described for PSTN network connections.

Double click on the Mobitex section to expand the modem list and choose your modem type.

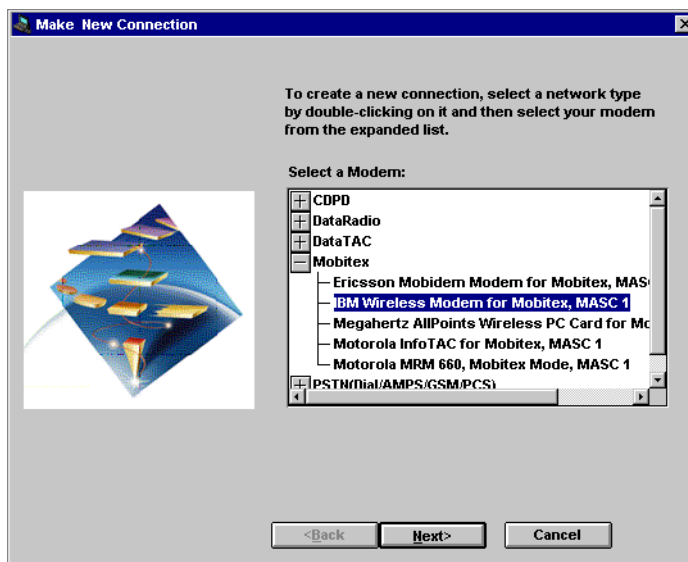


Figure 58. Modem Selection for Mobitex Networks

We used *IBM Wireless Modem for Mobitex*. Then click **Next**.

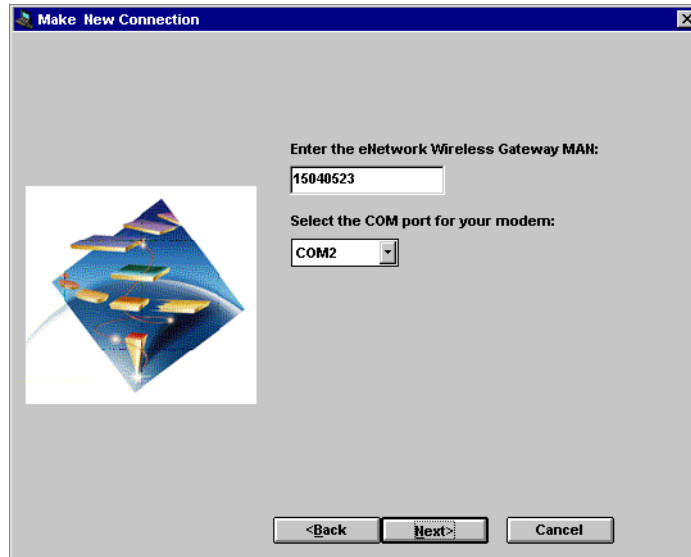


Figure 59. Mobitex Specific Settings

In the panel that shows up next, enter the Mobitex MAN number of the eNetwork Wireless Gateway (given to you by the gateway administrator) and select the correct COM port.

In our installation, we used MAN number 15040523 and COM2.

Then click **Next** to get to the panel to set Data Compression and Authentication parameters which was shown in Figure 53 on page 121. The rest of the configuration is common to all wireless network types.

4.2.6.4 What's Different for CDPD Networks

Configuring a connection to the eNetwork Wireless Gateway over a CDPD is again very similar to the configuration of a PSTN connection as described in 4.2.6.1, "Configuring the eNetwork Wireless Client for a PSTN Network" on page 117. That means you have to create a new connection profile but instead of selecting the *Dial* option, click on one of the CDPD modems.

The panels following the radio modem selection are specific to the network type the modem belongs to. The configuration for CDPD modems which differs from the other networks is described below.

Start configuring the wireless client by selecting **<Make New Connection>** and clicking on the **Settings...** button as described for PSTN network connections.

Double click on the CDPD section to expand the modem list and choose your modem type.

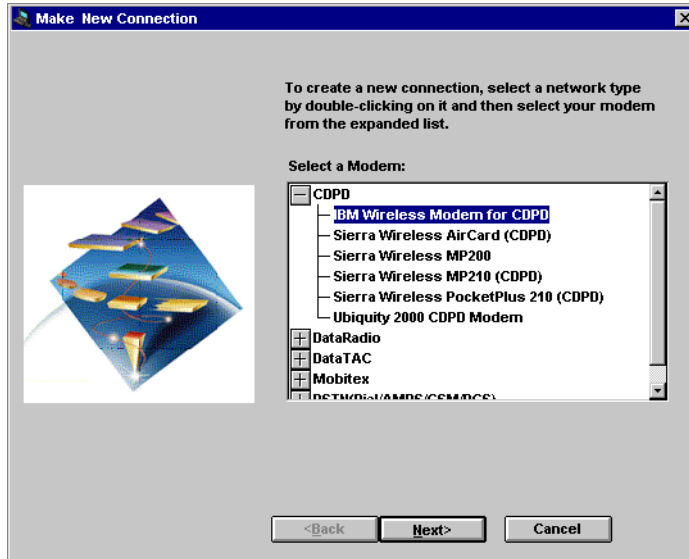


Figure 60. Modem Selection for CDPD Networks

We used IBM Wireless Modem for CDPD. Then click **Next**. The panel that comes up allows you to select the COM port. We went okay with the default setting, which is COM2. Click **Next** again.

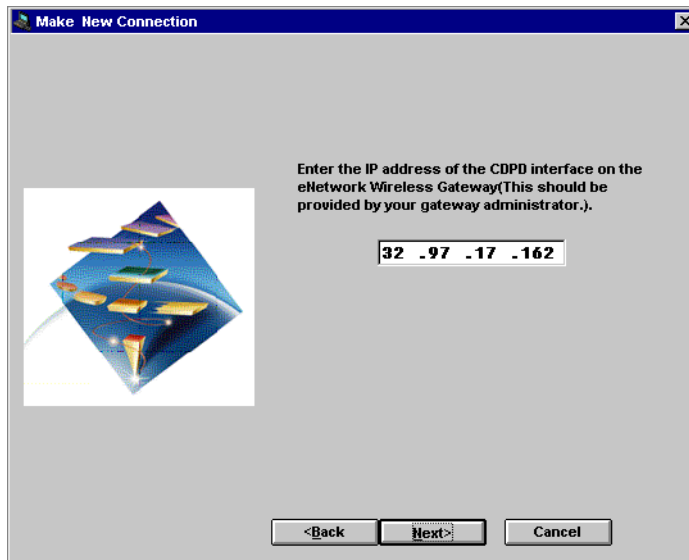


Figure 61. Mobitex Specific Settings

In the panel that shows up, enter the IP address under which the eNetwork Wireless Gateway is reachable from the CDPD provider. This may be the address of the gateway's IP interface connected to the Internet. You get this information from the gateway administrator. In addition you have to select the correct COM port.

In our installation, we used the IP address 32.97.17.162.

Then click **Next** to get to the panel to set Data Compression and Authentication parameters which was shown in Figure 53 on page 121. The rest of the configuration is common to all wireless network types.

4.2.6.5 Client Configuration under OS/2

Figure 62 on page 127 shows the eNetwork Wireless Client window where you find the icon to start the client software.

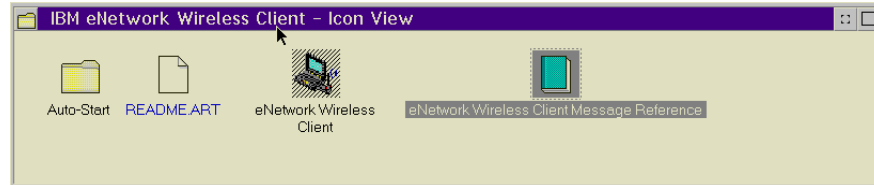


Figure 62. The eNetwork Wireless Client Icon in OS/2 Folder

You define a connection to the eNetwork Wireless Gateway in the same way as you would do in a Windows environment. Figure 63 on page 127 shows the client's startup panel under OS/2. After you configure a connection you may want to click the **Connect** button to start a connection after you enter the password.

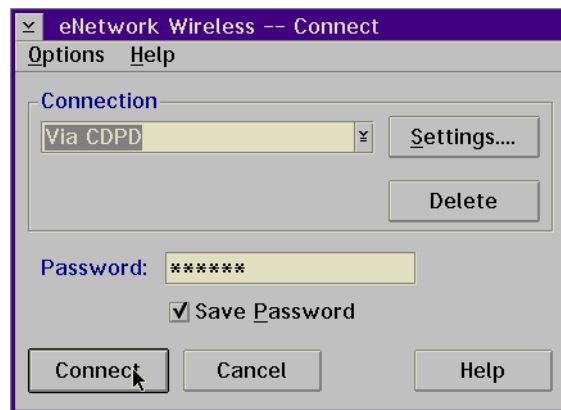


Figure 63. The eNetwork Wireless Client Connect Window on OS/2

Note

In Figure 63, the **Save Password** checkbox is marked for demonstration purposes only. We discourage you from using this feature in a production environment.

4.2.7 Advanced Configuration Issues

Some features of the eNetwork Wireless Client cannot be configured using the standard configuration method. These features may be used to set up a more convenient client environment on the mobile computer and are described below.

4.2.7.1 Creating an Icon to Automatically Start a Network Connection

This feature is optional, but sometimes very useful. Under Windows, the best way to create an eNetwork Wireless Client icon on the desktop is to drag the

eNetwork Wireless Client from the window that is left open (after installation on the desktop or wherever you want).

You can also create an icon to start the eNetwork Wireless Client afterwards. To do this, move your mouse pointer to the place where you want to create the icon, click with the right mouse button, and select **New -> Shortcut**. On the panel that appears, click **Browse...** and go to the eNetwork Wireless Client install directory, which may be *C:\Program Files\IBM\ARTour*. Find the Program **Artgui** and double click with the left mouse button, click **Next** and enter a name for this connection. Then click **Finish**. An icon (computer with an antenna) will appear on your screen.

4.2.7.2 Defining Autostart Applications

This section describes how to specify programs to run after the eNetwork Wireless Client has successfully established a connection to the gateway.

Under OS/2, you just copy or move application programs such as the eNetwork Emulator Express Client and terminal emulation program to a specific folder called Auto-Start in the IBM eNetwork Wireless Client folder.

Under Windows operating systems you have to modify your artour.ini file. This file located is in the directory where you installed the eNetwork Wireless Client. Per default this is: *C:\Program Files\IBM\ARTour*.

In each section labeled [**Connection<no>**], where <no> has to be replaced with a number, you may find the following statement:

```
AutoStartCommand=
```

You may modify this line by inserting the name of an executable program or batch file after the equal sign. Use absolute path names to make sure that the client is able to locate the program. Here is an example:

```
AutoStartCommand=c:\progra-1\ibm\artour\autostrt.bat
```

You can only enter one program to start. If you want to start several programs in sequence, use a batch file.

The AutoStartCommand definition only applies to the corresponding connection section. You may autostart different programs when you are connecting to the gateway for different networks.

Note

You have to use the old DOS format to specify path names (directory names have to be in the 8.3 format). The program or batch file specified in this line is automatically started after this connection is established

4.2.7.3 Starting Client from a Command Line Shell

To start the eNetwork Wireless Client from a command line shell or a batch file the command line should be of the form:

```
<client directory>\artgui.exe <options> <connection to start>
```

Three command line options are recognized: /s, /p and /t.

- /s** Disables the ability to edit the settings of a connection or create a new connection. With this option set the user may not select any connection or edit the connection settings.
- /p** Disables the ability to change the password when the client is connected to the gateway.
- /t** Disables the ability to enable or disable the transmitter (if the modem type supports transmitter functions).

Following the command line options you may specify a connection name to let the client directly proceed to the password entry panel (if authentication is required) and connect to the network. The connection name may contain spaces and special characters, but enter the connection name exactly as shown in the General tab on the Settings panel.

Note

The command line options must occur before the connection to start, and all parameters are optional.

4.2.7.4 Disabling the Save Password and Delete Feature

By default, the Save Password checkbox and the Delete button are enabled on the Connection screen. It may be desirable to disable these features, forcing the user to enter their password each time they go to connect, thereby securing the access point to the enterprise network without requiring the security of the device (workstation). It is usually also desirable to keep users from deleting connections.

To disable the Save Password checkbox and the Delete button, locate the following line in the artour.ini file:

```
EnableSavePassword=1
```

This line may be found in each Connection section entry. See 4.2.7.2, “Defining Autostart Applications” on page 128 for more information about the artour.ini file.

Now, set the line to read:

```
EnableSavePassword=0
```

As an alternative, deleting the entire line from the INI file will result in the same function.

4.2.7.5 Limiting What Settings Users Can Update (Windows Only)

By default, a user can click on the Settings button on the Connection screen and change the settings of the selected connection. It may be desirable to limit what settings a user can update. An example may be allowing the user of a client configured for a dial-in network to only change phone numbers.

To limit the access to configuration panels in the Settings dialog, locate the following line in the artour.ini file:

```
GUISettingsToShow=...
```

The value following this entry is 0x003F for dial connections and 0x003B for non-dial connections. This line may be found in each Connection section entry. See 4.2.7.2, “Defining Autostart Applications” on page 128 for more information about the artour.ini file.

Each bit in the number following this entry refers to a specific configuration panel. The values are as follows:

Options Page	0x0001
Connections Page	0x0002
Phone Page	0x0004
Counter Page	0x0008
Toolbar Page	0x0010
General Page	0x0020

So if you wanted the user to have access to only the Options and General panels make a logical OR operation to the values above to get the actual number for this setting. In our example the line would read:

```
GUISettingsToShow=0x0021
```

Use extreme caution in deciding which panels to show. It is possible to show a phone page on connections that don't use a phone number. Note that showing only a phone page on a connection that doesn't use a phone number will cause the program to consistently end abnormally.

4.2.7.6 Changing UDP Ports Used by the eNetwork Wireless Client

As shipped the UDP ports 8888 and 8889 are used by the eNetwork Wireless Gateway and Client software. Therefore applications running on the client or the gateway host should not use these ports. If your application requires the use of one of these ports, eNetwork Wireless allows you to configure these ports to avoid conflicts. Be warned that when manipulating entries in the artour.ini file you must totally be aware of the consequences.

To change these ports you will have to modify the eNetwork Wireless configuration file which has the name artour.ini and can be found in the install directory. Port 8888 is used to change passwords and is set in every Connection section. If you have to change it, be sure to change it in every section, and on every client connecting to the same gateway.

Make sure that these values are consistently changed with the gateway. Be aware that changing these values at the gateway affects all clients connecting to this gateway.

4.2.8 Managing eNetwork Wireless Client Connection Profiles

You may have more than one profile in your eNetwork Wireless Client configuration. These profiles refer to connections to the eNetwork Wireless Gateway over different wireless networks or PSTNs and you can select one of them before entering the password and connecting to the gateway.

This section describes how to manage the profile settings.

4.2.8.1 Adding a Connection Profile

To add another modem definition, just start the eNetwork Wireless Client. Instead of selecting an existing profile, select **<Make New Connection>** as depicted in Figure 47 on page 117. This is a pseudo-entry which leads you to the same configuration panels that are described in 4.2.6, "Configuring the eNetwork Wireless Client" on page 116.

4.2.8.2 Deleting an Existing Connection Profile

To delete an existing profile start the eNetwork Wireless Client select the profile and press the **Delete** button. This deletes the profile from the configuration file.

4.2.8.3 Modifying a Connection Profile

In some cases, you may have problems with your modem or COM port settings. This may be because the Windows plug-and-play feature changed COM port assignments, or your PSTN modem or cell phone did not appear in the list. In these cases you have to review and possibly change the connection settings.

To do this, start the eNetwork Wireless Client, select the right connection profile and click the **Settings...** button to get the following panel.

The panel shown in Figure 64 on page 131 appears. This panel has several tabs:

- Options
- Connection Details
- Phone (on PSTN connections only)
- Counter
- Toolbar
- General

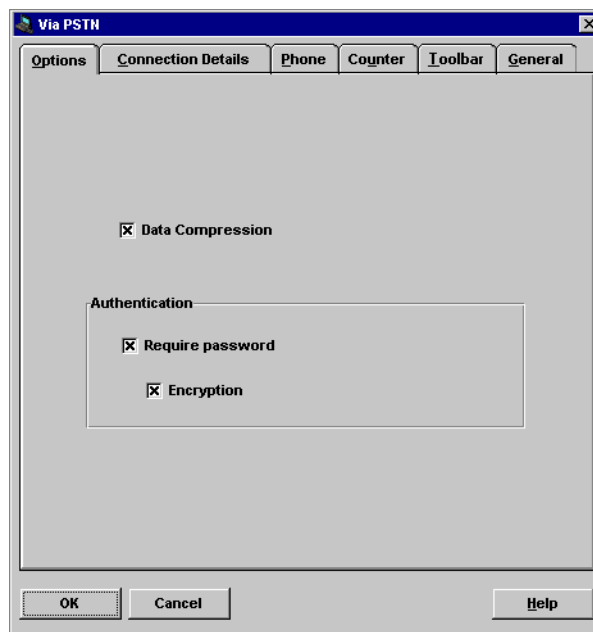


Figure 64. Settings Panel for PSTN Connections (Options Tab in Front)

The Options tab contains the data connection parameters. This panel doesn't contain any additional parameters.

Note

In former versions of the eNetwork Wireless Client software on the Options tab, you might have found a checkbox labeled Connecting to v.3.1.0 Gateway which had to be checked when setting up a connection to a Version 3 gateway.

The tabs Connection Details and Phone (latter for dial-connections only) are the only ones relevant for modifying a connection profile and are described in more detail in 4.2.8.4, “Modifying Connection Details in the Connection Profile” on page 132.

The Counter tab shows the client’s accumulated transmission statistics as described in 4.2.9.4, “The Client Toolbar” on page 136. It has a button to reset the statistics.

The Toolbar tab allows you to selectively display the eNetwork Wireless Client’s toolbar buttons.

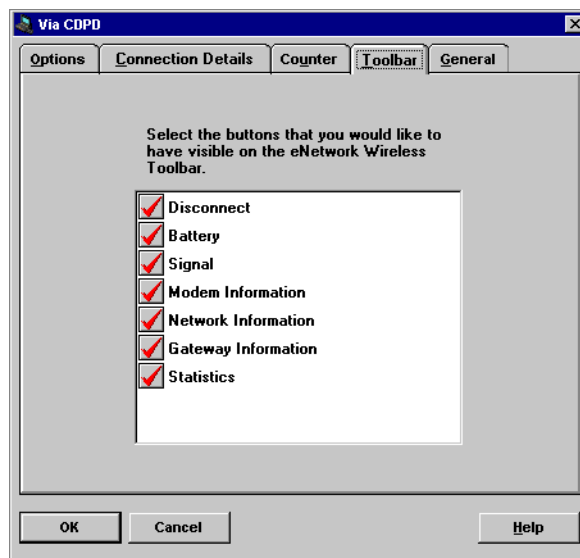


Figure 65. Settings Panel for CDPD Connections (Toolbar Tab in Front)

Finally there is the General tab which allows you to change the name of the connection and to specify whether an exit dialog should appear and whether the eNetwork Wireless Client should gracefully terminate the connection with the gateway upon exit.

4.2.8.4 Modifying Connection Details in the Connection Profile

The Connections Details tab differs between the wireless networks. For DataTAC type networks this panel doesn’t have any additional parameters.

For Mobitex networks this panel allows you to set the COM port speed and the modem’s power saving mode. Leave the default settings unless you really know what you are doing.

The CDPD Connection Detail tab allows you to set IP addresses and ports as well as modem initialization strings. Normally you do not have to change any of these values, except if the gateway administrator or CDPD provider tells you to change the network side.

The panel for network type PSTN is shown in Figure 66 on page 133. It allows you to configure the short-hold mode parameters.

The Suspend Timeout field specifies the amount of time in seconds that a connection has to be idle before the mobile client suspends it. Note that the

eNetwork Wireless Gateway also has a timeout configured and may enforce connection suspension. If the both client and gateway have a timeout value configured, the side with the value set to a shorter time period will suspend the connection. It is a good idea to set the gateway value to a long period and let the client usually initiate the short hold.

Specifying a value of 0 disables the mobile client short-hold timer, but does not affect the timer at the gateway.

The Connection Timeout field specifies the time period the client waits for a dial-up connection to be successfully established. If the connection is not established within this period, the client assumes that the gateway cannot be connected at his time due to lack of radio coverage.

There is also an option to enable suspend and resume dialogs.

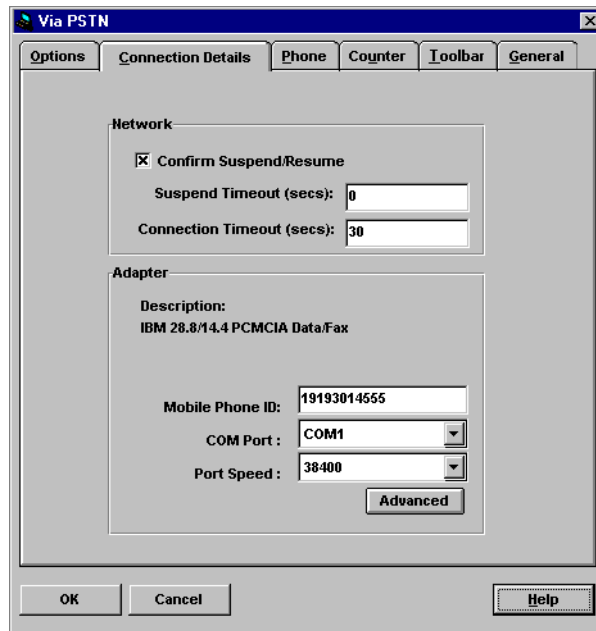


Figure 66. Settings Panel for PSTN Connections (Connection Details Tab in Front)

The **Advanced** button allows you to set every AT command string the client uses and the responses it expects from the modem. This makes it possible to adapt the client to modems which are not included in the modem list.

Under the Phone tab, you can change the dial information to call the gateway. This panel is similar to the one seen when creating a connection.

4.2.9 Preparing and Running the eNetwork Wireless Client

This section discusses the things you need to do before connecting to the eNetwork Wireless Gateway with the client and gives you some information about what you can do when you have a connection established.

Frequently used applications

In Windows OS, you almost always need to run these applications, so you better put them in one folder. The following applications are:

- PC Card
- Modem
- Network



Drag them from the Control Panel to your folder and create a shortcut.

4.2.9.1 Things to Do before Running the Client

Running a plug-and-play operating system lets your machine make changes to definitions which had worked previously. To make sure that your modem is ready and accessible under the COM port you defined at the client configuration, please check the following:

- On an NT machine you can run PC Card utility to check the PC Card status. The modem should be displayed either on socket 0 or 1, which refers to the PC Card slot you plugged the modem into. Then look at the COM port assignment by clicking the Properties option.

Note that Windows NT is not a plug and play operating system. It will require a reboot if you change a PC Card.

- In Windows 95, it's better to insert the modem after booting, if you change your PC Cards frequently. Then run the PC Card utility application and see whether it recognizes the modem or not. If it recognizes it, click the Modems application to see the COM port assigned to the PC Card and compare it with your eNetwork Wireless Client configuration.

4.2.9.2 Checking the Wireless Modem

Note: If you are using an external antenna, please do not forget to plug the antenna module cable in to your PC Card slot.

The wireless modem might have LEDs (Light Emitting Diodes) which may give you valuable information about modem status and coverage. Using the IBM Wireless Modems such as IBM Wireless Modem for ARDIS or CDPD which have an external module, you can find the LED on the back of the external module.

Note that this module is powered by batteries, which may go empty.

The meaning of the three LEDs are:

- OK status, means the antenna power status is OK or it still has enough power from the batteries, and the LED is green or off.
- Network status is the middle LED. It becomes green if the connection to the communication infrastructure is established.
- Traffic flow, if the first two stages above are successful, then the third LED blinks when the packets flow.

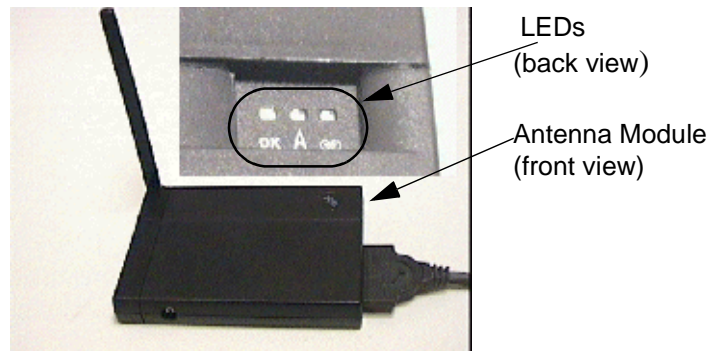


Figure 67. Antenna Module and LEDs on the Back

Figure 67 on page 135 shows the external module of an IBM Wireless Modem from both the front and back views.

4.2.9.3 Running the eNetwork Wireless Client

This section describes how we ran an eNetwork Wireless connection. This sample test was performed on a Windows NT notebook using an IBM CDPD Modem. We inserted the CDPD PC Card prior to booting the machine.

After starting the eNetwork Wireless Client we chose the profile named **Via CDPD** and clicked the **Connect** button.

At this stage, a connection panel shows up indicating the progress in establishing the connection to the gateway.



Figure 68. Connection Progress

It shows the following activities:

1. Initializing the modem, if it is successful, the first black bar above the small ThinkPad picture becomes green otherwise it continues initializing until timeout and an error occurs.
2. Then the modem tries to access the communication infrastructure. If it is successful, the second bar becomes green too, otherwise an error will occur.
3. During the third stage, the computer tries to access the gateway. If it is successful, the third bar also becomes green and the link from the Wireless Client to the Gateway is established, otherwise an error will occur.

Note: Please see Chapter 5, “Troubleshooting” on page 141 for more information on error situations.

After the connection to the gateway has been established you may then start TCP/IP-based applications.

4.2.9.4 The Client Toolbar

While the connection is established, the following eNetwork Wireless Client toolbar appears on the bottom right of your screen:

Figure 69 on page 136 shows the eNetwork Wireless Client toolbars for PSTN and CDPD connections. Note, that the actual display will vary by what type of network and modem you use, as well as the settings chosen on the Toolbar tab of the Settings panel.

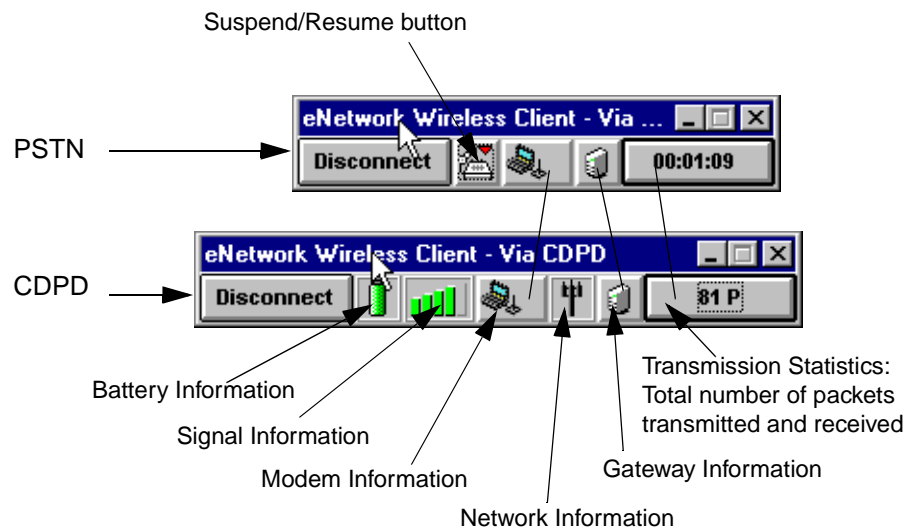


Figure 69. Toolbar's Button Information

- **Disconnect button:** Use this button to disconnect from the eNetwork Wireless Gateway and exit the client. Depending on the configuration settings on the General configuration tab, you might be prompted to confirm the disconnect.
- **Battery Information:** This icon shows the wireless modem's actual battery strength if the modem supports some means to get this value.
- **Signal Information:** The five bars on this icon give you information about which signal strength the wireless modem reports. This is only available if the modem provides some means for requesting this value. If signal strength is normally too weak for communication, only one bar appears, which is colored red. If it climbs to two bars, they become yellow and if the signal is getting stronger the bars become green.

Note

The bars shown are only a rough indicator of signal strength. With some experience, you may know at which level you probably run into communication problems. Note also, that there may be situations, where you notice a high signal but you cannot communicate due to interference problems. It may be the case, that the base station reaches the modem very well, but the modem cannot reach the base station.

- **Suspend/Resume** (Dial networks only): The Suspend/Resume button serves two purposes. One is to reflect the current status of the dial connection, showing an off hook or on hook icon. This is because the client automatically goes into short-hold mode (suspends) when there is no traffic going between the client and the gateway. When either the client or the gateway wants to send packets over the network it dials the other one thus resuming the connection. The other purpose of this button is to manually go into or come out of the short hold-mode by pressing this button. This button works as a toggle button.
- **Modem Information**: Pressing this button shows you detailed information on the modem and its settings. The window that shows up depends on the modem and the type of network. Figure 70 on page 137 shows an example for a CDPD modem.

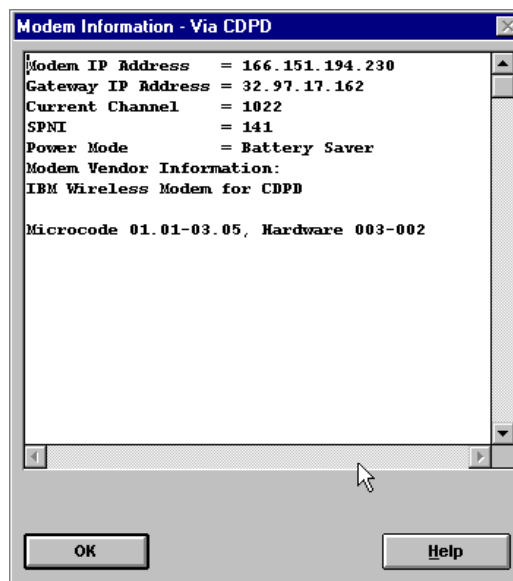


Figure 70. Modem Information for CDPD

- **Network Information**: This icon will be grayed out when the modem is not connected to a base station of the wireless network. It will be marked with a red X when it moves out of range of the base station.
- **Gateway Information**: This icon is grayed out until the eNetwork Wireless Client is connected to the gateway. When it is connected to the gateway you may click on this button to see the actual connection settings. Figure 71 on page 138 shows an example. The window that shows up also allows you to

change your password if it is not disabled by the startup options as described in 4.2.7.3. The fields in this window are self-explanatory.

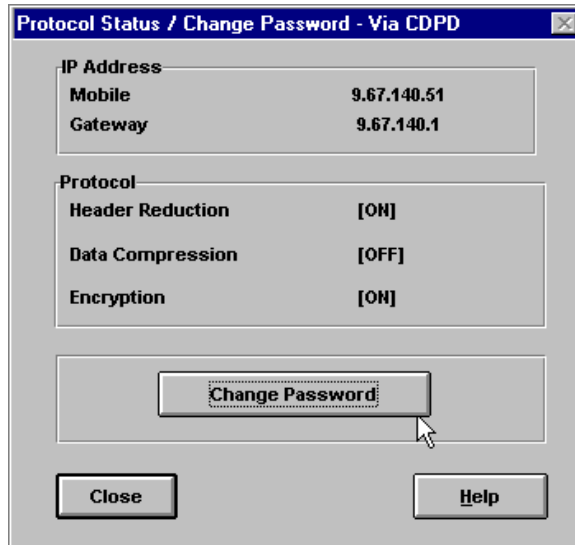


Figure 71. Gateway Information

- **Transmission Statistics:** This button shows a key value assigned to network transmissions, which depends on the type of radio network. On the PSTN toolbar it displays the time the connection is established (not counting short-hold periods). On packet radio networks like CDPD, the total number of packets sent and received is displayed.

You may click on this button to get a detailed statistics window. An example for CDPD networks is shown in Figure 72 on page 138.

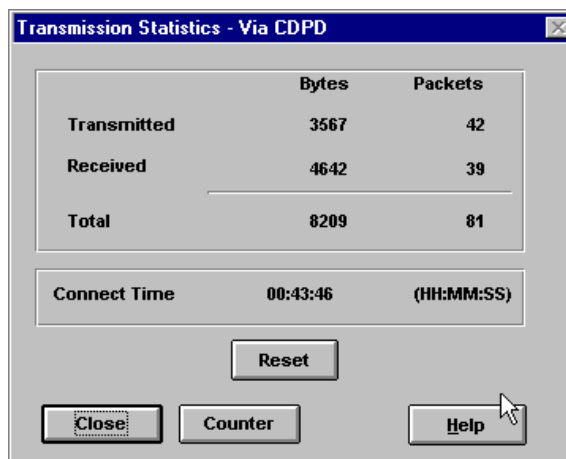


Figure 72. Transmission Statistics for CDPD

To monitor a communication sequence, you can reset the actual statistics values. There is another set of statistic counters which are saved between successive connections. You may access these values by clicking on the

Counter button. The values displayed then can also be seen on the Settings panel by clicking on the Counter tab.

Chapter 5. Troubleshooting

This chapter discusses common problems in eNetwork Wireless environments, how to do troubleshooting and who should fix the problem. The scope of troubleshooting to be discussed ranges from the eNetwork Wireless Client to the Gateway. Some problem handling at the application level, such as Web Express Client/Server, Emulator Express Client/Server are also discussed where appropriate.

From the discussion in this chapter, the eNetwork Wireless Administrator or eNetwork Wireless Client should be able to detect and fix the problems quickly.

5.1 A Communication Problem Overview

Connecting to a network such as a LAN is relatively much more stable than wireless technology. The LAN technology is much more robust in terms of the media usage, area coverage, connection speed etc. But there are still a lot of connection problems. Users sometimes cannot connect to the LAN even though the computer is physically attached to the LAN.

What about connecting to the network wirelessly?

Wireless technology is much more complicated than LAN technology. For example, the position of wireless users is different. While a LAN user sits in a fixed place in the office, a wireless user can be anywhere outside of the office and is mobile from one place to another. Another thing that makes wireless connections fragile is the wireless coverage area. The signal can be very strong one place and very weak or even nonexistent in other areas, say in the building.

In the eNetwork Wireless Network implementation, the media between client and gateway uses a wireless communication infrastructure such as DataTAC, CDPD, Mobitex network or Dataradio. The infrastructure is handled by another company that the gateway administrator never touches. If there are any problems in this area, end users and gateway administrators do not have access to fix, but may be able to inform the wireless provider who can then fix the problem.

5.2 Categories of Problems in Wireless Network Environments

As administrators or customer service representatives, we sometimes get a customer problem report with very limited information or symptoms. The end user only says that his/her computer is not operational and commonly does not know which part is causing the problem.

We can help our customer/user to solve the problem quickly if we can analyze the symptom we get from them. What do we have to do?

It is a good idea to analyze the problem by separating the problem into different parts. See the following picture:

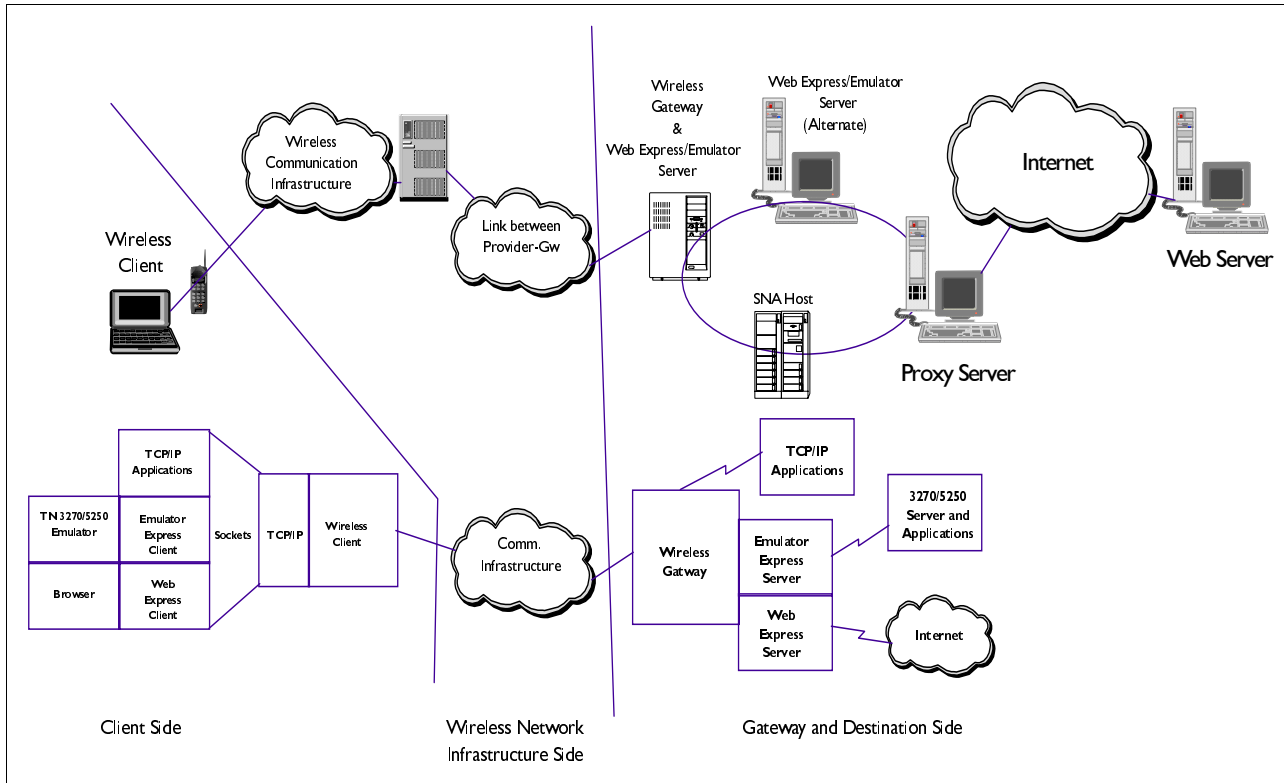


Figure 73. The eNetwork Wireless Components

The picture above illustrates the client and gateway components of an eNetwork Wireless network.

5.2.0.1 The eNetwork Wireless Components and Their Elements

In order to locate the problem, we separate the network into several components. Here are the four components involved:

- eNetwork Wireless Client side
- Wireless network infrastructure side
- eNetwork Wireless Gateway side
- The end application and other hardware/software between intranet and Internet.

5.2.0.2 Category of Problem

The problem can be caused by:

- eNetwork Wireless Client side
 - On this side the problem can be caused by applications such as:
 - Web browser, 5250/3270 emulation software or other TCP/IP application
 - Web Express Client or Emulator Express
 - TCP/IP stack and eNetwork Wireless client driver
 - COM port, modem or antenna
- The wireless communication infrastructure

Most of the problems in this area cannot be handled by either the eNetwork Wireless Client user or gateway administrator. Problems here can be caused by:

- The link between users to the communication infrastructure
- The link from communication infrastructure to the gateway
- The wireless gateway side

Gateway involves many parts of hardware and software. The problem can be caused by:

- Gateway physical WAN or LAN hardware such as:
 - X.25 card
 - COM port
 - ISDN card
 - LAN card (token-ring, Ethernet or any other type of LAN)
- Link problem to the wireless provider
- Gateway application such as:
 - eNetwork Wireless Gateway application or one of its subsystems
 - eNetwork Web Express Server application
 - eNetwork Emulator Express Server application, or
- External resources

The problem can also be caused by external gateway applications:

- The proxy server, firewall or other security boxes
- Communication box that communicates intranet and Internet
- HTTP Web server or Telnet 3270/5250 server

As an eNetwork Wireless Gateway administrator we should have the ability to access and detect the problem at least from the gateway. The following section discusses common problems and the ways we monitor and fix such problems.

5.3 Accessing the Wireless Network

If a radio modem cannot, for some reason, register with any base station, it will indicate the fact to the user by means of an "out of service" indicator.

The most common reasons for not being able to register are:

- The modem is not in an area of cellular coverage.
- The modem is in a "blackspot" (radio coverage hole).
- The base station is busy with other callers (often the case at GSM networks).
- The phone is not registered as a valid subscriber to the network.
- The phone is for some reason blacklisted (bill not paid).

Note

For a detailed description on how a successful login connection to the eNetwork Wireless gateway is obtained, see 4.2.9.3, "Running the eNetwork Wireless Client" on page 135.

5.4 X.25 Problems

Addressing X.25 problems depends on whether you are connected to a real X.25 network or are accessing the wireless network via X.25 over a leased line.

If connected to a real X.25 network it is a good idea to have at least one spare SVC requested from your X.25 provider and configured to your adapter. This allows you to test without the need to shut down the eNetwork Wireless Gateway in order to perform connectivity tests to other sites.

In every X.25 network you should find some network nodes which allow you to connect to and simply echo all the packets they are receiving. These stations are often referred to as *echo nodes*. Ask your X.25 network provider for the address of such an echo node.

There is a program included in the AIX Link software component, called:

```
xtalk
```

Refer to redbooks dealing with X.25 to learn how to configure this program.

In order to use the xtalk program, you must enable the Com I/O interface. Going down the following smit menus:

```
smitty devices
-> Communication
-> X.25 Coprocessor...
-> Adapter
-> Manage Device Drivers for X.25 CoProcessor/2 or Multiport/2 Adapters
-> Manage X.25 LPP Device Driver
-> Manage X.25 Ports
```

the screen should look like this:

Manage X.25 Ports

Move cursor to desired item and press Enter.

```
List All Defined Ports
Add Port
Move Port Definition
Change / Show Characteristics of Port
Remove Port
Configure a Defined Port / Interface
Add Comio Interface to Port
Remove Comio Interface from Port
```

F1=Help
Esc+9=Shell

F2=Refresh
Esc+0=Exit

F3=Cancel
Enter=Do

Esc+8=Image

If the last two lines are missing, you definitely have to install the AIX Link component:

```
sx25.comio.
```

This component also includes the xtalk program.

You must add the Comio interface to the X.25 port which is connected to the X.25 network before you can use xtalk. Remember to deactivate the Comio interface again before making parameter changes to the X.25 adapter. Otherwise the change operation will fail.

If everything goes wrong, you may trace the X.25 adapter. Call an X.25 expert to help you in this undertaking.

5.5 Mobile User Reports Problem

Just a view tips of how to start, when a user of a mobile client calls the eNetwork Wireless administrator and reports that he cannot get a connection now, but did have one some time before:

1. First check the ARTour.log file for error messages.
2. Get an actual status of the mobile client in eNetwork Wireless Gateway

```
lsARTour -devstatus
```

You will see the connection status and if connected, what has been negotiated at the eNetwork Wireless protocol level.

3. Look at the account file if you see any previous activity with that client.
4. If you cannot isolate the problem, turn on full logging and ask the mobile client to reconnect. Look if you see any activity in the ARTour.log file.

5. If you see no data coming in, check the radio network connectivity and the mobile client configuration. A listing of the client's artour.ini file helps.

5.6 Some Problem Scenarios, Analysis and Troubleshooting

This section discusses some possible problems in the real world where the eNetwork Wireless Client or Gateway administrator gets the problem and what action should be taken by the client or the administrator in order to resolve the problem.

5.6.1 General Information

5.6.1.1 Modem Identifier

The modem identifier is called different names in different network technologies:

Table 5. Modem Names

Network Provider	Modem ID Name
CDPD	Equipment ID (EID)
DataTAC (ARDIS)	- LLI (Logical Link Identifier) or - SUI (Subscriber Unit Identifier)
Mobitex	-MAN (Mobitex Access Number)

Note: You can see the modem ID on the back of the modem.

Assumptions

This troubleshooting scenario assumes that:

- Your modem is registered at the wireless communication provider, and you are connected to the wireless network.

Displaying the ARTour Log

Note: To monitor the ARTour activities on the log file, you can issue the command:

```
tail -f /val/adm/ARTour.log
```

The command will display the latest entry in the error log file.

5.6.2 The Problem Scenarios

To simulate the problem, we did the following scenarios by generating:

- eNetwork Wireless Gateway X.25 down
- eNetwork Wireless Gateway application down
- Invalid modem ID definition on the gateway
- Invalid gateway definition on eNetwork Wireless Client
- eNetwork Wireless Client types an invalid password

For these examples, we only discuss troubleshooting problems on an ARDIS network. Error and problem handling on other types of wireless networks are similar.

5.6.3 DataTAC ARDIS Network Problem

5.6.3.1 The eNetwork Wireless Gateway X.25 Down

In this scenario we brought the X.25 down by turning the modem off.

If X.25 is down, the problem may be caused by the following:

- The X.25 modem cable is disconnected.
- The modem malfunctioned.
- The X.25 card has malfunctioned.
- The X.25 link to the network provider is broken, in which case most probably the modem light is off.

Error Messages and Problems on eNetwork Wireless Client:

If X.25 is down while the client is connecting to the gateway, the following error message occurs:

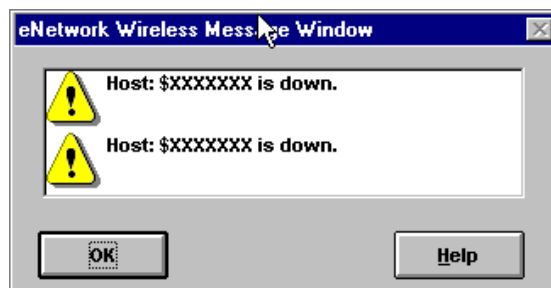


Figure 74. Host Down Error Message

Now, the eNetwork Wireless Client is disconnected and no traffic flows, but the client keeps trying to connect to the gateway. It repeats the error continuously until the gateway comes up or you turn the connection off.

- If the client is connected to the gateway and X.25 goes down, the message will be like this:

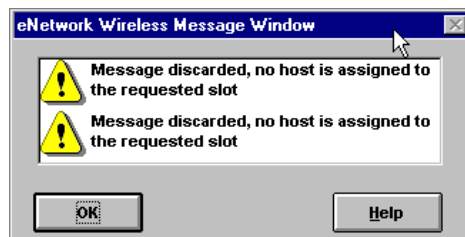


Figure 75. Gateway Available Error Message

The client cannot reach the Gateway

eNetwork Wireless Client Action:

In this case, the client actually cannot do anything, because the problem is not on the client side. The user should do the following:

- Call the administrator and provide the above error information.
- Wait for establishment.

eNetwork Wireless Gateway Action:

1. Check whether the application is running or not. Refer to Chapter 3, "Install, Configure and Manage the Wireless Gateway" on page 53 for more information.
2. Check physical X.25 connection by inspecting the modem connection, modem light and message on the console by issuing the following command:

```
lsARTour -devstatus
```

If the X.25 is the problem, the following error will be seen on the gateway console:

```
27878 (Nov 18 98/15:56:22): npi::read: received disconnect indication, reason=0
27878 (Nov 18 98/15:56:22): Ardis: lost connection to address '34525'
27878 (Nov 18 98/15:56:22): Ardis::drop (entry)
27878 (Nov 18 98/15:56:22): Trap: 'AG: connection dropped' (10.10.1.10/ardis)
27878 (Nov 18 98/15:56:22): Trap: 'AG: connection dropped' (10.10.1.20/ardis)
27878 (Nov 18 98/15:56:22): Ardis::drop (return), rc=0
27878 (Nov 18 98/15:56:22): LdX25::receive (return), rc=-1
27878 (Nov 18 98/15:56:22): IOMgr: rc=-1 from receive, rebuilding poll

26744 (Nov 18 98/15:56:27): LdX25::constructor (return), rc=0
26744 (Nov 18 98/15:56:27): LdX25::connect (entry)
26744 (Nov 18 98/15:56:27): npi::connect: received disconnect indication, reason=1024
26744 (Nov 18 98/15:56:27): LdX25::connect (return), rc=-1
26744 (Nov 18 98/15:56:27): X25LD: failed to establish connection (Operation already in progress)
26744 (Nov 18 98/15:56:27): Ardis::open (return), rc=-1
26744 (Nov 18 98/15:56:27): ARTourOpen: unable to open connection to '10.10.1.10', RDN 'ardis'
System call error number -1.
```

Figure 76. ARTour Log File (X.25 Problem)

In the above log, we see that X.25 is down. The gateway application is trying to re-establish the X.25 connection, which means there is something wrong with the X.25 hardware, modem or link to the ARDIS wireless provider.

3. Fix the physical hardware or link problem, and the gateway application should re-establish the X.25 link automatically.

When X.25 is up, the following messages appear on the console:

```
26744 (Nov 18 98/15:57:42): CMon: started (16)
26744 (Nov 18 98/15:57:42): Ardis::open (entry)
26744 (Nov 18 98/15:57:42): X25LD::open (entry)
26744 (Nov 18 98/15:57:42): LdX25::connect (entry)
26744 (Nov 18 98/15:57:42): LdX25::connect (return), rc=0
26744 (Nov 18 98/15:57:42): X25LD::open (return), rc=0
26744 (Nov 18 98/15:57:42): Ardis::open (return), rc=0
26744 (Nov 18 98/15:57:42): Trap: 'AG: connection open' (10.10.1.10/ardis)
26744 (Nov 18 98/15:57:42): Ardis::open (entry)
26744 (Nov 18 98/15:57:42): X25LD::open (entry)
26744 (Nov 18 98/15:57:42): X25LD::open (return), rc=0
26744 (Nov 18 98/15:57:42): Ardis::open (return), rc=0
26744 (Nov 18 98/15:57:42): Trap: 'AG: connection open' (10.10.1.20/ardis)
26744 (Nov 18 98/15:57:42): CMon: finished (16)
```

Figure 77. ARTour Log (X.25 UP)

5.6.3.2 The eNetwork Gateway Application Down

In this scenario we stopped the gateway application by changing the *current state* parameter on the mobile network interface from **UP** to **DOWN**.

If the X.25 link is up, but user cannot connect to the gateway, it could be caused by the following:

- Gateway application is not started
- TCP/IP subsystem problem

Problem and Error Messages on the eNetwork Wireless Client

The gateway application is down while the client is trying to connect to the gateway. The following error message will be seen:

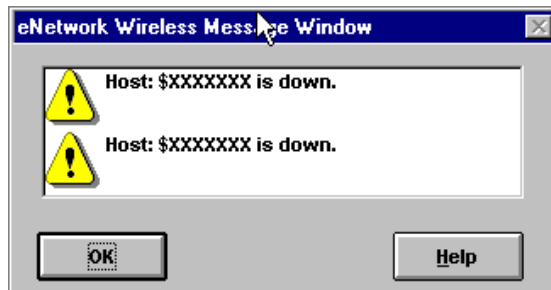


Figure 78. The Gateway Down Error Message

The client has reached the gateway over the communication link, such as X.25, but when it arrives there, the gateway is not available. This error is the same as the network link down. See the previous error.

The client will keep trying to reach the gateway until the user disconnects the client application.

eNetwork Wireless Client Action:

Since the problem is on the gateway side, wireless clients cannot fix the problem but they can:

- Call the administrator and provide the above error information.
- Wait for establishment and reconnect.

eNetwork Wireless Gateway Action:

As an administrator, check the error log first before doing other things:

1. Check WAN connection such as X.25 card, modem, etc.
2. See whether the application is running or not.
3. If the application is running, check the subsystem such as X.25 interfaces.

5.6.3.3 Invalid Modem Identifier on the Gateway

In this scenario we configure an invalid SUI (Subscriber Unit Identifier) definition on the gateway.

In the real world, this is very possible. The administrator or operator types a wrong SUI, or the client misuses a registered modem.

An incorrect SUI definition on the gateway can cause the following:

- The eNetwork Wireless Client cannot connect to the gateway.

Problem and Error Messages on the eNetwork Wireless Client

Even though the eNetwork Wireless Client connects to the gateway, the gateway rejects the connection, and displays the following error to the client:

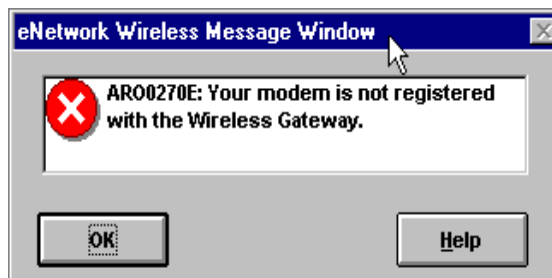


Figure 79. Unknown Modem Error Message

When you connect to the gateway, you will fail to make a connection, because the gateway application cannot recognize the incoming modem ID.

eNetwork Wireless Client Action:

In this case, the client uses a correct modem, but the modem ID is not recognized by the gateway. If we use an unregistered modem, the packet is discarded by the wireless network. In other words, the packet cannot arrive at the gateway. Do the following:

- Record your modem ID. **Note:** See the back of your modem.
- Contact the administrator and provide the above error information and modem ID.
- Retry to connect after the modem definition on the gateway is fixed.

eNetwork Wireless Gateway Administrator Action:

The administrator can check the log file, but unfortunately there is no message of the unregistered incoming modem. Administrator should correct the wrong modem ID on the gateway.

5.6.3.4 eNetwork Wireless Client Uses an Invalid Gateway Definition

In this scenario we configure an invalid gateway address on eNetwork Wireless Client. In the real world this is common, if the gateway administrator or operator enters incorrect gateway information.

An invalid gateway definition on the client can cause the following:

- The eNetwork Wireless Client cannot connect to the gateway.

Problem and Error Messages on the eNetwork Wireless Client

When the eNetwork Wireless Client uses an invalid gateway address, the following message appears.

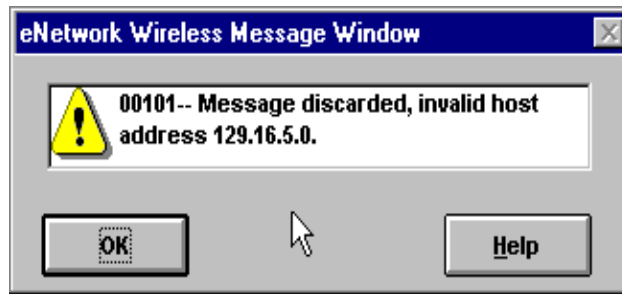


Figure 80. Invalid Gateway Address Error Message

This message indicates that the wireless gateway couldn't be reached.

User should know the gateway address. This address is provided by the administrator. See Chapter 4, "Wireless Client" on page 107 for more information.

eNetwork Wireless Client User Action:

- Verify that you have entered the correct gateway address in the Wireless Client Configuration. If the problem continues, contact the gateway administrator.

eNetwork Wireless Gateway Action:

Provide the client with the correct gateway address.

5.6.3.5 eNetwork Wireless Client Uses an Invalid Password

In this scenario we entered an invalid password on eNetwork Wireless Client. In the real world, it is easy to type an invalid password.

Attempting to reach the gateway with a wrong password can cause the following problems on the client side:

- The eNetwork Wireless Client cannot connect to the gateway.
- The ID will be automatically locked by the gateway application.

Problem and Error Messages on the eNetwork Wireless Client

When the eNetwork Wireless Client tries connecting to the gateway with an invalid password, the following error occurs:

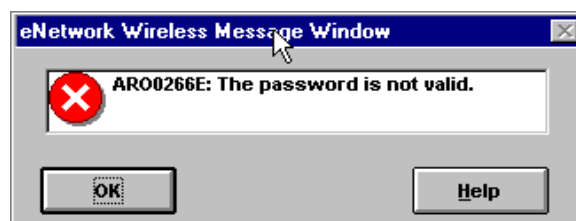


Figure 81. Invalid Password Error Message

User should know the password provided by the administrator. See Chapter 4, "Wireless Client" on page 107 for more information.

eNetwork Wireless Client User Action:

- If you know the correct one, change it, otherwise call the administrator for the correct password and change it.

- Re-connect the eNetwork Wireless Client.

Gateway Locks the User

If an eNetwork Wireless Client tries to connect a number of times and exceeds the maximum allowed, the account is locked. Further login attempts will be rejected. The following message appears on the eNetwork Wireless Client.



Figure 82. Locked Account Error Message

eNetwork Wireless Client User Action:

- You have to report to the gateway administrator anyway to get a new password.

eNetwork Wireless Gateway action:

The administrator can see the user status from SMITTY menu. Here we can see that the user is locked.

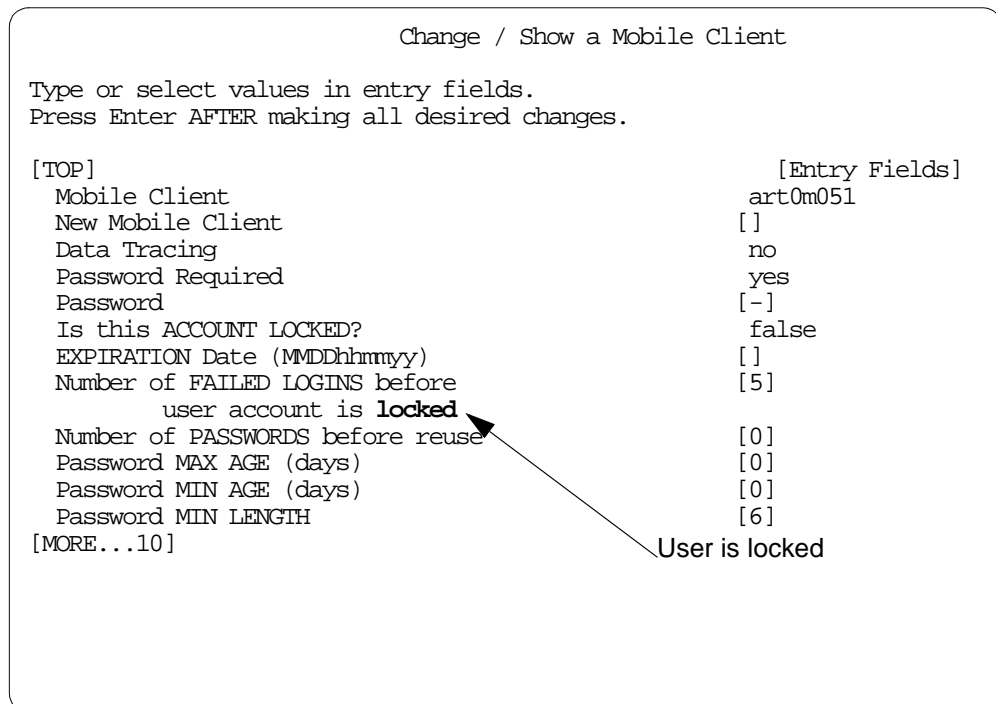


Figure 83. Showing a Mobile Client Status

Administrator can see that the user is locked, and if it is necessary, a new password can be created for that user. See Chapter 3, "Install, Configure and Manage the Wireless Gateway" on page 53 for details.

Chapter 6. Performance and Security Issues

In this chapter we will discuss some issues related to the eNetwork Wireless Gateway and Client performance. This performance depends heavily on the wireless network technology and the network provider you are connected to, especially the network load produced by other subscribers having a big impact. Therefore we won't come up with performance values, but put you into the position to perform measurements by yourself and give you some hints how to do some optimization. We also give you some configuration information for the eNetwork Wireless Gateway for varying numbers of users.

With the eNetwork Wireless Gateway installed at a customer site, the corporate network may become exposed to potential penetration. After reading the security issues in this chapter, you will understand why the eNetwork Wireless Gateway, provided that it is configured correctly, can be considered as a safe and secure bridge between the enterprise network and the mobile clients; thus, the gateway may be safely placed within the enterprise network.

Another exposure exists, when the eNetwork Wireless Gateway is connected to a wireless network provider via TCP/IP. No matter how this connection is physically made, since the wireless network provider is connected to the Internet, you will have to consider this IP interface as a link to the Internet as well. This chapter will give you some background information and tips on how to build secure configurations, even when the gateway has to be connected to the Internet.

6.1 Measuring Performance

Performance of eNetwork Wireless configurations depends most heavily on the wireless networks. In most cases, the relevant packet delays are not in the eNetwork Wireless software but rather in the wireless or wireline networks themselves. Note for example, that benchmarking Web page downloads, easily may measure overloaded Web servers instead of the wireless access.

The MTU size which the IP stack on an endpoint system uses for transmitting packets may vary significantly depending upon the networks and routers the packet passes until it finally reaches its destination. Therefore, keep in mind, that results from measurements with server applications located on the eNetwork Wireless Gateway itself may differ from measurements when the server applications are located somewhere else in the intranet.

The mobile client and the gateway's mobile network interface are in the same IP subnet, while other machines are in a different IP subnet with the eNetwork Wireless Gateway acting as a router.

6.1.1 Measuring Wireless Network Transmission Parameters

The first thing you may want to know about are the packet transmission characteristics of the wireless network you are using. The program *ping* enables you to get packets transmitted in the size you want and gives the round trip times (RTT) for each packet. By comparing RTT for various packet sizes, you may get values for the basic transmission time which have to be added to each packet and a portion dependent on the packet size. The ping program also reports lost packets, giving you some idea of the wireless network's reliability. Note that due

to the restricted bandwidth you will have to configure an appropriate *wait interval* for making correct measurements.

Keep in mind that you always measure both transmission directions at the same time. Results may vary significantly over time. Measurements performed one day may differ significantly from tests you've done the day before.

Below you find an example. It assumes that you have access to the client and the gateway at the same time. We did this test with a Windows 95 client connected via the ARDIS radio network. The mobile network interface has been given the IP address 10.10.1.1. Note, however, that your results may be totally different.

1. Log into the eNetwork Wireless Gateway and get yourself a Telnet session or an XTERM window on an X server. In that window, issue the command:

```
ARTouracct -f -l 10
```

This command gives you the last 10 packets and sets up a running display to show you what is going on.

2. Start the eNetwork Wireless Client and log on.
3. Open the Statistics window and reset the values.
4. Open a command line window and issue the ping command with short packets, like this:

```
C:\WINDOWS>ping -l 10 -w 5000 10.10.1.1
```

```
Pinging 10.10.1.1 with 10 bytes of data:
```

```
Reply from 10.10.1.1: bytes=10 time=2189ms TTL=255
```

```
Reply from 10.10.1.1: bytes=10 time=2298ms TTL=255
```

```
Request timed out.
```

```
Request timed out.
```

5. Look at the Statistics window:

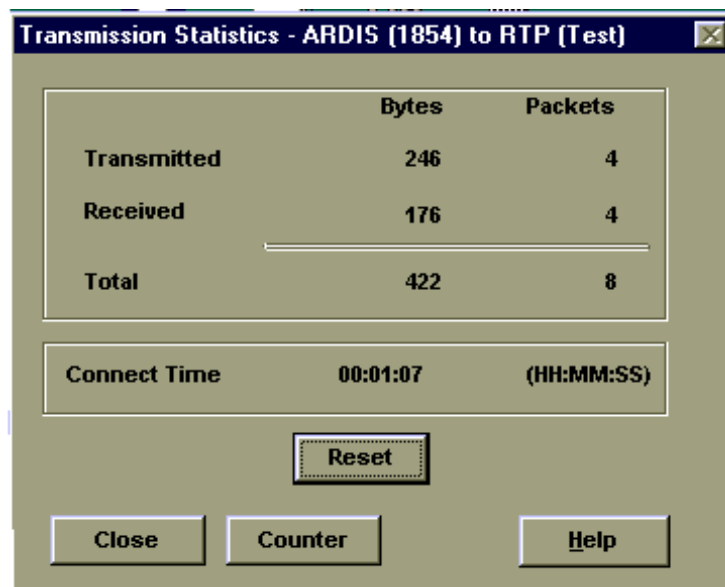


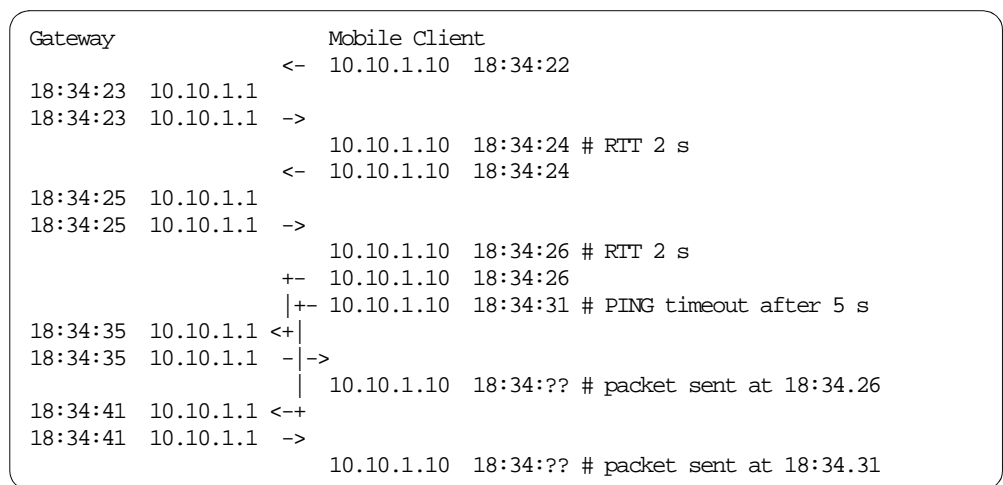
Figure 84. eNetwork Wireless Client Statistics after a Small Packet PING Command

6. Look at the eNetwork Wireless Gateway Account file. The following screen shot shows the accounting records resulting from the PING command on the client shown above under item 4. Every packet crossing the eNetwork Wireless Gateway is logged showing the IP addresses of the mobile client and the destination host in the wireline network. The arrow indicates the packet direction. The time stamp refers to the instance when the packet was sent or received by the gateway. The numbers on the six rightmost columns indicate the packet sizes on the different eNetwork Wireless protocol layers.

Date	/	Time	Other Dev.		Mobile Dev.	Network	IP	Red	Comp	Cryp	Fram	Sent
Nov 16	98/18:33:30		10.10.1.1	<-	10.10.1.10	ardis	-	-	-	-	68	86
Nov 16	98/18:33:30		10.10.1.1	->	10.10.1.10	ardis	-	-	-	-	11	32
Nov 16	98/18:33:30		10.10.1.1	->	10.10.1.10	ardis	-	-	-	-	73	94
Nov 16	98/18:33:37		10.10.1.1	<-	10.10.1.10	ardis	-	-	-	-	64	82
Nov 16	98/18:33:37		10.10.1.1	->	10.10.1.10	ardis	-	-	-	-	34	55
Nov 16	98/18:33:43		10.10.1.1	<-	10.10.1.10	ardis	-	-	-	-	56	74
Nov 16	98/18:34:23		10.10.1.1	<-	10.10.1.10	ardis	38	-	-	41	43	61
Nov 16	98/18:34:23		10.10.1.1	->	10.10.1.10	ardis	38	-	-	41	43	64
Nov 16	98/18:34:25		10.10.1.1	<-	10.10.1.10	ardis	38	-	-	41	43	61
Nov 16	98/18:34:25		10.10.1.1	->	10.10.1.10	ardis	38	-	-	41	43	64
Nov 16	98/18:34:35		10.10.1.1	<-	10.10.1.10	ardis	38	-	-	41	43	61
Nov 16	98/18:34:35		10.10.1.1	->	10.10.1.10	ardis	38	-	-	41	43	64
Nov 16	98/18:34:41		10.10.1.1	<-	10.10.1.10	ardis	38	-	-	41	43	61
Nov 16	98/18:34:41		10.10.1.1	->	10.10.1.10	ardis	38	-	-	41	43	64
Nov 16	98/18:40:14		10.10.1.1	<-	10.10.1.10	ardis	-	-	-	-	11	29
Nov 16	98/18:40:14		10.10.1.1	->	10.10.1.10	ardis	-	-	-	-	7	28

Figure 85. eNetwork Wireless Account File

In the example above you see that compression was turned off because the column with the title *Red* (stands for reduction) has dashes only. Only packets where there is no dash in the *IP* column are IP packets. The others are eNetwork Wireless control packets from logging in and out of the gateway. When you combine this log with the information you received on the client that packets 1 and 2 had a round trip delay of about 2 seconds, you can reconstruct the following scenario:



You see, that the third packet took 9 seconds and the fourth packet took 10 seconds to transmit.

Note

To measure Round Trip Times (RTT) it is better to ping the client from the gateway. However, having the client and gateway machines not close together and having no way to establish a telnet connection to it, you have to go with PING commands originated by the client.

As shown in the example above, pings from the client allow you to perform pretty accurate transmission time measurements from the client to the gateway.

Some tips when using ping:

- Always ping to a numeric IP address, not a host name. Pinging to numeric IP addresses will prevent the measurement from being distorted by name server lookups. A good idea is to ping the eNetwork Wireless Gateway mobile interface.
- Specify a time-out value of several seconds when going over packet-oriented networks like ARDIS or Mobitex.
- The ping command syntax varies between Windows95 and Windows/NT.
- Note that the ping command may get mixed up if the response from the first packet arrives after the second one has been transmitted. Ping will time-out all following packets. In that case use the eNetwork Wireless Client statistics to check how many packets have been received. Reset the statistics and then issue the ping command. Wait some time and the difference between the sent and received packets will give you the packets lost on the wireless network. So, be sure to have the time-out value set long enough.
- Wait some time between two measurements to allow the wireless network to deliver outstanding packets.
- You should repeat your tests several times at different times of the day.
- You can get a running display of the eNetwork Wireless Gateway account file and save it to a file (here xx.log) for later analysis with the following command:

```
ARTouracct -f -l 10 | tee - xx.log
```

- When other people are on the system, you may use the *grep* command to filter out the correct lines from the file or use the parameter *-m* in the ARTouracct command (example here with IP address 10.10.1.10):

```
ARTouracct -f -l 10 -m 10.10.1.10
```

6.1.2 Benchmarking Application Scenarios

The performance of an eNetwork Wireless solution depends on different factors:

- Wireless network
- Application characteristics (the way the application client and server part communicate over TCP/IP), see also 1.6, "Optimizing Other TCP/IP-Based Applications" on page 10.

- Wireline network connection between the eNetwork Wireless Gateway and the application server.
- The way the application is used (interactive/replication).

There may be two main reasons for benchmarking an application scenario. The first one is to check whether the scenario is feasible at all. The second one is to compare different solution strategies or options for this application scenario.

In any case, you have to find application scenarios which easily can be reproduced under identical conditions. The things you may measure while exercising the use cases are:

- Response times
- Exchanged data volume (may be measured in bytes **and** packets)

Pay attention to the preconditions, especially when there are caching mechanisms used at some point. Be sure that the caches are either properly preloaded or they are empty, but don't mix them up. Also be aware of caches which are not under your control, for example at Web proxies included in your firewall.

Since the overall environment may change significantly during the day and between different days, you should repeat your tests several times when the use cases actually will happen in real life. When comparing two configurations, do interleaved tests, so changes in performance of the infrastructure will compensate over several test runs.

Note that for packet-oriented networks time is not the most important issue. Usually, the customer will have to pay for the number of packets and/or data volume. You can measure both values at your mobile client with the Statistics window. You can reset the statistics before you start the scenario while keeping the total statistics for the session.

Similar to the previous test with the *ping* command, it is a good idea to have both sides of the solution under control, the mobile client and the eNetwork Wireless Gateway. If possible, try to have a look at the application server, too. That means you should have two computers, one connected to the eNetwork Wireless Gateway (and probably to the application server) and the other being the mobile client.

As described in 6.1.1, "Measuring Wireless Network Transmission Parameters" on page 153, you may use the ARTouracct command to see the packets flowing from and to the eNetwork Wireless Gateway. You may also use the accounting statistics functions to get cumulative results.

When the results are not the ones you expected, you may want to analyze what's happening on the link between the mobile client and the server, in order to check for misbehavior due to the wireless connection, for example, retransmissions or out of sequence delivery. To do so, the eNetwork Wireless Gateway provides you with packet tracing facilities.

Note

Tracing packets will put extra load on the eNetwork Wireless Gateway and shouldn't be left turned on without a need. Tracing single clients should not be a problem. Be sure to have enough disk space in the `/var/adm` directory where eNetwork Wireless Gateway usually puts its log and trace files.

Do not forget to deactivate the trace after you finish your test.

When you are testing performance you may not want to be disturbed by other activities. Not-captured interleaved transactions may severely distort your measurement. On the other hand, stressing the system with performance tests may bother other users. So, use a test environment, if you can. Otherwise inform the other users and the responsible administrators.

The following procedure may be used as a template for application performance tests.

1. Select a new set of files:

```
smitty artour -> File Management -> Use new Set of Log Files
```

You may delete the old files or move them to another place in the file system to get some free space on the directory `/var/adm`.

2. Activate the trace for the mobile client:

```
smitty artour
-> Mobile Client Configuration
-> Change / Show a Mobile Client
```

Select the mobile client and set the parameter `Data Tracing` to `yes`.

3. Set up a running window of the account file. You may stream the output to a file simultaneously using the `tee` command. (See Chapter 5, "Troubleshooting" on page 141 on how to do this.)
4. Start the eNetwork Wireless Client software and log in to the gateway. Watch the login process on the server window.
5. Now perform the test scenario. This depends on the application you are testing.
6. End the ARTouracct command by pressing Control-C.
7. Disable the tracing (see item 2 but set the parameter to `no`).
8. Look at the trace using:

```
smitty artour -> File Management -> Show Trace Information
```

If you are the only one who is tracing and you reset the trace file before performing the test, you do not need to fill anything in the following panel. Press Enter to look at the trace within smitty. It may look like this:

```

COMMAND STATUS

Command: OK          stdout: yes          stderr: no

Before command completion, additional instructions may appear below.

[TOP]

Nov 17 98/16:06:12    192.1.1.200 <- 192.1.1.100    62
PPP-LCP: Configure Request id=0x01
<magic 0x36520e72> <pcomp> <accomp> <encrypt CDMF>
<auth TPKDP MD5> <VJ-red> <ip-addr 10.10.1.10>
<TPKDP Key Request nonce=165dab6e375d8400ba8ea3c2c912fbc2 peer=4d4f42494c45>

Nov 17 98/16:06:12    192.1.1.200 -> 192.1.1.100    12
PPP-LCP: Configure Nack id=0x01
<ip-addr 192.1.1.100>

--- some lines missing ---
Nov 17 98/16:16:50    192.1.1.200 <- 192.1.1.100    94
IP
V: 0x04, L: 0x05, TOS: 0x00, Total Len: 0x5e
Ident: 0xaa37, FragOffs: 0x00
Time: 0x80, Prot: 0x11, HdrChecksum: 0x0d29
Src IP Addr: 192.1.1.100
Dst IP Addr: 192.1.1.200
UDP
Src Port: 0x22b8, Dst Port: 0x22b8
Length: 0x4a, Checksum: 0x8fde
0000:   i   t   s   o   0   1   .   .   .
      69  74  73  6f  30  31  .   .   .

[MORE...6]

F1=Help          F2=Refresh          F3=Cancel          Esc+6=Command
Esc+8=Image      Esc+9=Shell         Esc+0=Exit         /=Find
n=Find Next

```

In this trace, you will see all packets belonging to the eNetwork Wireless protocol and all IP packets in both directions decoded up to TCP or UDP level. This allows you to check for retries, out of sequence packets and so on.

You may specify an output file and process it with a text editor or some scripts to extract the fields you are interested in. You may find that *awk* or *perl* scripts ease your life tremendously when you try to understand what happens in this connection.

6.2 Optimizing IP MTU Sizes for Single Radio Networks

Both the IP stack and the eNetwork Wireless Software provide the functionality to fragment messages according to Maximum Transmission Unit (MTU) size of the underlying network. The IP stack regards the mobile network interface as the underlying network. eNetwork Wireless, however has to deal with different MTU sizes depending on the wireless network over which the mobile user is connected.

The MTU size for the eNetwork Wireless Client or Gateway in the IP stack is a constant value and is determined at boot time on Windows systems. So, when

dealing with different wireless networks either at the client or the server side, you will have to make a compromise, which means using the default values is usually a good choice.

If, however an eNetwork Wireless installation only works with one wireless network, or if one client does not switch between wireless networks, you may want to optimize the wireless network performance by setting the MTU size to take into account the maximum message size of the wireless network. This has the advantage that the eNetwork Wireless Software does not need to fragment packets received from the IP stack, where they may have been fragmented already. This usually results in better performance values.

Optimizing the MTU size at the client is most effective when large amounts of data are to be sent to the wireline network using a TCP connection. This is because TCP may adjust its flow control mechanism to the MTU size of the interface below. The value of the MTU size is located in the *eNetwork Wireless Interface*. The methods by which it is set differ between operating systems.

In Windows 95 you are able to set the MTU size Adapter tab of the Network Settings panel. Open the Start menu, select Settings and open the Control Panel. Find the Network icon and open it. Select the Adapter tab and there select the *IBM eNetwork Wireless Interface*. Click on Properties and you should see the window shown in Figure 86 on page 161.

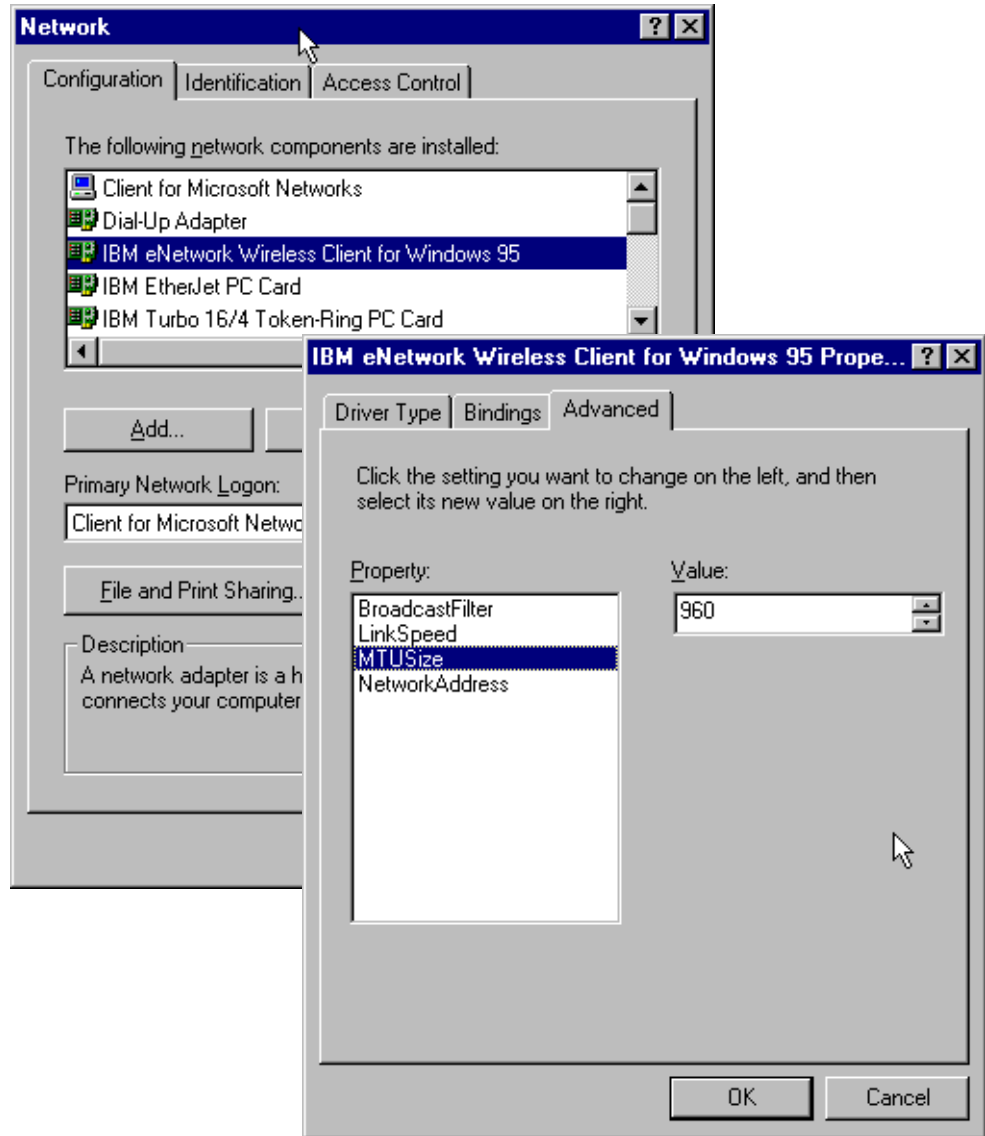


Figure 86. Setting the MTU Size of the eNetwork Wireless Interface on Windows 95

In this panel you can set the MTU size to whatever you need and close all panels. Restart Windows 95. The next time you start the eNetwork Wireless Client, the new MTU size value will be used.

Note

In order to set the MTU size on a Windows NT client, you will have to edit the Windows Registry manually. This is complicated and you can damage your system severely. Be aware, that you do this at your own risk.

This is the method for changing the MTUSize under Windows NT 4.0:

1. Press the **Start** button and select Run. Enter **regedit** in the prompt and press the **OK** button.

2. When the Registry Editor is opened, select the following registry-key by pressing the "+" character next to each key. Open the folder:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ARTour#\Parameters`
3. Select the Value Name MTUSize (case sensitive) and choose Edit, Modify.
4. Fill in the value for the MTUSize (for example, 500). Make sure the "decimal" radio button is selected.
5. Save and close the Registry Editor by choosing Registry, Exit.
6. You will have to restart Windows NT in order for the changes to take effect.

Finding a good value for the MTU size presented to the IP stack, is a difficult task. It depends on how efficiently eNetwork Wireless is able to compress packets received from IP. Let us assume that the packet size is not changed by the compression and TCP header reduction function. This may be the case, that it is switched off, or the data is not compressible. In this case the optimal MTU size will be the maximum message size of the radio network minus the eNetwork Wireless protocol overhead for that wireless network. This value is around 4 to 8 bytes for the current version. Having a radio network, supporting 512 bytes only, for example, 500 would be a good choice, but the best thing to do is to determine this value by running some tests yourself. You can do this by performing an FTP PUT operation on the client.

When considering to reduce the MTU size the eNetwork Wireless Gateway's mobile network interface presents to the IP stack, be aware that the gateway acts as an IP router. It gets packets from the intranet and sends them to the mobile network interface. Now you could argue that the gateway already receives packets of a specific maximum size and it doesn't matter which party is going to fragment them, the gateway's IP stack or the eNetwork Wireless Gateway software itself. You may, therefore, prefer to set the MTU size to its maximum and let eNetwork Wireless fragment the packets after compression.

The eNetwork Wireless Gateway has two types of MTU sizes configured in the mobile network interface section. The MTU size that is associated with the mobile network interface by the eNetwork Wireless Gateway is called *Maximum IP Packet Size*. This is one value for all mobile network connections. For each mobile network connection the gateway supports, there is an MTU value too. For example, for the DataTAC-ARDIS network this is called *ARDIS Maximum Transmission Unit*. This value always has to be set to the maximum message size the radio network supports, or at which the radio network shows optimal performance.

To prevent the eNetwork Wireless Gateway from fragmenting packets received from the IP stack, you must set the Maximum IP Packet Size of the mobile network interface. Note that this change affects all mobile network connections.

6.3 How eNetwork Wireless Scales

When planning eNetwork Wireless solutions, it is important to know which hardware has to be used for a specific number of users assuming a certain activity. First of all, the eNetwork Wireless marketing group will provide answers on which RS/6000 configuration will fit the customer's needs.

Development is frequently asked to provide specific RS/6000 configuration information and here there are some numbers, which have been compiled in 1998.

The eNetwork Wireless Gateway “solution” capacity (measured by number of simultaneous clients) is very dependent on the type of wireless network - packet vs. circuit switched - and connectivity to that wireless network. It is realistic to expect the “processing” in the eNetwork Wireless Gateway to support thousands of clients, for example 10,000 or maybe more. However, it is more likely that physical limitations will restrict connectivity to wireless networks, like the number of phone lines you can put on the gateway or the link capacity to your wireless network provider.

The methodology to get these numbers was to determine platform architectural constraints or bottlenecks and size capacity requirements to install and operate applications on a per user basis and at various usage levels. Then required processor speed and RAM capacity would be calculated.

The estimates are based on the following assumptions:

- AIX 4.3 (64-bit).
- Configurations do not take into account recommended high availability requirements.
- No other applications are installed or running on the RS/6000.
- Most connections are made from packet-radio networks such as DataTAC (American Mobile ARDIS), Mobitex (BellSouth Wireless Data) and CDPD.
- Routine Wireless Gateway user administration will be done via network management, for example, Tivoli NetView running on a separate system.
- Maximum of approximately 65% of the users registered on the eNetwork Wireless Gateway are concurrently logged-in.
- Wireless Gateway logging is only turned on for problem determination.
- Accounting file is processed in a timely fashion (Wireless Gateway).
- Compression and encryption are enabled on the eNetwork Wireless Gateway, except eNetwork Wireless Client compression is disabled when primary application is Emulator Express.

Please note the following disclaimer:

While the information contained herein is based upon our knowledge of the respective products, it is nevertheless only an estimate; it is not based upon specific benchmarks. Due to the large number of usage variables, specific requirements for individual situations will vary widely.

Configuration requirements for eNetwork Wireless Gateway and (eNetwork Emulator Express Server for AIX are expected to change as additional performance and capacity information becomes known to the development team.

Table 6. Scalability of the eNetwork Wireless Gateway

Users	RS/6000 Model	Processor	RAM	Hard Drive
100	43P 7043-140	200 MHz	64 MB	2.1 GB
500	43P 7043-140	200 MHz	96 MB	2.1 GB
1000	43P 7043-140	233 MHz	128 MB	2.1 GB
5000 (light)	43P 7043-140	233 MHz	256 MB	2 x 2.1 GB
5000 (heavy)	43P 7043-140	332 MHz	256 MB	2 x 2.1 GB
10000	43P 7043-140	332 MHz	512 MB	4.5 GB

6.4 Security Issues

The eNetwork Wireless Gateway acts as a routing device, allowing IP packets coming from wireless or dial-up networks. That means that anyone registered to one of these networks (for PSTN dial-up, no registration is necessary) may try to penetrate the corporate network. The terms corporate network and intranet are used as synonyms in this section.

This section outlines the possible security threats that apply to a remote access router in general and then explains how eNetwork Wireless Gateway and Client addresses them.

One security threat is the exposure of the corporate network to the world outside the company buildings or a firewall. Using a proprietary protocol to access a remote access router does not automatically lead to a secure system. You may compare this threat to an eNetwork Wireless Gateway with the one for a PPP dial in server, with the exception that over a wireless network (dependent on the technology) it may be easier to listen to traffic and to send arbitrary packets to the eNetwork Wireless Gateway. This includes replay attacks.

Another exposure is the remote access router itself. Rather than trying to penetrate the corporate network, a potential aggressor can also try to break into the access router, if it supports some remote operation facility, like the eNetwork Wireless Gateway does. The potential intruder may try to establish regular permission to access the intranet. Since normally the eNetwork Wireless Gateway can be managed using telnet and SNMP, this is possible in principal. Of course managing the gateway remotely can be turned off, but is very useful even when you use this for debugging purposes only.

However, it must be said, that the AIX operating system itself has powerful means to prevent the system from unauthorized access, as long as the suggestions to make the system safe are followed. One of the most important things is to strictly obey the password rules for every account.

The level of network security can only be measured against the company's requirements and the process followed for the rest to this intranet. This is normally expressed in a network a security policy, which every company should have. This policy describes which accesses are tolerated to allow the required business activities and the circumstances under which they have to happen. This

includes physical access to essential network resources and their management. Note, that a network security policy has to be known to and obeyed by all employees accessing the intranet remotely. All efforts to establish network security are easily bypassed by careless users, for example, when users store their passwords (even encrypted by the client software) on their notebook and leave it unattended. Also automatic startup routines which include the entering of passwords contradicts any network security policy.

Assuming that a security policy exists and eNetwork Wireless is going to be installed, include in this policy that the eNetwork Wireless password and encryption functions have to be activated for every user defined in the gateway. The use of passwords can be required by the gateway and password rules can be applied satisfying higher requirements concerning a password policy.

Regarding physical access to the machine itself, treat the eNetwork Wireless Gateway as any other routing device or access server in the intranet. We recommend locating such devices in restricted access areas.

The following section discusses the security aspects of different possibilities where to place the eNetwork Wireless Gateway and how to connect it to the intranet and, if required, to the Internet.

6.4.1 Not Connected to the Internet

If the eNetwork Wireless Gateway is only connected to wireless networks without using TCP/IP protocols, as depicted in Figure 87 on page 165, you have to trust the wireless network provider that there will be no risk of penetration from the provider itself. As long as there is a special protocol, there will be no possibility to access applications other than the eNetwork Wireless Gateway itself.

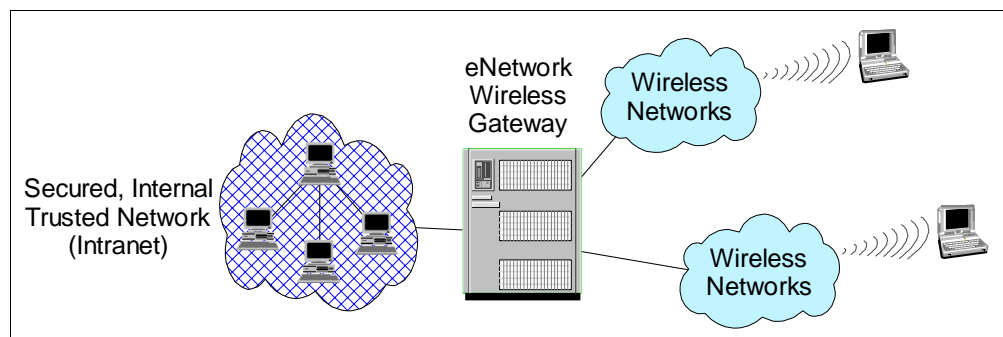


Figure 87. Intranet Access via eNetwork Wireless Gateway

The eNetwork Wireless Software itself can be considered safe, provided passwords are required and encryption is turned on by all clients. This is due to the following reasons:

1. eNetwork Wireless provides two-way authentication using the *Two Party Key Distribution Protocol* (2PKDP). With this protocol the client authenticates itself against the gateway using a password as a shared secret and the gateway authenticates itself against the client by proving that it could decode some arbitrary information which can only be decoded by knowing the password. The password itself is only used for encryption and decryption, and is not transmitted over the communication channel.

2. In the authentication phase eNetwork Wireless Gateway and Client exchange a session key which is used after connection establishment to encrypt each packet.

Both security mechanisms are resistant to interception, and replay attacks. They secure the communication channel between the client and the gateway. This includes the wireless link and the wireline link as well.

Even if communication between the eNetwork Wireless Gateway and Client is secured, we strongly recommend for a productive installation to manage the gateway the same way you would manage a firewall. That means:

- Regularly archive the account logs and error logs.
- Check the error log and have a look at the account logs.
- Log all configuration activities.
- Record and examine excessive login attempts with invalid passwords.

6.4.2 Gateway Connected to the Internet

If you want to have a corporate intranet connected to the Internet and protect it from unauthorized external access at the same time, you would normally install a *firewall* between these two networks. Figure 88 on page 166 shows a general configuration.

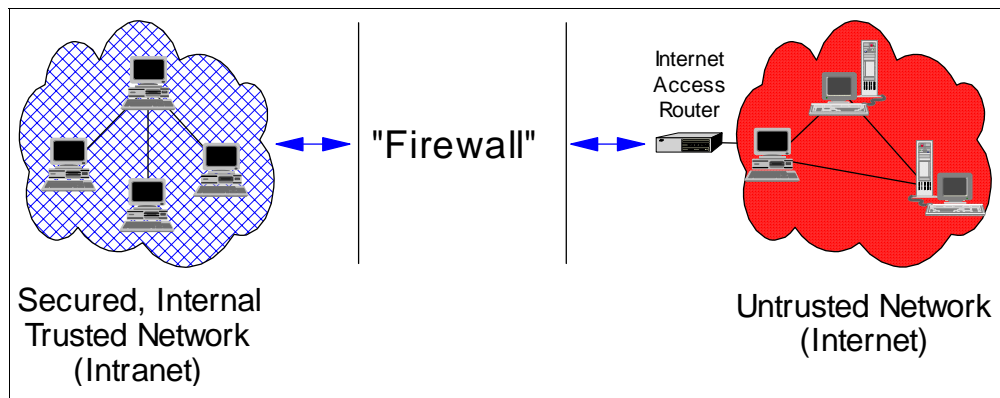


Figure 88. Using a Firewall to Protect Corporate Intranets

From the IP point of view, a firewall is a dual homed computer that is attached to a *trusted network*, the intranet and an *untrusted network*, the Internet at the same time. A firewall controls all external connections and traffic over these connections. It enforces the company's security policy. It repels and reports attacks and policy violations. A very important function is that it shuts itself down, when under severe attacks.

The firewall may route traffic, intercept IP connections, change IP packet address information and act as a proxy for some applications. Usually it prevents IP addresses used in the trusted network from being visible in the untrusted network. This prevents potential hackers from finding possible targets by observing the network traffic. It may allow specific stations or users to access the Internet but normally blocks any direct access to Intranet resources.

The connection between the firewall and the Internet is normally intercepted by an access router provided and managed by the Internet Service Provider (ISP). Depending on the type of Internet access there may be one or several IP nodes beyond the router visible from the Internet.

In the following, we assume that the company is already connected to the Internet and has a firewall in place.

When the eNetwork Wireless Gateway connects to a wireless network provider via TCP/IP, there must be a TCP connection over the Internet. If the gateway is responsible for establishing the TCP connection, the connection may eventually be socksified and protected by the firewall. However, if the network provider uses the originating IP address for authentication purposes, which usually is the case, the firewall external IP address has to be used, allowing everyone in the intranet to access the wireless network provider (not a good idea!).

Keep in mind that even if you have a leased line or frame relay connection to that provider, the provider will probably exclude packets from other than the wireless clients from being routed to the eNetwork Wireless Gateway. If the provider guarantees the customer that no external packets will reach the eNetwork Wireless Gateway via this TCP/IP connection, the customer may truly believe in this and be happy. Depending on the network security policy, other customers may want to control external IP access themselves.

Having the eNetwork Wireless Gateway connected to the Internet results in the following additional threats above and beyond those discussed in 6.4.1, "Not Connected to the Internet" on page 165:

1. It is easier to fake packets from the wireless network, unless there is encryption in the wireless network.
2. Someone may send IP packets to the eNetwork Wireless Gateway intending to get them routed to the intranet.
3. Since the eNetwork Wireless Gateway may be managed over a telnet connection, it has a telnet daemon listening, and this daemon cannot distinguish from which interface this connection is coming. So the gateway may be the target of remote access attacks.
4. Packets may be directed to the eNetwork Wireless Gateway in order to put it under stress. (In contrast to a firewall, the gateway will not automatically shut itself down.)

To face threat 2 in the enumeration above, make the eNetwork Wireless Gateway a *multi-homed* IP node with one IP interface for communicating with the intranet and the other IP interface for external communication. An AIX workstation can be configured in a way that effectively blocks any IP transit traffic.

There are two options for placing the eNetwork Wireless Gateway:

- Inside the firewall
- Outside the firewall

6.4.2.1 eNetwork Wireless Gateway Inside a Firewall

A configuration having the eNetwork Wireless Gateway inside a firewall is depicted in Figure 89 on page 168. All mobile users have access to all

applications and data within the corporate network, since they access the intranet via the eNetwork Wireless Gateway directly.

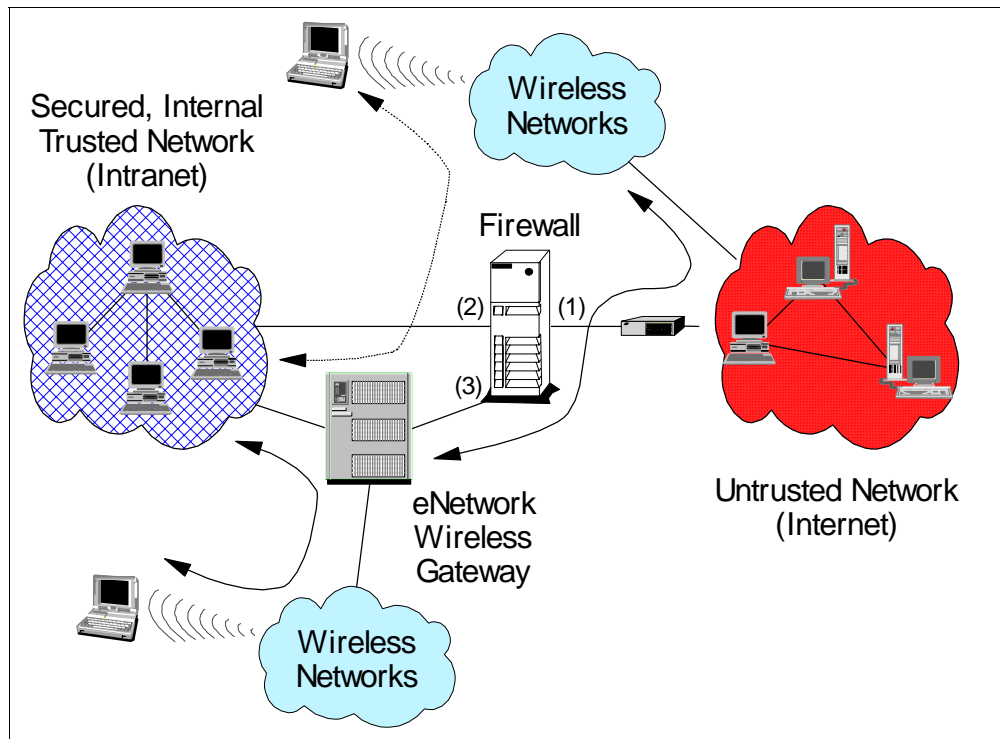


Figure 89. eNetwork Wireless Gateway Positioned Inside a Firewall

The firewall has three interfaces:

- The interface connected to the Internet (1).
- The interface connected to the Intranet (2).
- The interface connected to the eNetwork Wireless Gateway (3)

Between interfaces (1) and (2) the company security policy applies.

Depending on the wireless radio network that the gateway is connected to, there has to be some “open port” between interfaces (1) and (3). For connections to DataTAC networks over TCP, it is sufficient to allow a single TCP connection to be established from a specific IP port on the gateway to the wireless network provider represented by a specific IP address and port. In order to support CDPD, the firewall has to be transparent for UDP packets directed to a specific IP port of the gateway. There is no need to map the external IP address of the eNetwork Wireless Gateway to another one by the firewall. All other traffic to the gateway may be blocked by the firewall, thus protecting the gateway to a maximum extent.

Should there be an attack to the eNetwork Wireless Gateway’s IP ports that are open to wireless network providers, this will be reported by the gateway’s error log indicating invalid packets or packets from unknown mobile users, protocol conflicts or packet discards due to encryption failures. You can then easily arrange to change port numbers with the wireless network provider. Any other attack will be shielded by the firewall. This addresses even the problem of the gateway not shutting down under heavy attacks.

If there is a separate connection to the wireless network provider, the company's firewall need not be touched. A small firewall, filtering all traffic except the packets directed to the ports the gateway is listening for, as shown in Figure 90 on page 169, is enough to protect the eNetwork Wireless Gateway.

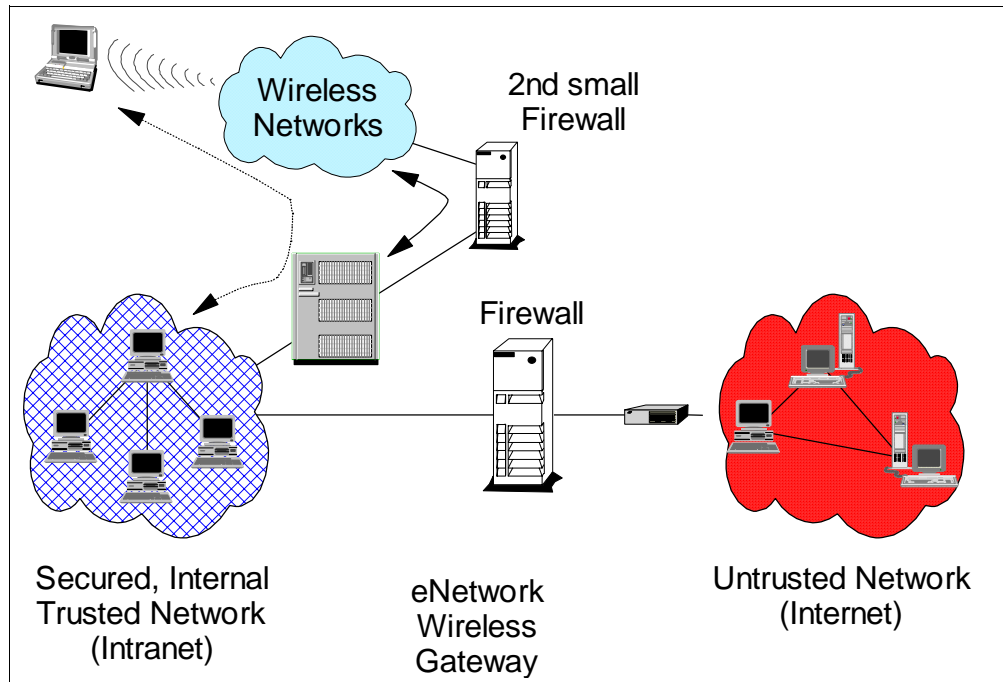


Figure 90. Gateway Inside a Firewall with Separate Connection to the Wireless Network

6.4.2.2 eNetwork Wireless Gateway Outside a Firewall

There may be situations where a company's network security policy does not allow external access to the intranet without passing the company's firewall. It can, however, then be assumed that the firewall will provide some means for accessing the intranet externally.

For example, consider the following situation. A company has a very sensitive corporate network infrastructure and a very strong and powerful firewall, which allows remote access, after the remote user has successfully authenticated himself via an ID, password and a smart card at an authentication server outside the intranet. Since this mechanism is more secure than our eNetwork Wireless security mechanisms, there is no reason why the eNetwork Wireless Gateway cannot be placed outside the firewall as depicted in Figure 91 on page 170. The gateway remains dual homed in this case.

Note that you still have to protect the eNetwork Wireless Gateway itself against external attacks. Similar to the configuration shown in Figure 90 on page 169, this can be achieved by placing a second small firewall which allows for the TCP connection to the wireless network provider or UDP traffic from CDPD only.

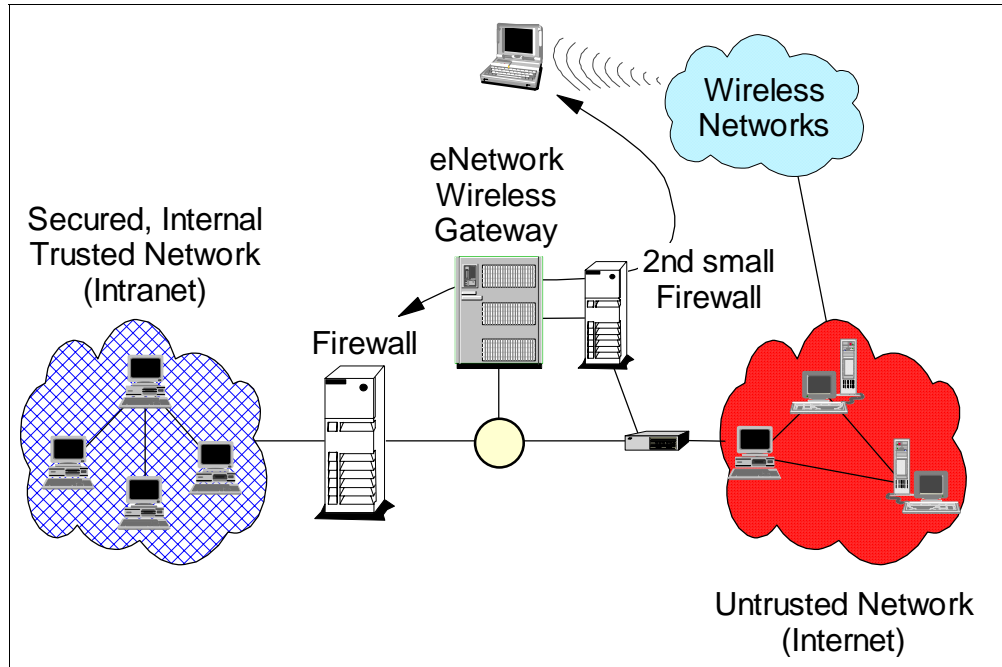


Figure 91. eNetwork Wireless Gateway Positioned Outside a Firewall

Part 3. The eNetwork Express Software Family

This part of the redbook provides useful information for understanding the implementation of the eNetwork Emulator Express and eNetwork Web Express products. You will find very detailed information on the installation, configuration and management of these two products. Sample scenarios are included where you will find step-by-step guidelines to successfully install, configure, monitor and troubleshoot configuration problems. When required some tips and hints are inserted to provide you with a better understanding of the products.

Chapter 7. IBM eNetwork Emulator Express

IBM eNetwork Emulator Express is a client/server product in the IBM eNetwork Wireless product family. The IBM eNetwork Wireless Product family is an open systems communication platform that enables Internet Protocol (IP) applications to run in a wireless environment. It gives mobile computers wireless access to host and network resources through radio and dial-up networks.

In this chapter we provide an overview of the eNetwork Emulator Express server in a Windows for NT platform, its installation, configuration and monitoring. We also include a section on how you will install and configure the eNetwork Emulator Express server in an AIX system. The eNetwork Emulator Express client is available for Windows 95, Windows NT and OS/2 platforms.

7.1 Overview

With the IBM eNetwork Wireless product family, application programs using the standard TCP/IP interface have access to both wireless networks and wireline networks. This access is integrated under a common interface layer that shields all network-specific details from the user application and provides network-specific enhancements such as data compression, data encryption, and authentication.

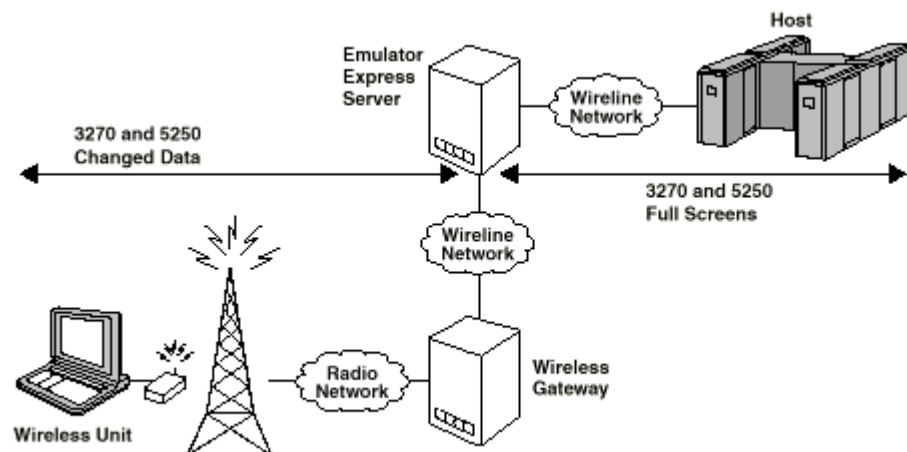


Figure 92. eNetwork Emulator Express in a Wireless Network

Data transmission over wireless and dial-up networks is often more expensive and slower than over wireline networks. To overcome these shortcomings, the eNetwork Wireless Gateway and Client uses a 3270/5250 terminal emulator optimizer called IBM eNetwork Emulator Express. However, you should be aware that eNetwork Emulator Express does not require a wireless network.

The eNetwork Emulator Express enhances the throughput of 3270 and 5250 Telnet emulators over slow or congested links by reducing the number of packets or bytes sent by the application. The customer benefits with reduced network costs, reduced response time, or both. Emulator Express enhances throughput of 3270 and 5250 Telnet sessions by intercepting the session on the client, reducing

the data, transferring the data to the eNetwork Emulator Express server, and then faithfully restoring the data after it travels across the network. The restored data is then sent to the SNA host.

The Emulator Express Client resides in the same computer (usually a laptop for the mobile environment) as the emulator. The Emulator Express Server is in a computer on the other side of the wireless (or wireline) network from the Emulator Express Client. It can be in the same computer as the Telnet 3270/5250 server. The Emulator Express Client intercepts the Telnet session that the emulator would have normally established with the Telnet server. From the emulator's viewpoint, the Emulator Express Client appears to be a Telnet server. In other words, the interface between the emulator and the Emulator Express Client is the same as the interface between an emulator and a Telnet 3270/5250 server. Similarly, the Emulator Express Server provides the same interface as the emulator to the Telnet 3270/5250 server or SNA host. In other words, when an Emulator Express Server requests a connection to a Telnet 3270/5250 server, it appears to the Telnet 3270/5250 server as if the request was coming from an emulator client.

7.2 IBM eNetwork Emulator Express Architecture

In this section we provide a brief overview of the architecture implemented in eNetwork Emulator Express. It includes information about the data reduction process supported by the client and server.

7.2.1 IBM eNetwork Emulator Express Components

A basic IBM eNetwork Wireless configuration is illustrated in Figure 92 on page 173. The mobile unit with IBM eNetwork Wireless software on the left is a mobile computer, such as a ThinkPad or notebook, with a wireless or dial-up modem. The mobile unit connects through a wireless or dial-up network to the wireless gateway and servers. The wireless gateway and servers give the mobile unit access to TCP/IP applications, 3270 and 5250 applications, and the Internet.

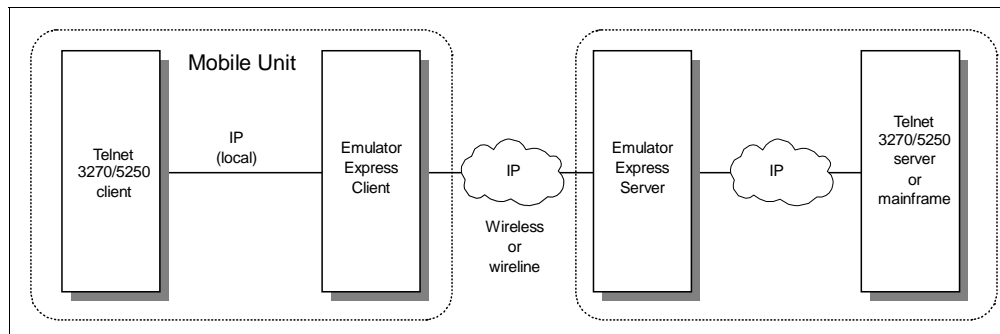


Figure 93. Telnet 3270/5250 and Emulator Express

As part of the IBM eNetwork Wireless Family of software products, Emulator Express Servers and Clients can take advantage of the wide range of wireless and dial protocol support available through the wireless gateway and wireless client. The need for optimized wireless Telnet emulation is a result of the growing demand by mobile workers for access to existing legacy applications. Most legacy applications, however, were designed for high-speed, less expensive, wired

connections. To make mobile access to these applications more practical, the Emulator Express products are designed to optimize data transfer through caching, data compression, and protocol reduction. Descriptions of these functions follow in "Data Reduction Process".

The communication between the Telnet 3270/5250 client/server and Emulator Express client/server is via TCP/IP. Therefore, three IP connections must be established. However, the Emulator Express client and the Telnet 3270/5250 client need to reside in the same mobile unit as shown in Figure 93 on page 174.

7.2.2 Data Reduction Process

Residing on either side of the wireless or dial-up network, Emulator Express clients and servers work together to reduce significantly the amount of data sent over the network. Emulator Express enhances throughput of 3270 and 5250 Telnet sessions by intercepting the session on the client, reducing the data, and then faithfully restoring the data after it travels across the network. The restored data is then sent on to the SNA host or Telnet 3270/5250 server.

The following techniques are used by Emulator Express for data reduction:

- Caching

Most 3270 and 5250 application screens contain many fields with static data followed by variable fields or input fields. Static fields describe the variable data displayed from the host or entered by the user. Examples are fields containing the words "Name", "Address", "Account Number", "Account Balance", etc.

When applications run over a high-speed wireline connection, there is little impact transmitting these fields back and forth between the host and the user. However, with low-bandwidth, expensive wireless or dial-up connections, transmitting these fields can affect response time and increase cost. Through caching, Emulator Express significantly reduces the retransmission of static data, which reduces the amount of data transferred to and from the mobile device. By storing field images at both the IBM eNetwork Emulator Express clients and servers, only new or modified data is transmitted. The cache is normally built and updated as a session proceeds.

To further reduce transmission costs, the user can load the cache by running applications while the mobile device is connected to the wired network. In this way, the cache is "warmed up" before being used in a mobile environment. The warmed up cache is shared by all emulator sessions for a particular configured host connection.

Caching is applied to variable fields also and it will usually give you traffic reduction when doing field sorting for example or when invoking the same screen several times for the duration of the session.

- Data Compression

After the caching routines eliminate static data, the remaining data is further reduced by applying arithmetic compression algorithms. The result is that only a fraction of the original data stream (in bytes) is transmitted over the mobile connection.

- Protocol Reduction

Because of the unique relationship between the IBM eNetwork Emulator Express Clients and Servers, the flows in the standard Telnet connection protocol can be reduced by approximately half.

7.2.3 3270 File Transfer

The 3270 file transfer protocols are supported when the Telnet 3270 sessions use the eNetwork Emulator Express. This protocol is known as the IND\$FILE protocol and it is supported by most of the Telnet 3270 clients, such as PCOMM and Host On-Demand (HOD). However, because data streams need to be translated into 3270 EBCDIC characters, longer messages can be generated since the supported 3270 character set is a subset of the full EBCDIC character set and special techniques must be used. The eNetwork Emulator Express reduction protocol does not work well when data compression is implemented at a higher level.

In other words, eNetwork Emulator Express works well when traffic is for text or small files and it will not be so efficient when data traffic is already compressed, encrypted or it is hexadecimal data.

For this reason, whenever possible, we highly recommend the use of the FTP protocol for file transfers. File transfer via FTP requires however the IP stack at both ends. In other words, the main system (host) must support TCP/IP.

7.3 Emulator Express Server Installation

The Emulator Express server is available on the AIX and Windows NT platforms. In this section we show you the installation procedure. For more information on how you will install Emulator Express server, see *eNetwork Emulator Express Administrator's Guide*, GC31-8636.

7.3.1 Installing Emulator Express Server for Windows NT

Although eNetwork Emulator Express is shipped on CD-ROM only, you can install Emulator Express from diskettes or directly from the CD-ROM. Choose the proper national language directory as required. To install from diskettes, you will need to create diskettes from the CD-ROM. In this section we show you the installation from diskettes. To install an Emulator Express server for Windows NT you will execute the following steps:

5. Insert the Emulator Express Server for Windows NT diskette into the A drive.
6. Select **Start→Run**.
7. Select or enter: **A:\SETUP**
8. Click on **Next** on the Welcome window to start the installation.
9. On the Choose Destination Location window, click on **Next** to accept the default directory. (Click on **Browse** to choose another destination path.)
10. In the "Select Program Folder" window, select the folder that will contain the IBM eNetwork Emulator Express icons, then click on **Next** to continue. (The default is IBM eNetwork Emulator Express Server.)
11. Your selections are displayed in the "Start Copying Files" window. Click on **Back** to return to a previous window. When satisfied with your choices, click on **Next**.

Files will be copied to your destination directory. Click on **Cancel** at any time to stop the copy process. (If you cancel the install, all IBM eNetwork Emulator Express server files are deleted.)

12. You are asked if you want to review the README file. If you click on **YES**, close the README file when finished.
13. If required the eNetwork Emulator Express server can be set to run as a Windows NT service. See the README file for instructions.
14. You need not restart the computer. Remove the diskette from the A drive and click on **Finish**.

7.3.1.1 Re-installing Emulator Express Server for Windows NT

To re-install the Emulator Express Server over the previous version, stop the server, follow the same steps for installing and select **Yes** on the Confirm Installation window. Cache files and configuration settings are kept from the previous install.

7.3.1.2 Uninstalling Emulator Express Server for Windows NT

Stop your Emulator Express Server session before uninstalling it. To uninstall the Emulator Express Server product and all of its components, select **Start—>Programs—>IBM eNetwork Emulator Express Server—>Uninstall IBM eNetwork Emulator Express Server**.

Using the **Start** menu selection is preferable to using Add/Remove Programs; the latter method might not uninstall Emulator Express correctly. If you are running the eNetwork Emulator Express server as a service, you will need to use Windows NT facilities to disable it before you uninstall. If this is your case, the README file provided with the product contains information on how you would do this.

7.3.2 Installing Emulator Express Server for AIX

In this section we show you the installation of the eNetwork Emulator Express Server for AIX. The installation is available from the CD-ROM only. The README file provided in the CD contains details for a proper installation. Choose the proper national language directory as required. You will execute the following steps:

1. Insert the CD in the proper drive.
2. Log on as root.
3. Start SMIT by entering the following at the command prompt:

```
smit install
```

4. Beginning at the displayed SMIT installation menu, choose:

```
Install and Update Software
Install / Update Selectable Software
Install Software Products at Latest Level
Install New Software Products at Latest Level
```

5. In the dialog panel, press F4 to choose the device type from which you are installing the Emulator Express Server.
6. In the next dialog panel, move the cursor to the following field:

```
SOFTWARE to install
```

Press F4 to view the list of program files on the device.

7. Move the cursor to the following line:

```
4.1.3.2 emexpress ALL
```

Press F7 and then press Enter.

8. Review the remaining options in the Install Software Products at Latest Levels panel. If acceptable, or after making desired changes, press Enter.

After you have installed the Emulator Express Server, refer to the README file in the /usr/lpp/emexpress directory for more information.

7.4 Emulator Express Server Configuration

In this section we show you the Emulator Express configuration process for Windows NT and AIX. For more information on how you will configure Emulator Express Server, see *eNetwork Emulator Express Administrator's Guide*, GC31-8636.

7.4.1 Emulator Express Server for Windows NT Configuration

The Emulator Express configuration offers a basic and an advanced configuration screen.

7.4.1.1 Basic Configuration

The port number used for the IP connection between the Emulator Express client and server must be entered. The default value is port number 17000. The Emulator Express server will listen for client requests on this port. The port number is entered as illustrated in Figure 94 on page 178.

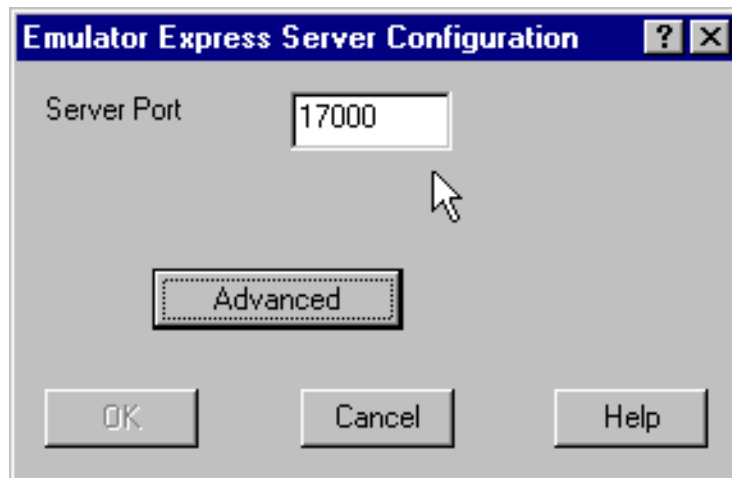


Figure 94. Emulator Express Server - Basic Configuration

The server port is the access point for data transfer on the Emulator Express server. The server port monitors connection requests from the Emulator Express clients. If you select a port number other than 17000, use a number not already defined by another application. Because numbers 1–5000 are commonly used, you may want to pick a number greater than 5000.

Optionally, you may select the Advanced configuration option to change the default values for the cache size, maximum number of supported sessions, idle timeout value and trace options.

7.4.1.2 Advanced Configuration

Advanced configuration of the Emulator Express Server for Windows NT enables you to:

- Set the size of the cache file.
- Set the maximum number of emulator sessions the server will accept.
- Set the number of minutes of idle time before an emulator session times out.
- Turn tracing on or off and set various traces to troubleshoot a problem.

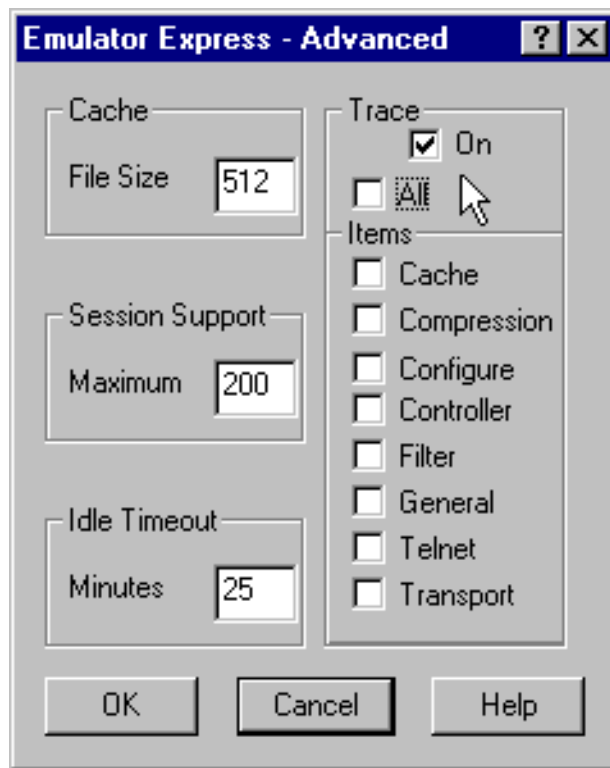


Figure 95. Emulator Express Server - Advanced Configuration

Setting the Cache Size

Cache size is the size of the file that holds reuse data for each Emulator Express client session. Cache size is transmitted from server to client when the session is initiated. Data is replaced in least-recently used (LRU) order and when the cache file is full, new data overwrites the oldest data. The default file size is 512 KB with a range of possible values from 12 KB to 4000 KB.

Note

The number you enter for the cache size is an approximation of the actual data, in KBs, that can be stored in the cache file. However, the cache index and overhead will roughly double the size of the cache.

Setting the Maximum Number of Sessions

Session support is the total number of concurrent client sessions from all Emulator Express clients that an Emulator Express server will support. The number of sessions an Emulator Express client can run concurrently is eight. The input maximum for server session support is 2000, but resource and system limitations may make this number of concurrent sessions unachievable. The default is 200 sessions.

Note

Setting the maximum number of sessions to a very large number may use up the system resources and affect the performance of the Emulator Express server.

Setting Idle Timeout

Idle timeout is the number of minutes an emulator session can remain idle before it is automatically ended. There is an idle timeout field on the configuration window of the Emulator Express server for Windows NT and an idle timeout can be set on the Emulator Express client. When the number of minutes until timeout differs on a server and its clients, the session is closed based on the client or server whose timeout expires first. For example, if a server has 25 minutes for idle timeout and its client has 15 minutes, the emulator session closes after 15 minutes of idle time.

If you do not want to end emulator sessions when they are idle, set the idle timeout to 0 on both the Windows NT server and the client. If only one is set to 0, the 0 is ignored, and the remaining idle timeout number is used. The default idle timeout is 25 minutes, with a range of values from 0 to 1440 minutes.

Using a Trace File

A trace file for the Emulator Express server can be started on the server by turning trace on in the advanced configuration.

Here is a sample portion of a trace file:

```
-- 1998-10-26 --
14:17:53 [CNFG] GUI: Set trace values
14:17:54 [TRAN] TCPCircuit: 0001 Closing listen socket 156
14:17:54 [TRAN] TCPCircuit: 0001 Listen socket 320 opened
14:17:54 [TRAN] TCPCircuit: 0001 Socket local address bound
14:17:54 [TRAN] TCPCircuit: 0001 Listening to socket 320
14:17:54 [CTRL] Open_Listener: 0001 Listening for client calls on TCP port
17000,
14:17:54 [CNFG] Create_Listeners: 0000 Finished reading config
-- 1998-10-26 --
14:24:29 [TRAN] TCPCircuit: 0001 Closing listen socket 320
-- 1998-10-26 --
14:24:36 [CNFG] GUI: Set trace values
14:24:36 [CNFG] HandleRegistryNotification: Opening Registry subkey
'SOFTWARE\IBM\eNetwork Emulator Express Server'.
14:24:36 [SERV] GUI: Starting session support
14:24:36 [CTRL] Startup: Emulator Express Server (version 4.1.3A) - execution
starting on host artsrv.
```

```

14:24:36 [CTRL] Create_Listeners: 0000 Maximum sessions supported is now 200
14:24:37 [TRAN] TCPCircuit: 0001 Listen socket 164 opened
14:24:37 [TRAN] TCPCircuit: 0001 Socket local address bound
14:24:37 [TRAN] TCPCircuit: 0001 Listening to socket 164
14:24:37 [CTRL] Open_Listener: 0001 Listening for client calls on TCP port
17000,
14:24:37 [CNFG] Create_Listeners: 0000 Finished reading config
14:24:37 [CTRL] Listen_Loop: 0 Sessions active
-- 1998-10-26 --
14:28:07 [TRAN] TCPCircuit: 0001 Closing listen socket 164

```

The active trace file for the Emulator Express Server is a 10 MB file named `emexpr.trc`. Each time the server starts or when the trace file reaches the maximum 10 MB capacity, the file is renamed to `emexpr2.trc` and a new `emexpr.trc` file becomes the active trace file. Only two trace files are kept, the active current trace file and the most recent previous trace file. If you installed Emulator Express in the default directory, the trace file is located in the directory `C:\Program Files\IBM\enNetwork Emulator Express Server`.

Unless you are troubleshooting a problem, it is generally best to run with trace turned off because of performance considerations. When looking in a trace file for clues about a problem, start at the end of the file, where the most recent data is stored, and work backwards.

Selecting Events to Trace

You can trace all types of events in the Emulator Express Server, or you can select one or more event types to trace. The following events can be traced in Emulator Express server:

- **Cache**—The cache is the component of Emulator Express that stores portions of previously transmitted screens. Only screens from the host to the client are cached. Cache events are written to the trace file with the heading `[CACH]`.
- **Compression**—Compression is applied to all data packets transmitted between client and server. Compression reduces data sent over slow links and improves performance. Compression events are written to the trace file with the heading `[COMP]`.
- **Configure**—Configure events provide information about configuration parameters from the Emulator Express configuration. Configure events are written to the trace file with the heading `[CNFG]`.
- **Controller**—Controller events indicate main connection management events, such as program start/stop, session start/stop and listen ports. Controller events are written to the trace file with the heading `[CTRL]`.
- **Filter**—Filter events are transformations on data not included under cache or compression. Filter events are written to the trace file with the heading `[FILT]`.
- **General**—General events are miscellaneous events not covered by the other categories. General events are written to the trace file with the heading `[CLNT]` for client general events and `[SERV]` for server general events.
- **Telnet**—Telnet events are the Telnet protocol negotiation packets that are exchanged at the beginning of a session. Emulator Express attempts to reduce the number of negotiation packets exchanged in order to improve performance and lower costs over a slow link. Select this trace option if you

are having difficulty initiating an emulator session. Telnet events are written to the trace file with the heading [TNPR].

- **Transport**—Transport events are the results of open, close, read, and write operations to TCP sockets of the underlying TCP/IP stack. Select this trace option if you suspect a problem with your TCP/IP implementation. Transport events are written to the trace file with the heading [TRAN].

7.4.2 Emulator Express Server for AIX Configuration

There is no graphical user interface for the Emulator Express Server for AIX. After installation, the sample configuration shown in “AIX Emulator Express Server Sample Configuration” on page 185 is in the file `/etc/emexpsrv.cfg`. You can modify this file as needed. However, in most cases, you probably will not change the file, as the sample configuration is generally adequate. (You will need to make changes to the configurations of your Emulator Express Clients.)

The configuration file for an Emulator Express Server for AIX needs exactly one listen statement to set the server (listen) port number. Read 7.4.2.1, “Setting the Server (Listen) Port Number” on page 182 for more information about setting the port number. Also see “Configuration Options Common to AIX Servers” for other parameters you can set in the configuration file. Keywords and values inside the configuration file `emexpsrv.cfg` are not case sensitive.

Save the configuration file after editing it. To activate changes, end any client sessions and clients that are running and restart the Emulator Express Server for AIX.

7.4.2.1 Setting the Server (Listen) Port Number

The server (listen) port is the access point for data transfer on the Emulator Express Server. The server port monitors connection requests from the Emulator Express Client. The default server port number is 17000.

If you select a port number other than 17000, use a number not already defined by another application. Because numbers 1-5000 are commonly used, pick a number greater than 5000. Enter listen followed by the server (listen) port number.

An example of setting the server port number is:

```
listen 17000
```

7.4.2.2 Configuration Options Common to AIX Servers

Configuration options for AIX enable you to:

- Set the size of the cache file.
- Set the number of minutes of idle time before an emulator session times out.
- Turn tracing on or off, set the size of the trace file, and trace various types of events to troubleshoot a problem.
- Set the maximum number of emulator sessions the server will accept (server only).
- Specify the directory to which the server will write trace, log, and cache files (server only).

Setting the Cache Size

Cache size is the size of the file that holds reuse data for each Emulator Express Client session. Cache size is transmitted from server to client when the session is initiated. Data is replaced in least-recently used (LRU) order and when the cache file is full, new data overwrites the oldest data.

The default file size is 512 KB with a range of possible values from 12 KB to 4000 KB.

To set the cache size in the configuration file, enter *cachesize* followed by the size in kilobytes. For example:

```
cachesize 512
```

Note

The number you enter for the cache size is an approximation of the actual data, in KBs, that can be stored in the cache file. However, the cache index and overhead will roughly double the size of the cache.

Setting Idle Timeout

Idle timeout is the number of minutes an emulator session can remain idle before it is automatically ended. When the number of minutes until timeout differs on a server and its clients, the session is closed based on the client or server whose timeout expires first. For example, if a server has 25 minutes for idle timeout and its client has 15 minutes, the emulator session closes after 15 minutes of idle time.

If you do not want to end emulator sessions when they are idle, set the idle timeout to 0 on both the server and the client. If only one is set to 0, the 0 is ignored, and the remaining idle timeout number is used.

The default idle timeout is 25 minutes, with a range of values from 0 to 1440 minutes.

To set the idle timeout in the configuration file, enter *idletime* followed by the timeout in minutes. For example:

```
idletime 25
```

Using a Trace File

Use a trace file to help debug problems. In this section we discuss how to start a trace file, how to set the size of the trace file, and which items can be traced.

Starting a Trace

To write a trace file for an Emulator Express Server for AIX, enter the following line in the configuration file:

```
trace 1
```

To prevent tracing, enter:

```
trace 0
```

The default is no tracing, although this may be overridden by using the *-d* parameter on startup.

The active trace file for the Emulator Express Server is a file named `emexpsr.trc`. Each time the server starts or when the trace file reaches the maximum capacity, the file is renamed to `emexpsr2.trc` and a new `emexpsr.trc` file becomes the active trace file. Only two trace files are kept, the active current trace file and the most recent previous trace file.

The trace file is normally located in the directory `/var/emexpress`. The location of the trace file can be overridden by the `filepath` statement in `emexpsrv.cfg`.

When looking in a trace file for clues about a problem, start at the end of the file, where the most recent data is stored, and work backwards.

Setting the Trace File Size

To set an approximate limit on the maximum size of the trace file, enter in the configuration file: `tracesize` followed by the size limit in megabytes (MB). For example:

```
tracesize 10
```

The valid range of the size limit is from 1 (MB) to 20 (MB).

The default trace file size for the Emulator Express Server for AIX is 10 MB.

Trace Options

You can trace all of the following event types, or you can select one or more event types to trace.

- Cache

The cache is the component of Emulator Express that stores portions of previously transmitted screens. Only screens from the host to the client are cached. Cache events are written to the trace file with the heading [CACH].

- Compression/Decompression

Compression is applied to all data packets transmitted between client and server. Compression reduces data sent over slow links and improves performance. Compression events are written to the trace file with the heading [COMP].

- Configure

Configure events provide information about configurable parameters from the Emulator Express configuration. Configure events are written to the trace file with the heading [CNFG].

- Controller

Controller events indicate main connection management events, such as program start/stop, session start/stop and listen ports. Controller events are written to the trace file with the heading [CTRL].

- Filter

Filter events are transformations on data not included under cache or compression. Filter events are written to the trace file with the heading [FILT].

- General

General events are miscellaneous events not covered by the other categories. General events are written to the trace file with the heading [CLNT] for client general events and [SERV] for server general events.

- Telnet

Telnet events are the Telnet protocol negotiation packets that are exchanged at the beginning of a session. Emulator Express attempts to reduce the number of negotiation packets exchanged in order to improve performance and lower costs over a slow link. Select this trace option if you are having difficulty initiating an emulator session. Telnet events are written to the trace file with the heading [TNPR].

- Transport

Transport events are the results of open, close, read, and write operations to TCP sockets of the underlying TCP/IP stack. Select this trace option if you suspect a problem with your TCP/IP implementation. Transport events are written to the trace file with the heading [TRAN].

The default is to trace all these event types. To trace just some of them, enter, in the configuration file, *traceopts* followed by the event types you want to trace (cach, comp, cnfg, ctrl, filt, clnt, serv, tnpr, tran). For example:

```
traceopts comp filt tnpr
```

Setting the Maximum Number of Emulator Sessions

Session support is the total number of concurrent client sessions from all Emulator Express Clients that an Emulator Express Server will support. The number of sessions an Emulator Express Client can run concurrently is eight. The default session limit for an AIX server is 500 sessions, with a valid range of 1 to 2000 sessions. Resource and system limitations may make 2000 concurrent sessions unachievable. The actual number of concurrent sessions you will be able to achieve is dependent upon system resources such as memory, processor speed, and so on.

To set the maximum number of emulator sessions, enter *maxsessions* followed by the session limit. For example:

```
maxsessions 1000
```

Specifying a Directory for the Trace, Log, and Cache Files

The *filepath* statement specifies the directory to which the server will write trace, log, and cache files. This directory must be on a local file system (not on a network file system), and the directory must exist. The default directory is */var/emexpress*.

To specify this file directory, enter *filepath* followed by the pathname. For example:

```
filepath /var/emexpress
```

7.4.2.3 AIX Emulator Express Server Sample Configuration

The following sample configuration file is provided with Emulator Express for AIX:

```
* Sample Emulator Express Server configuration file
```

```
* All statements may be entered in either upper or lower case.
```

```
* Each statement must be entered on its own line and it may not span
```

```
* multiple lines. The maximum allowed line length is 128 characters.
```

```
* In general, if a statement is specified multiple times, only the FIRST
```

```
* will be used.
```

```

* This file normally resides in /etc/emexpsrv.cfg. If a version is found in
* the current working directory at execution time it will be used instead.

* A server needs exactly one listen statement.
* If no listen lines are defined or the config file can't be opened
* then a single default listen will be set up on the default listen port.

* LISTEN [server_port]
*   default server port is 17000
*   This statement should only be changed while Emulator Express server
*   is not running. All clients must be reconfigured to use the new port.

*   listen 17000
listen 17000

* IDLETIME [minutes]
*   default timeout is 25 minutes
*   valid range is 0 to 1440 minutes where 0 is interpreted as no timeout.
*   This statement may be changed while Emulator Express server is running.
*   Changes will only affect sessions started after the change is made.

*   idletime 25
idletime 25

* CACHESIZE [kb]
*   default cachesize is 512
*   valid range is 12 to 4000
*   This is an approximate limit on the maximum cache size (in kilobytes)
*   used for the active cache or for either of the two possible cache
*   checkpoints.
*   This statement may be changed while Emulator Express server is running.
*   Changes will only affect sessions started after the change is made and
*   only if an existing cache checkpoint file is not used.

*   cachesize 512
cachesize 512

* TRACE [0|1]
*   default is 0 unless overridden by startup
*   0 means no tracing will be done. 1 means trace output will be
*   written to emexpsr.trc. When this file exceeds the maximum trace
*   size of specified by TRACE_SIZE (see below) it will be saved as
*   emexpsr2.trc and tracing will restart at the beginning of emexpsr.trc
*   Note: On AIX servers, trace (and log) files will be written to the
*   directory specified in the FILEPATH statement (see below).
*   This statement may be changed while Emulator Express server is running,
*   but will not take effect until it is restarted.

*   trace 0
trace 0

* TRACEOPTS [ALL] | [[COMP] [CACH] [TNPR] [FILT] [TRAN] [CTRL] [CNFG] [CLNT]
[SERV]]
*   default is ALL
*   These specify which component traces will be in effect if TRACE 1 is
*   specified. Components are:
*   COMP Compressor/decompressor
*   CACH Cache

```

```

*      CACH  Cache
*      TNPR  Telnet Protocol Reduction
*      FILT  General filtering
*      TRAN  Transport layer
*      CTRL  Controller/router function
*      CNFG  Configuration
*      CLNT  General client
*      SERV  General server
*      This statement may be changed while Emulator Express server is running,
*      but will not take effect until it is restarted.

*      traceopts comp cach tnpr filt tran ctrl cnfg clnt serv
*      traceopts all
traceopts all

* TRACE SIZE [mb]
*      default is 1 (client) or 10 (server)
*      valid range is 1 to 20
*      This is an approximate limit on the maximum trace file size
*      (in megabytes) for the active trace and the previous trace.
*      On AIX servers, trace (and log) files will be written to the
*      directory specified in the FILEPATH statement (see below).

*      On AIX servers, trace (and log) files will be written to the
*      directory specified in the FILEPATH statement (see below).
*      This statement may be changed while Emulator Express server is running,
*      but will not take effect until it is restarted.
*      tracesize 10
tracesize 10

* MAXSESSIONS [n]
*      default is 500
*      valid range is 1 to 2000
*      Server will not accept any more concurrent sessions than this value.
*      This statement may be changed while Emulator Express server is running,
*      but will not take effect until it is restarted.

*      maxsessions 500
maxsessions 500

* FILEPATH [pathname]
*      default is /var/emexpress
*      A trailing '/' is optional.
*      This statement specifies the location that the server will use to
*      write trace, log and cache files. This MUST be on a local

*      This statement specifies the location that the server will use to
*      write trace, log and cache files. This MUST be on a local
*      filesystem, NOT on a network file system and the directory MUST exist.
*      Server will create a Cache directory in the specified directory.
*      Within this directory another directory will be created for each
*      client that connects to this server and within those directories
*      one directory will be created for each of the client's host port
*      definitions to contain the cache files for sessions using that
*      port.
*      This statement should not be changed while Emulator Express server
*      is running.

```

```
*   filepath /var/emexpress
filepath .
```

```
* Comments are any lines whose first non-blank or non-tab is an '*'
* Anything else is invalid, but will be treated as a comment line.
* Non-comment lines should not contain additional tokens
```

7.5 Emulator Express Client Installation

The Emulator Express client is available on the OS/2 and Windows 95/NT platforms. In this section we show you the installation procedure on a Windows 95/NT machine. For information on how you will install Emulator Express client on OS/2, see *eNetwork Emulator Express Administrator's Guide*, GC31-8636.

Note

For wireless operations, you also need to install the IBM eNetwork Wireless client.

7.5.1 Installing Emulator Express Client for Windows 95/NT

The Emulator Express client can be installed from diskettes or from a CD-ROM and it uses the InstallShield product. Diskettes must be built from the CD-ROM. Choose the proper national language directory as required. To install IBM eNetwork Emulator Express client for Windows 95/NT from diskettes:

1. Insert the Emulator Express for Windows 95/NT diskette into the A drive.
2. Select **Start→Run**.
3. Enter or select:
A:\SETUP
4. Click on **Next** on the Welcome window to start the installation.
5. Click on **Next** on the Choose Destination Location window to accept the default directory. (Click on **Browse** to choose another destination path.)
6. In the Select Program Folder window, select the folder that will contain the IBM eNetwork Emulator Express icons, then click on **Next** to continue. (The default is IBM eNetwork Emulator Express Client.)
7. Displayed in the Copy window are your selections. Click on **Back** to return to a previous window. When satisfied with your choices, click on **Next**. Files will be copied to your destination directory. Click on **Cancel** to stop the copy process at any time. (If you cancel the install, all IBM eNetwork Emulator Express for Windows 95/NT files are deleted.)
8. Click on **YES** if you want to review the README file. Close the README file when finished.
9. You do not need to restart the computer. Remove the diskette from the A drive and click on **Finish**.

If you do not have a Telnet emulator already on your mobile computer, install the PCOMM Entry emulator.

7.5.2 Re-installing Emulator Express Client for Windows 95/NT

To re-install Emulator Express Client for Windows 95/NT over the previous version, follow the same steps for installing and select **Yes** on the Confirm Installation window. Cache files and configuration settings are kept from the previous install.

7.5.3 Uninstalling Emulator Express for Windows 95/NT

Stop your Emulator Express for Windows 95/NT session before uninstalling. To uninstall the Emulator Express for Windows 95/NT product, select:

Start—>Programs—>IBM eNetwork Emulator Express Client—>Uninstall IBM eNetwork Emulator Express Client.

Using the **Start** menu selection is preferable to using Add/Remove Programs; the latter method might not uninstall Emulator Express correctly.

7.6 Emulator Express Client Configuration for Windows 95/NT

The Emulator Express client is available on the OS/2 and Windows 95/NT platforms. In this section we show you the configuration procedure on a Windows NT machine. For information on how you will configure Emulator Express client on OS/2, see *eNetwork Emulator Express Administrator's Guide*, GC31-8636.

We also include guidelines for a Telnet client configuration, such as PCOMM, to use eNetwork Emulator Express.

7.6.1 Emulator Express Client for Windows 95/NT Configuration

To configure an Emulator Express Client for Windows 95/NT, select **Start—>Programs—>IBM eNetwork Emulator Express Client—>Emulator Express Client.**

If this is your first time starting the client, the Configuration window appears. Otherwise, to access the Configuration window from the Client window, click on **System** from the menu bar and select **Configure.**

To obtain online assistance:

1. Tab to a field or push button and press F1.
2. If there is a question mark in the upper right-hand corner of the window, click on it. Move the question mark to the field where you need information and click again.
3. Click on the **Help** push button to get overview information about the window.

7.6.1.1 Client Basic Configuration

In the Emulator Express client, you need to configure the following options:

- Emulator Express client port. This is the port number for the IP connection between the Telnet client (for example, PCOMM) and the Emulator Express client.
- Destination host. This is the host name (or IP address) and the port number for the connection between the eNetwork Emulator Express server and the target mainframe or Telnet server.

- Server address and port. This is the host name or IP address of the eNetwork Emulator Express server. You will also need to configure the port number for this connection. Default value for the port number is 17000.

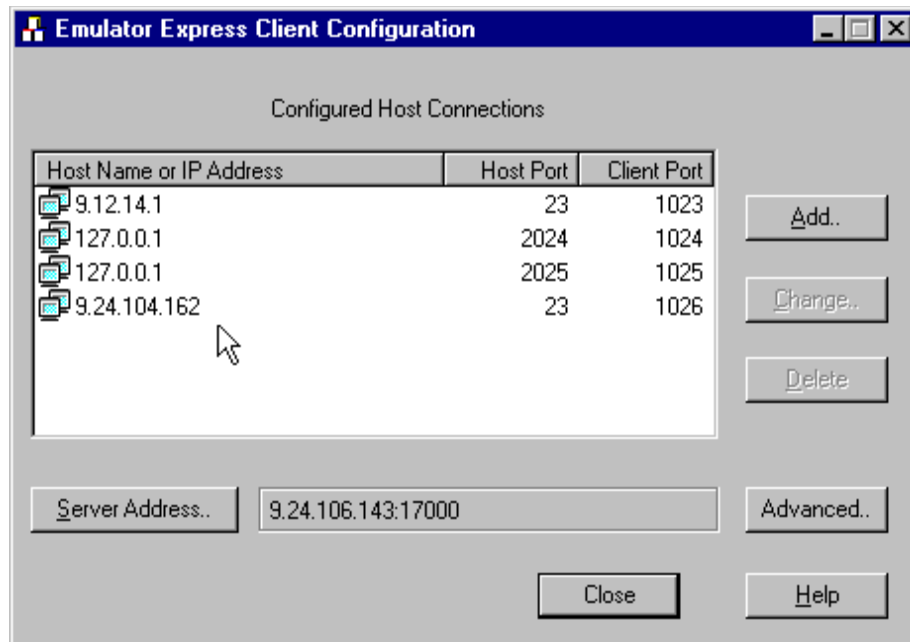


Figure 96. Emulator Express Client - Basic Configuration

Note

It is recommended that you use either dotted decimal IP addresses or a local hosts file with host names for the IP connection between the eNetwork Emulator Express client and server. This eliminates the need for DNS lookup and overhead to resolve the host name.

For more detailed information on how you configure the basic parameters in the Emulator Express client, see “Configuring Emulator Express Client” on page 193.

7.6.1.2 Client Advanced Configuration

Advanced configuration of the Emulator Express Client for Windows 95/NT enables you to:

- Set the number of minutes of idle time before an emulator session times out.
- Turn tracing on or off and set various traces to troubleshoot a problem.

A trace file for an Emulator Express Client for Windows 95/NT can be started on the client by turning trace on in the advanced configuration. The active trace file for an Emulator Express Client is a 1 MB file named emexpcl.trc. When the trace file reaches the maximum 1 MB capacity, the file is renamed to emexpcl2.trc and a new emexpcl.trc file becomes the active trace file. Each time the client starts, the existing client trace file is appended until it is full.

If you installed Emulator Express in the default directory, the trace file is located in the directory C:\Program Files\IBM\eNetwork Emulator Express Client.

From the Emulator Express Client for Windows 95/NT, you can set other advanced configuration parameters similar to ones set on the Emulator Express Server for Windows NT. These advanced parameters set trace options and the number of minutes before an idle emulator session is shut down. For more information, see 7.4.1.2, “Advanced Configuration” on page 179.

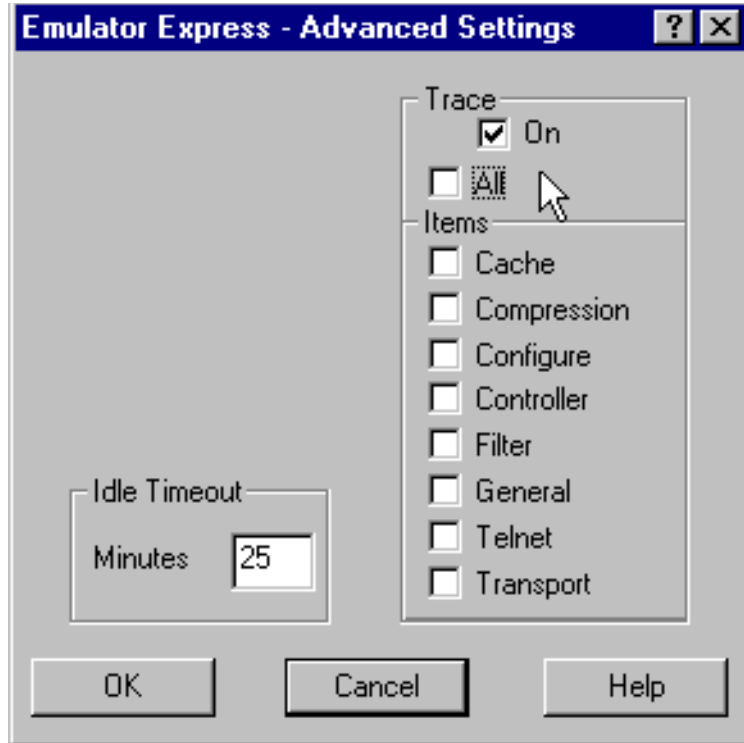


Figure 97. Emulator Express Client - Advanced Settings Configuration

7.6.2 Configuring Telnet 3270/5250 Emulator to Use Emulator Express

The basic steps for configuring any emulator to use Emulator Express are:

- Choose the type of Telnet emulator (3270 or 5250).
- Redefine the host IP address to be that of the Emulator Express Client (*localhost* or 127.0.0.1).
- Redefine the port to be that which Emulator Express has defined for a particular host. See “PCOMM Telnet 3270 Configuration” on page 195 for a Telnet 3270 sample configuration.

To have concurrent sessions to more than one Telnet server or SNA host, your emulator must allow you to change the standard port number 23 to a different port number. If your emulator does not allow you to change the port number, you will have to use port 23 as your intercept port, and you will have to change the Emulator Express client configuration each time you wish to connect to a different host.

Note

PCOMM allows you to change the port number in the Advanced configuration option for Telnet 3270/5250 clients.

7.7 Sample Scenario

In this section we show you how to configure the eNetwork Emulator Express to support multiple Telnet 3270 and 5250 sessions. To configure Emulator Express to optimize Telnet emulation, you replace the TCP connection between the emulator and the Telnet server or SNA host with three other connections. Each connection has an IP address/port number pair. In this scenario we configure four Telnet sessions as follows:

1. Session A: PCOMM Telnet 3270 session directly to a VTAM SNA host system
2. Session B: PCOMM Telnet 3270 session to a Communications Server for Windows NT TN3270E server

Note: Although eNetwork Emulator Express can connect to a TN3270E server, the connection will be negotiated down to TN3270 options.

3. Session C: PCOMM Telnet 5250 session to a Communications Server for Windows NT TN5250 server
4. Session D: PCOMM Telnet 5250 session directly to AS/400 host system

Note

The IP connection between Emulator Express client and server can be either wireless or wireline.

In this scenario, we have installed the Communications Server for Windows NT and the eNetwork Emulator Express Server on the same Windows NT server with IP address **9.24.106.143** as illustrated in Figure 98 on page 192.

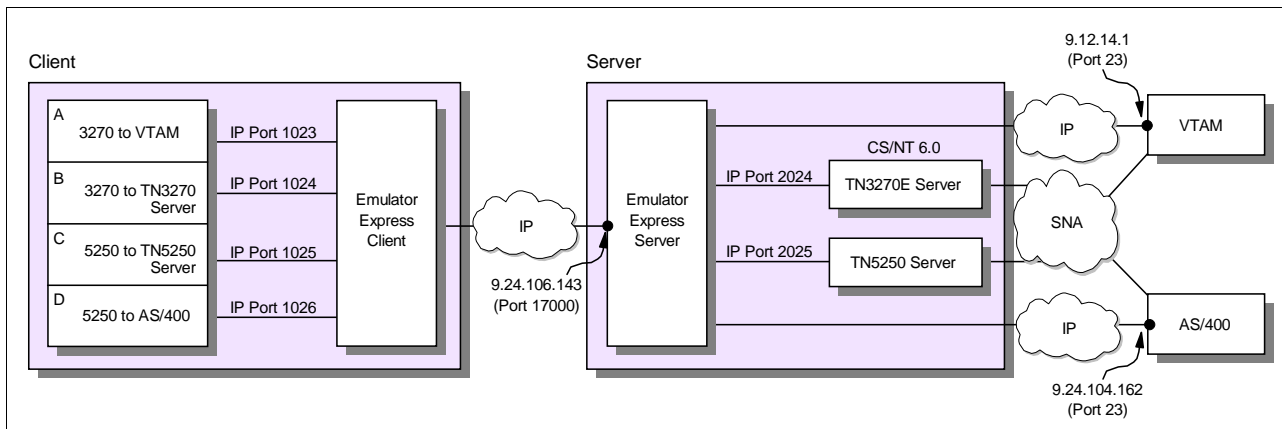


Figure 98. eNetwork Emulator Express - Sample Scenario

7.7.1 Configuring Emulator Express Server

In this step we have to configure the server port number, on which the Emulator Express server is listening, for the connection between the Emulator Express client and server. The server port number is the access point for data transfer on the Emulator Express server where the server monitors connection requests from Emulator Express clients. Click **System** to show Emulator Express Server Configuration. In this scenario we configure the server port number to 17000 which is the default port number, but any other port number can be entered as long as there are no conflicts in your machine.

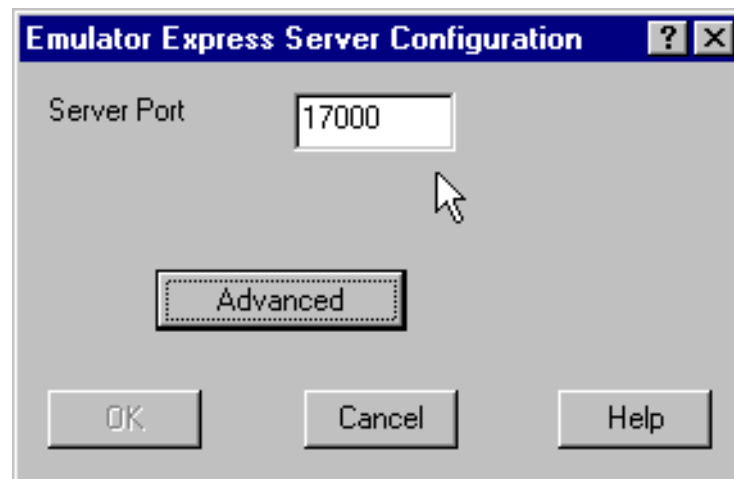


Figure 99. Emulator Express Server - Sample Configuration

Click **Advanced** to configure and change the default values for the cache file size, maximum supported sessions, idle timeout and trace options if required. For more detail about advanced configuration of the Emulator Express Server, see "Advanced Configuration" on page 179.

7.7.2 Configuring Emulator Express Client

In this step you configure the Emulator Express Server IP address and the port number for this connection (default value is port 17000). You also need to configure the Telnet host server IP address and port number for each supported Telnet session.

Click **Start→Programs→IBM eNetwork Emulator Express Client→Emulator Express Client** to configure an Emulator Express Client for Windows 95/NT.

When you create a configuration profile for the first time, you click **Add** to enter and configure the host connections. You will also click **Server Address** to configure the connection to the eNetwork Emulator Express server. See Figure 100 on page 194 for details.

Once the configuration profile has been entered, you can always select the configuration option in the System menu entry on the eNetwork Emulator Express Client screen (see Figure 104 on page 197) if you need to update the configuration parameters.

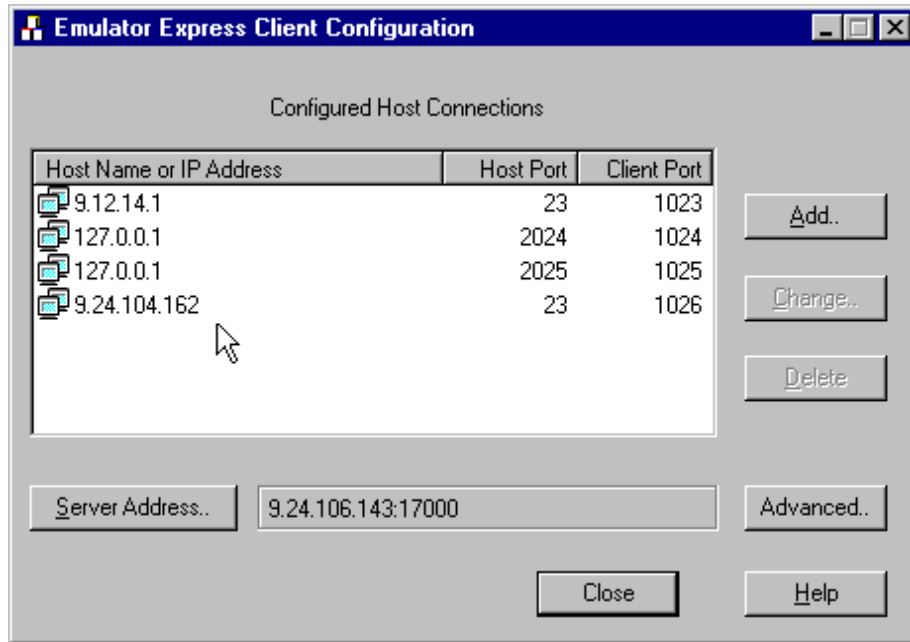


Figure 100. Emulator Express Client - Configuration

In our scenario, the Emulator Express server IP address is 9.24.106.143 and the port for this connection is the default value 17000 as shown in Figure 100 on page 194.

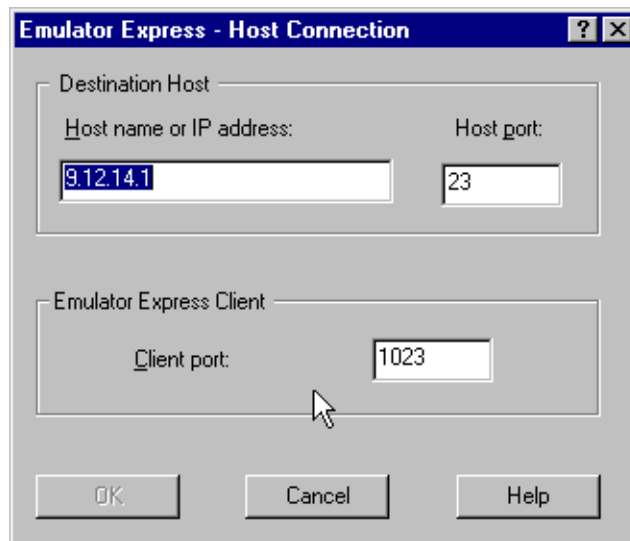


Figure 101. Emulator Express Client - Host Connection Configuration

Next, you will configure the host connection for session A. In our scenario, this session goes directly from the Emulator Express server to the VTAM system via IP. Therefore we configure the mainframe destination address (9.12.14.1) and the port number for this connection (23). This definition is for session A which is using port 1023 between PCOMM and the Emulator Express client.

In other words, any telnet traffic coming from PCOMM using port 1023 to the Emulator Express client will be directed to the Emulator Express server (9.24.106.143 and port 17000). From the Emulator Express server, traffic is sent directly to 9.12.14.1 (port 23).

The host name server or host IP address can be in the format of either dotted decimal (for example, 222.50.6.3) or a host name (for example, HOST1). If the IP address of the host is likely to change, using the host name is more reliable but more overhead.

In a similar way, you will configure the host connections for sessions B, C and D by entering the target host or Telnet server IP address and the port number. The following chart (Table 7 on page 195) illustrates the configuration values for the Telnet 3270 and 5250 sessions.

Table 7. Emulator Express Client - Emulation Sessions Configuration

Emulation Session	Host IP Address	Host Port	PCOMM Client Port
A	9.12.14.1	23	1023
B	127.0.0.1	2024	1024
C	127.0.0.1	2025	1025
D	9.24.104.162	23	1026

In our scenario, sessions B and C are configured with host server loopback IP address 127.0.0.1 because both the telnet server in Communications Server for Windows NT and the Emulator Express server reside in the same machine. In other words, there is no external communication between these two components.

7.7.3 PCOMM Telnet 3270 Configuration

In our scenario, PCOMM (configured as a Telnet 3270 client) and the Emulator Express client are installed in the same machine. Therefore, PCOMM is configured with Emulator Express client as the target for the 3270 traffic. That is, you enter the local loopback address 127.0.0.1 or the host name *localhost* which is always included in the hosts file in Windows NT for address resolution.

Note

Emulator Express client and the 3270/5250 emulator must reside in the same machine.

The real IP address interface can also be used but in this case we prefer to use the local loopback address because the IP address might change when using a DHCP server for example.

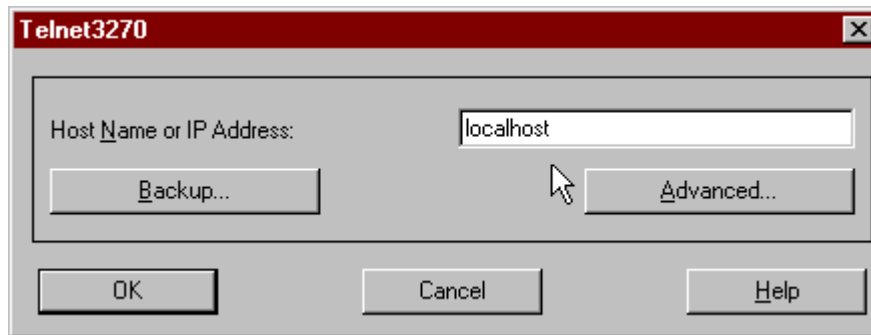


Figure 102. PCOMM Telnet Client Configuration - Target IP Address

By selecting the option **Advanced**, you enter the port number for the session between PCOMM telnet client and the Emulator Express client.

It is also recommended that you select the Auto-reconnect box. This option will allow PCOMM to retry the connection after session failures.

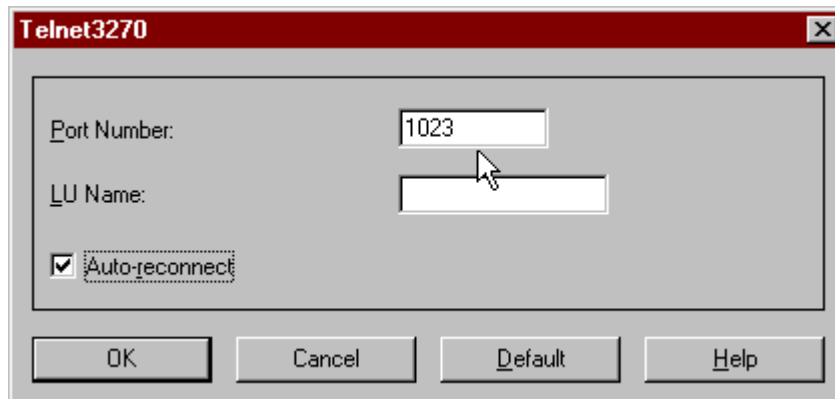


Figure 103. PCOMM Telnet 3270 Configuration - Port Number

Note

Although eNetwork Emulator Express is not TN3270E compliant, it supports the option (RFC 1646) to provide a specific LU name or pool name. However, you should also notice that printer selection is not available.

7.8 Troubleshooting

In this section we show you procedures for monitoring, viewing log messages and running traces. These tools are helpful if you need to troubleshoot configuration problems.

7.8.1 Monitoring

There are several tools you can use to monitor your Emulator Express sessions and you must be aware that both the Emulator Express client and server must be running in order to have all the connections established.

Note

In most cases, you will hear a beep if for any reason there is no communication between the Emulator Express client and server. However, this is a function provided by the Telnet 3270/5250 emulator and not by the eNetwork Emulator Express product.

7.8.1.1 Emulator Express Client Sessions

Every time a new session is established between the telnet client (PCOMM in our scenario) and the Emulator Express client, an entry is created for that connection (see Figure 104 on page 197). The entry shows the connection start time as well as the host IP address. The host IP address can be either a mainframe or a server supporting the telnet server protocols. For example, in our scenario we have configured the TN3270E server and the TN5250 server in eNetwork Communications Server for Windows NT, Version 6.0.

In this sample configuration, the *localhost* address 127.0.0.1 indicates that the TN3270 server and Emulator Express server are running in the same machine.

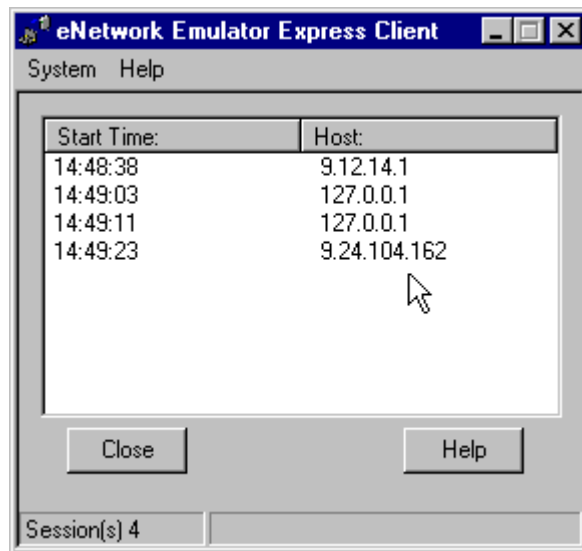


Figure 104. Monitoring Emulator Express Client

Note

Although up to twelve sessions can be configured, the Emulator Express client allows for a maximum of up to eight active emulation sessions at one time.

7.8.1.2 Emulator Express Server Sessions

When a new session is established the Emulator Express server displays an entry for that connection. The entry shows the connection start time, the telnet client IP address and the host IP address. The host IP address can be either a mainframe or a server supporting the telnet server protocols. For example, in our scenario we have configured the TN3270E server and the TN5250 server in eNetwork Communications Server for Windows NT, Version 6.0.

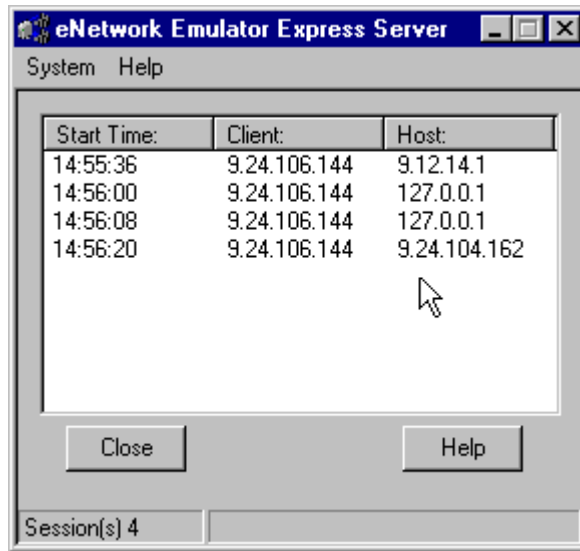


Figure 105. Monitoring Emulator Express Server

Since the telnet 3270 and 5250 servers are running in the same machine as the Emulator Express server, the loopback address 127.0.0.1 is used as the destination address for sessions B (TN3270) and C (TN5250).

7.8.1.3 Communications Server Telnet Sessions

If the Emulator Express server sessions are connected to a TN3270 (E) server or to a TN5250 server such as the support provided by eNetwork Communications Server for Windows NT, you may want to monitor the sessions using the provided Node Operations Facility (NOF) as explained in this section.

The Node Operations Facility (NOF) of eNetwork Communications Server for Windows NT is used to monitor the telnet sessions using the TN3270E server and the TN5250 server.

In most cases, you will need to verify that the configured ports are active to make sure the telnet server is listening on the properly configured port with the Emulator Express server.

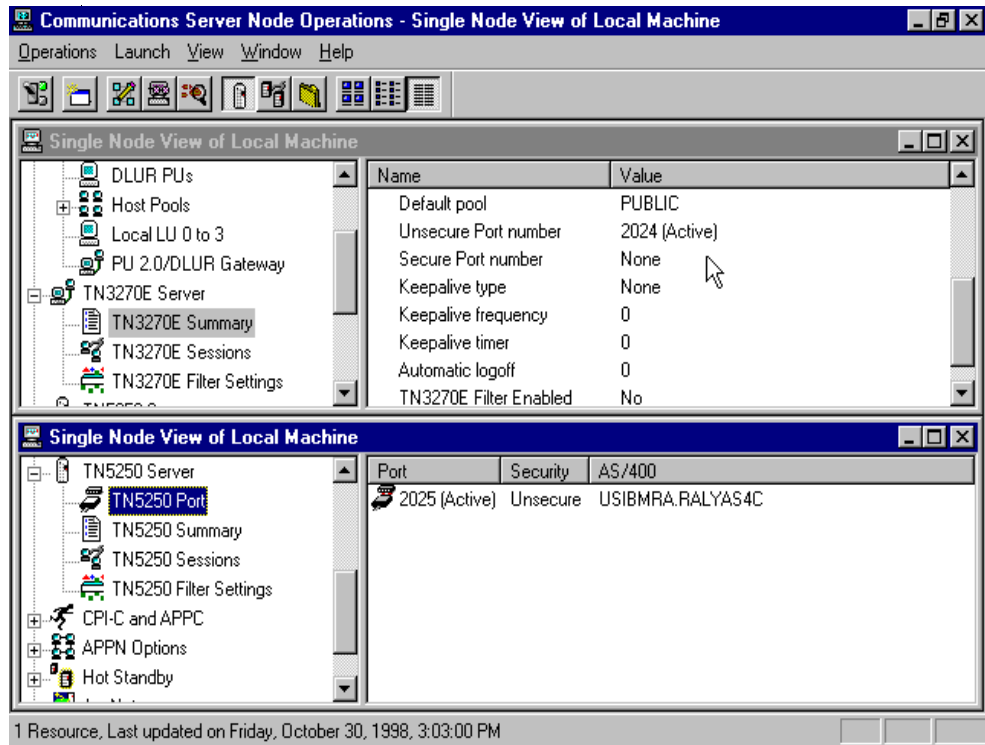


Figure 106. Monitoring Telnet 3270/5250 Active Ports in CS/NT Server

In our scenario, port 2024 is used by the TN3270E server for the connection with the Emulator Express server and it is active. Port 2025 is used by the TN5250 server and it is also active as indicated in Figure 106 on page 199.

The telnet sessions can also be displayed by using the Node Operations Facility as shown in Figure 107 on page 200.

When using a telnet server such as the TN3270E server in Communications Server for Windows NT, you will also need to configure the upstream connection to the mainframe. This connection can be either a subarea or APPN connection. In a subarea connection, the link configuration defines the Physical Unit (PU) while in an APPN connection a DLUR PU must be configured.

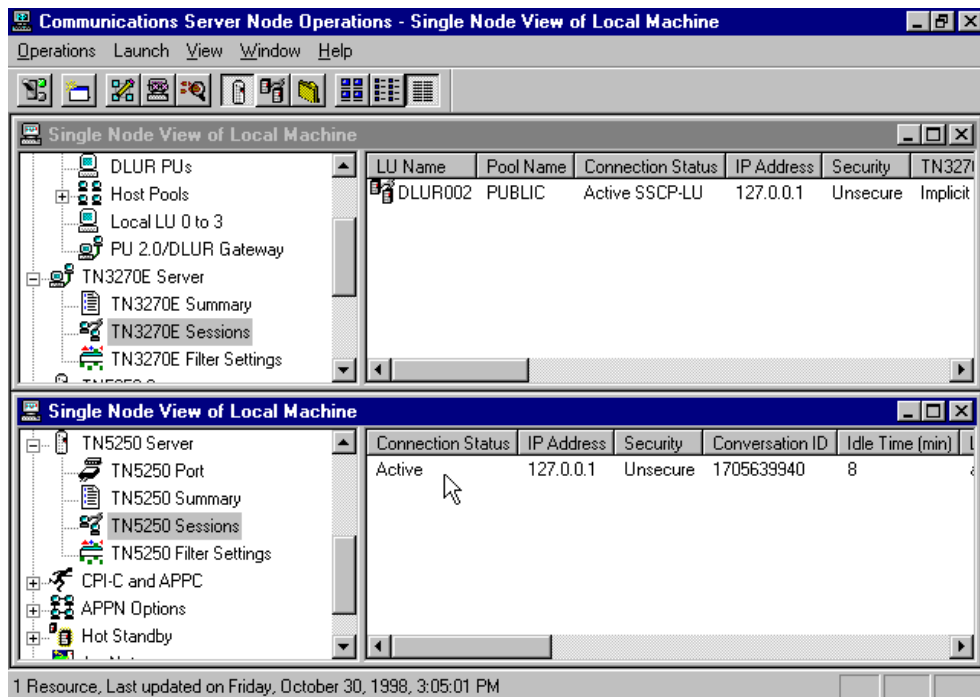


Figure 107. Monitoring Telnet 3270/5250 Active Sessions in CS/NT Server

In most cases, you will also need to configure host LU pools and multiple PUs are also allowed to support a large number of sessions. For information on how to configure a TN3270E server and a TN5250 server in Communications Server for Windows NT, see *IBM eNetwork Communications Server for Windows NT, Version 6.0 Enhancements, SG24-5232*.

7.8.2 Logging

Emulator Express implements a log facility that you can browse when required. You will find log files for both, the Emulator Express client and server. In this section we provide some information about how you can browse these files when looking for information about problems or simply when you just want to monitor the Emulator Express logged events.

7.8.2.1 Emulator Express Log File - Client

The Emulator Express client log file name is `emeexpl.log`. This file is dynamically updated when Emulator Express client is running.

Note

Emulator Express client should be started before you start any communications with the Telnet 3270/5250 clients.

Figure 108 on page 201 illustrates a portion of the log file. The file shows the Emulator Express client version number, the ports on which it is listening for Telnet 3270/5250 client requests and so on. In our scenario, our Telnet 3270/5250 client requests are coming through port numbers 1023, 1024, 1025 and 1026.


```

Emexpcl - Notepad
File Edit Search Help
Date Time Originator Message
10/16/98 15:04:46 05001BE1 EMX05081: Emulator Express Client (version 4.1.3A) starting on
10/16/98 15:04:46 05050FF1 EMX05021: Listening for connections on port 1023.
10/16/98 15:04:46 05050FF1 EMX05021: Listening for connections on port 1024.
10/16/98 15:04:46 05050FF1 EMX05021: Listening for connections on port 1025.
10/16/98 15:04:46 05050FF1 EMX05021: Listening for connections on port 1026.
10/16/98 15:05:24 040009C1 EMX05041: Closing listen socket 148.
10/16/98 15:05:24 040009C1 EMX05041: Closing listen socket 156.
10/16/98 15:05:24 040009C1 EMX05041: Closing listen socket 152.
10/16/98 15:05:24 040009C1 EMX05041: Closing listen socket 160.
10/16/98 15:05:24 05050FF1 EMX05021: Listening for connections on port 1023.
10/16/98 15:05:24 05050FF1 EMX05021: Listening for connections on port 1024.
10/16/98 15:05:24 05050FF1 EMX05021: Listening for connections on port 1025.
10/16/98 15:05:24 05050FF1 EMX05021: Listening for connections on port 1026.
10/16/98 15:06:07 05011501 EMX05111: Session 13 starting: client 127.0.0.1, destination ho
10/16/98 15:08:25 05011501 EMX05111: Session 14 starting: client 127.0.0.1, destination ho
10/16/98 15:08:26 050140C1 EMX05141: Session 14 statistics: 1 elapsed seconds; bytes 0 ->
10/16/98 15:08:26 05011FD1 EMX05121: Session 14 ending: client 127.0.0.1, destination host
10/16/98 15:08:27 05011501 EMX05111: Session 15 starting: client 127.0.0.1, destination ho
10/16/98 15:08:29 050140C1 EMX05141: Session 15 statistics: 1 elapsed seconds; bytes 0 ->
10/16/98 15:08:29 05011FD1 EMX05121: Session 15 ending: client 127.0.0.1, destination host
10/16/98 15:08:30 05011501 EMX05111: Session 16 starting: client 127.0.0.1, destination ho
10/16/98 15:08:31 050140C1 EMX05141: Session 16 statistics: 1 elapsed seconds; bytes 0 ->
10/16/98 15:08:31 05011FD1 EMX05121: Session 16 ending: client 127.0.0.1, destination host
10/16/98 15:08:32 05011501 EMX05111: Session 17 starting: client 127.0.0.1, destination ho
10/16/98 15:08:34 050140C1 EMX05141: Session 17 statistics: 1 elapsed seconds; bytes 0 ->
10/16/98 15:08:34 05011FD1 EMX05121: Session 17 ending: client 127.0.0.1, destination host
10/16/98 15:08:35 05011501 EMX05111: Session 18 starting: client 127.0.0.1, destination ho
10/16/98 15:08:36 050140C1 EMX05141: Session 18 statistics: 1 elapsed seconds; bytes 0 ->
10/16/98 15:08:36 05011FD1 EMX05121: Session 18 ending: client 127.0.0.1, destination host
10/16/98 15:08:37 05011501 EMX05111: Session 19 starting: client 127.0.0.1, destination ho

```

Figure 108. Emulator Express Client - Log File

7.8.2.2 Emulator Express Log File - Server

The Emulator Express server log file name is emexpsr.log. This file is dynamically updated when Emulator Express server is running.

```

Emexpsr - Notepad
File Edit Search Help
Date Time Originator Message
10/15/98 17:17:26 09010F13 EMX0923E: Cannot open pipe for NT service. ErrorCode = 2
10/15/98 17:17:26 05001C31 EMX05081: Emulator Express Server (version 4.1.3A) starting on
10/15/98 17:17:26 05050FF1 EMX05021: Listening for connections on port 17000.
10/15/98 17:17:34 040009C1 EMX05041: Closing listen socket 156.
10/15/98 17:17:34 05000BE3 EMX0506E: Session support ended. No new connections accepted.
10/15/98 17:17:47 09010F13 EMX0923E: Cannot open pipe for NT service. ErrorCode = 2
10/15/98 17:17:47 05001C31 EMX05081: Emulator Express Server (version 4.1.3A) starting on
10/15/98 17:17:47 05050FF1 EMX05021: Listening for connections on port 17000.
10/15/98 17:18:43 040009C1 EMX05041: Closing listen socket 156.
10/15/98 17:18:43 05000BE3 EMX0506E: Session support ended. No new connections accepted.
10/15/98 17:18:57 09010F13 EMX0923E: Cannot open pipe for NT service. ErrorCode = 2
10/15/98 17:18:57 05001C31 EMX05081: Emulator Express Server (version 4.1.3A) starting on
10/15/98 17:18:57 05050FF1 EMX05021: Listening for connections on port 17000.
10/15/98 17:20:31 040009C1 EMX05041: Closing listen socket 156.
10/15/98 17:20:31 05000BE3 EMX0506E: Session support ended. No new connections accepted.
10/15/98 17:21:12 09010F13 EMX0923E: Cannot open pipe for NT service. ErrorCode = 2
10/15/98 17:21:12 05001C31 EMX05081: Emulator Express Server (version 4.1.3A) starting on
10/15/98 17:21:12 05050FF1 EMX05021: Listening for connections on port 17000.
10/15/98 17:21:35 040009C1 EMX05041: Closing listen socket 156.
10/15/98 17:21:35 05000BE3 EMX0506E: Session support ended. No new connections accepted.
10/15/98 17:21:42 09010F13 EMX0923E: Cannot open pipe for NT service. ErrorCode = 2
10/15/98 17:21:42 05001C31 EMX05081: Emulator Express Server (version 4.1.3A) starting on
10/15/98 17:21:42 05050FF1 EMX05021: Listening for connections on port 17000.
10/15/98 17:42:45 05011501 EMX05111: Session 2 starting: client 192.168.20.2, destination
10/15/98 17:44:29 05014211 EMX05141: Session 2 statistics: 104 elapsed seconds; bytes 80 -
10/15/98 17:44:29 05014531 EMX05431: Session summary,2,10/15/98,17:42:45,10/15/98,17:44:29
10/15/98 17:44:29 05011FD1 EMX05121: Session 2 ending: client 192.168.20.2, destination ho
10/15/98 17:44:55 05011501 EMX05111: Session 3 starting: client 192.168.20.2, destination
10/15/98 17:46:00 05011501 EMX05111: Session 4 starting: client 192.168.20.2, destination
10/15/98 17:46:56 05014211 EMX05141: Session 4 statistics: 56 elapsed seconds; bytes 91 ->

```

Figure 109. Emulator Express Server - Log File

When troubleshooting for configuration problems, the Emulator Express server provides valuable information in the log file. In our scenario, the log file contains entries related to the connection activity. For example, it shows that the Emulator Express server is listening for client connections on port 17000 which, in our scenario, is the port number used with the Emulator Express client stations.

Note

Emulator Express server should be started before you attempt any connections with Emulator Express clients.

You should also note that the eNetwork Emulator Express log files can be used for statistical analysis of traffic, for example, using spreadsheet tools. For details see <http://www.ibm.com/software/enetwork/mobile/support>.

7.8.3 Traces

A trace facility has been implemented in the Emulator Express client and server. In this section we provide a sample of the trace files.

Note

Running traces in Emulator Express will always create an extra overhead. You should only enable traces when specifically required.

7.8.3.1 Emulator Express Trace File - Client

If the Emulator Express client log file does not give you enough information to troubleshoot a potential problem, your last resort is to run traces. You will also be required to run traces if there is a potential product defect.

```
Emexpc1.trc - Notepad
File Edit Search Help
-- 1998-11-16 --
16:59:56 [CNFG] GUI: Set trace values
16:59:56 [TRAN] TCPCircuit: 0001 Closing listen socket 148
16:59:56 [TRAN] TCPCircuit: 0002 Closing listen socket 156
16:59:56 [TRAN] TCPCircuit: 0003 Closing listen socket 152
16:59:56 [TRAN] TCPCircuit: 0004 Closing listen socket 160
16:59:56 [TRAN] TCPCircuit: 0001 Listen socket 148 opened

16:59:56 [TRAN] TCPCircuit: 0001 Socket local address bound

16:59:56 [TRAN] TCPCircuit: 0001 Listening to socket 148

16:59:56 [CTRL] Open_Listener: 0001 Listening for host connection requests on TCP port 1023
16:59:56 [TRAN] TCPCircuit: 0002 Listen socket 152 opened

16:59:56 [TRAN] TCPCircuit: 0002 Socket local address bound
16:59:56 [TRAN] TCPCircuit: 0002 Listening to socket 152

16:59:56 [CTRL] Open_Listener: 0002 Listening for host connection requests on TCP port 1024
16:59:56 [TRAN] TCPCircuit: 0003 Listen socket 156 opened

16:59:56 [TRAN] TCPCircuit: 0003 Socket local address bound

16:59:56 [TRAN] TCPCircuit: 0003 Listening to socket 156

16:59:56 [CTRL] Open_Listener: 0003 Listening for host connection requests on TCP port 1025
16:59:56 [TRAN] TCPCircuit: 0004 Listen socket 168 opened

16:59:56 [TRAN] TCPCircuit: 0004 Socket local address bound
```

Figure 110. Emulator Express Client - Trace File

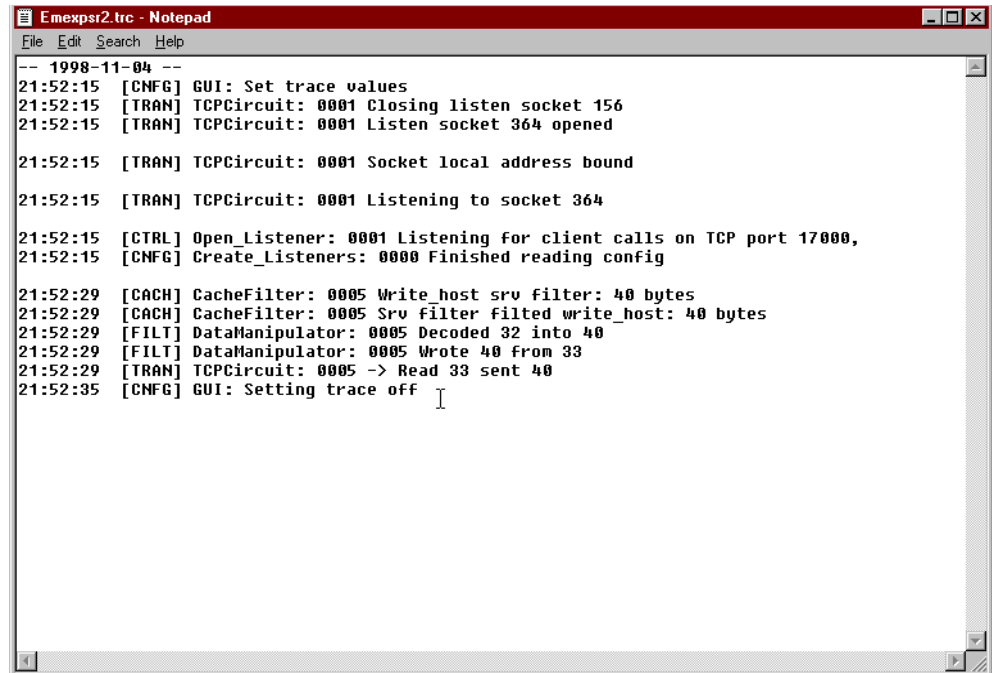
The trace facility is activated in the Emulator Express advanced configuration. For details on how you activate traces in your workstation see Figure 97 on page 191.

The name of the trace file is emexpcl.trc. A sample trace is provided in Figure 110 on page 202. In this trace, you can, for example, see the TCP circuit entries and the open listener entries for the Telnet 3270/5250 session ports we are using in our scenario (1023, 1024 and so forth).

7.8.3.2 Emulator Express Trace File - Server

In a similar way, the Emulator Express server trace facility can be invoked to trace the server activity. Traces are set in the Emulator Express server advanced configuration. For details on how you can set these traces, see Figure 95 on page 179.

Figure 111 on page 203 illustrates a sample trace with entries related to the server itself. Notice, for example, that it shows an entry indicating that the server is listening for client calls on the default TCP port 17000. This port is used for connections with the Emulator Express clients.



```
Emexpsr2.trc - Notepad
File Edit Search Help
-- 1998-11-04 --
21:52:15 [CNFG] GUI: Set trace values
21:52:15 [TRAN] TCPCircuit: 0001 Closing listen socket 156
21:52:15 [TRAN] TCPCircuit: 0001 Listen socket 364 opened

21:52:15 [TRAN] TCPCircuit: 0001 Socket local address bound

21:52:15 [TRAN] TCPCircuit: 0001 Listening to socket 364

21:52:15 [CTRL] Open_Listener: 0001 Listening for client calls on TCP port 17000,
21:52:15 [CNFG] Create_Listeners: 0000 Finished reading config

21:52:29 [CACH] CacheFilter: 0005 Write_host srv filter: 40 bytes
21:52:29 [CACH] CacheFilter: 0005 Srv filter filtered write_host: 40 bytes
21:52:29 [FILT] DataManipulator: 0005 Decoded 32 into 40
21:52:29 [FILT] DataManipulator: 0005 Wrote 40 from 33
21:52:29 [TRAN] TCPCircuit: 0005 -> Read 33 sent 40
21:52:35 [CNFG] GUI: Setting trace off
```

Figure 111. Emulator Express Server - Trace File

The name of the trace files in the Emulator Express server are emexpsr.trc, emexpsr2.trc and so on.

Chapter 8. IBM eNetwork Web Express

Wireless communications in Wide Area Networks (WANs) present several problems when running Web-based applications. This is mainly because, at the present time, mobile communication links are slow, more expensive than wireline links and often they are not so reliable. In addition to this, Web-based applications use the Hyper Text Transport Protocol (HTTP) which is more suitable for wireline WAN networks. When implemented over wireless networks, the HTTP protocol also presents some inefficiencies related to its architecture and implementation issues. In addition, as compared to 3270 or 5250 data, the use of HTML documents and images greatly increases the burden placed on these links.

This chapter provides an overview of the IBM eNetwork Web Express product and how it addresses these issues. We also include a section on the installation process, configuration and a sample scenario.

8.1 Introduction

Although Web Express can run over any network supporting TCP/IP, it allows Web-based applications to run over wireless networks supported by the IBM eNetwork Wireless Gateway.

Web technology has rapidly become very popular as a standard interface for network access to information. Today, more and more Web-based applications are being deployed over local area networks (LANs) and wireline wide area networks (WANs). Furthermore, wireless WANs are also becoming increasingly popular and the ability to run Web-based applications over these networks is a critical requirement.

In this section we present some issues on how wireless networks affect Web-based applications.

8.1.1 Wireless Networks and Web-Based Applications

In general, wireless networks present the following negative characteristics which affect the transport of native Web applications using the HTTP protocol:

- High cost. Transporting HTML pages over wireless networks is several times more expensive than using a traditional LAN or WAN wireline network.
- Slow response time. The response time for wireless connections is very slow compared to LAN or WAN wireline connections.
- Low bandwidth. Wireless link's capacity is very limited compared to a wireline link. For example, Ardis MDC4800 offers 4800 bps and CDPD offers 19200 bps. Moreover, the effective rate becomes substantially lower due to slow response times, re-transmission and so on.
- Very unreliable. Wireless connections are significantly less reliable than wireline connections as they are constantly being disrupted for various reasons, such as mobile device out of range conditions, signals are blocked and time-outs due to delayed responses.

Web-based applications implement Hyper Text Markup Language (HTML), for the representation of the information, and the Hyper Text Transfer Protocol (HTTP) for the communication between Web browsers (clients) and Web servers.

The Web browser is responsible for sending a client request to a Web server and for formatting and displaying HTML data streams returned as a response to the request.

Besides enabling information retrieval and browsing, Web technology provides an inexpensive, and hence attractive, way to create form-based applications. The ease of creating forms using HTML and of writing Web applications using the HTTP-defined Common Gateway Interface (CGI) provide the standard way to handle transactions between the World Wide Web and end users.

When running Web applications over wireless networks without the assistance of eNetwork Web Express, the following issues make Web applications not suitable to run over wireless networks:

- Connection overhead. Each request for an HTML page or graphic object (for example, GIF or JPEG) requires the Web browser to open a TCP/IP connection where each request/response usually requires a minimum of 11 packet exchanges.
- Redundant transmission of capabilities. The HTTP protocol is stateless and therefore the Web browser must send its capabilities within each request.
- Verbose protocol. HTTP control information is coded in standard ASCII which considerably increases the number of bytes being transmitted.

8.2 Web Express Implementation

eNetwork Web Express implements an efficient technique to intercept HTTP messages aimed to reduce the traffic volume and optimize the communication protocol in order to improve the response time.

Web Express uses paired proxies to optimize communication in low-bandwidth networks and to support an asynchronous browsing model that helps mask the effect of slow and unreliable networks. The resulting environment allows Web-based applications to be effectively used over wireless networks.

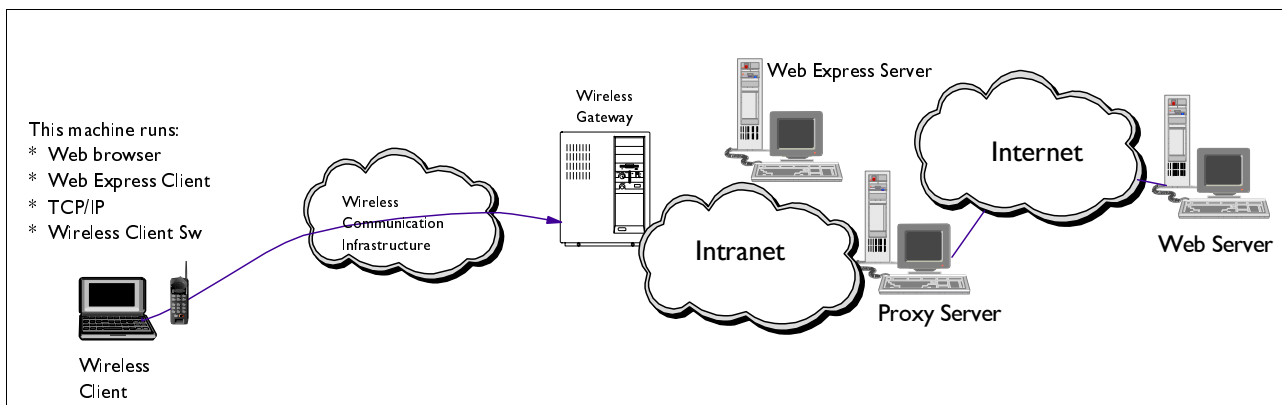


Figure 112. Web Express in a Wireless Network

An important objective of eNetwork Web Express is to be able to run with any Web browser. For example, Netscape, Internet Explorer or any other Web browser without requiring any changes to it.

A proxy server is software inserted into the client-to-server communication path. An intermediary proxy sees all data and control information that flows between client and server. A proxy server may perform arbitrary actions on the data that flows through it, including the caching of data for later processing. Any number of proxies may be arranged in sequence. Both client and server are generally unaware of any proxies that stand between them.

eNetwork Web Express uses proxies to intercept and control communication over the mobile link for the purposes of reducing traffic volume and optimizing the communications protocol to reduce latency.

8.2.1 eNetwork Web Express Components

Web Express implements the client/server model. The Web Express client and server collaborate to reduce the number of requests and the quantity of data sent over a wireless network. The Web Express client intercepts Web browser requests and forwards only the minimum information to the Web Express server. Likewise, the Web Express server intercepts Web server responses and provides corresponding data reductions when returning those responses to the Web Express client.

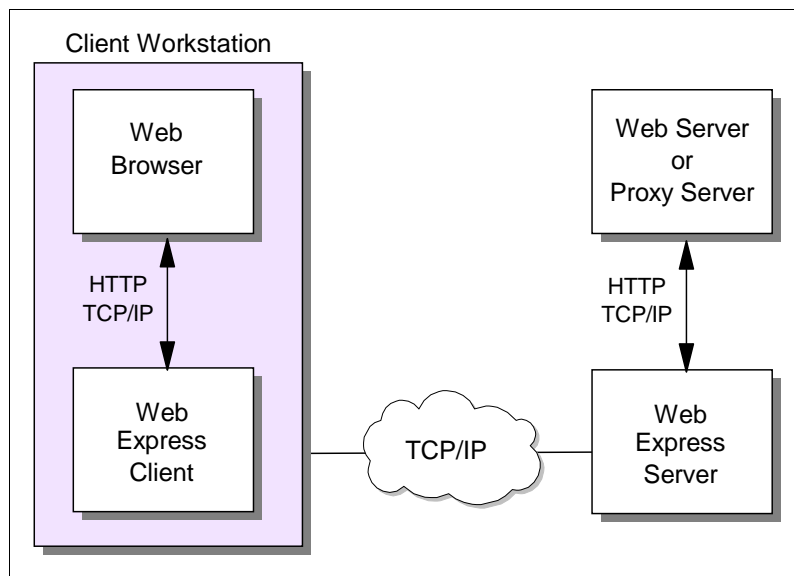


Figure 113. Web Express Client/Server Components and Connectivity

In this implementation of the Web Express, we notice that the Web browser sees the Web Express client as a proxy server. For this reason, the Web Express client is actually intercepting the HTTP requests from the Web browser. In most of the cases, the Web browser and the Web Express client reside in the same machine as illustrated in Figure 113 on page 207.

The Web Express client and server communicate using a TCP/IP sockets session and the connection can be either wireless or wireline. Finally, the Web Express server uses the HTTP protocol to connect to a Web server (or Proxy server if

required). To the Web server (or Proxy server) the Web Express server is acting as a Web browser

Note

In the current release of the Web Express server, you cannot configure a Socks server. Therefore, if you are required to use a Socks server, you will need to "socksify" the machine using the operating system facilities.

8.2.2 eNetwork Web Express Optimization Methods

The components that implement the HTTP intercept technique are shown in Figure 113 on page 207. Two proxies are inserted into the data path between the Web client and the Web server: the *Client Side Interceptor* (CSI), implemented in the Web Express client, runs in the client's mobile device and the *Server Side Interceptor* (SSI), implemented in the Web Express server, runs within the wireline network. The CSI intercepts the HTTP requests and, together with the SSI, performs optimizations to reduce data transmission over the wireless link.

The optimization methods implemented in the Web Express client/server can be summarized as follows:

- **Caching:** The CSI caches graphic and HTML objects. If a URL corresponds to an object in the CSI's cache, the object is returned immediately to the browser as the response. The cache functions guarantee cache integrity within the client-specified time interval.
- **Differencing:** CGI requests result in responses that normally vary for multiple requests to the same URL. The concept of differencing is to cache a common base object on both the CSI and SSI. When a response is received, the SSI computes the difference between the base object and the response and sends the difference to the CSI. The CSI then merges the difference between HTML documents.
- **Protocol reduction:** Each CSI connects to its SSI with a single TCP/IP connection. All requests are routed over this connection to avoid the costly overhead of connection establishment. Requests and responses are multiplexed over the connection.
- **Header reduction:** The HTTP protocol is stateless, requiring that each request contain the browser's capabilities (called access list in HTTP). For a given browser, this information is the same for all requests. When CSI establishes a connection with its SSI, it sends its capabilities only at the first request. This information is maintained by the SSI for the duration of the connection. The SSI includes the capabilities as part of the HTTP request that it forwards to the target server in the wireline network

8.2.3 Web Express Solution Highlights

The current implementation of the eNetwork Web Express meets the objectives to be able to run Web applications over wireless networks by providing the following functionality:

1. Gives access to the Internet and World Wide Web over wireless and dial-up networks.
2. Processes Web requests in the background while mobile users perform other browser tasks.

3. Allows Web page downloads to be stored locally for offline access to reduce wireless network connect-time charges.
4. Enables Web transactions to be prepared offline to reduce connect time and expenses.
5. Includes cost-efficient queuing, caching, image intercept, data compression, and differencing through patented optimization techniques.
6. Reduces data traffic by 70% to 95% or more and uses industry-standard browsers.
7. Supports a wide range of networks for a truly global solution.

8.2.4 Supported Platforms

The Web Express server is available on the AIX and Windows NT platforms and it can reside:

- On the same system as your Web server
- On the same system as your eNetwork Wireless Gateway server (AIX only)
- On a system separate from the eNetwork Wireless Gateway server (for example, connected through a LAN)

The Web Express client usually runs on a mobile computer such as an IBM ThinkPad with one of the following operating systems:

- Windows 3.1 (a subset of the Web Express is available)
- Win95/Win98
- Windows NT workstation or server

8.2.5 Web Express Server Installation - Windows NT

The Web Express server can be installed from CD-ROM or from diskettes. To install the product, run "Setup" from diskette or from CD-ROM drive. You will then proceed to enter or take default values for the following installation options:

- Select the target directory for the installation.
- Select how you want to start the Web Express server. It can be started either from an icon or from NT services in a Windows NT machine.
- Provide the program folder name to be used if required.

If this is your first installation of the Web Express server, you may want to read the included READ.ME file for details before you attempt the actual installation.

If you need to uninstall the Web Express server, make sure your server sessions have ended and for example, in Windows NT, use the Add/Remove Programs option in the Windows NT control panel to remove the Web Express server.

8.2.6 Web Express Server Installation - AIX

Web Express server can also be installed on the same machine where the Wireless Gateway resides in order to give a shortest path to the entrance of the client stations.

The Web Express Server Version 2.1.1 for AIX software comes with the CD-ROM. To install it, for example, you log on as **root** and run **smitty**. You will then select

Software Installation and Maintenance and Install and Update Software to obtain the following screen:

```
Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry Fields]
* INPUT device / directory for software      /dev/cd0
* SOFTWARE to install                       [webexpress.rte]      +
PREVIEW only? (install operation will NOT occur) no      +
COMMIT software updates?                   yes                +
SAVE replaced files?                       no                 +
AUTOMATICALLY install requisite software?  yes                +
EXTEND file systems if space needed?       yes                +
OVERWRITE same or newer versions?         no                 +
VERIFY install and check file sizes?       no                 +
Include corresponding LANGUAGE filesets?   yes                +
DETAILED output?                          no                 +
Process multiple volumes?                  yes                +
```

You specify the input device to be used, in this case, we enter **/dev/cd0** for the CD-ROM drive and the Object Name is **webexpress.rte**. To list a specific object, press **F4** at the Entry Field.

8.3 Sample Scenario

In this section we show you a Web Express configuration for the scenario shown in Figure 114 on page 211. In this scenario, we install a Web browser and the Web Express client in the same workstation. The workstation communicates via a wireless or wireline to a machine running the Web Express server. The Web Express server connects to the Internet via an HTTP Proxy server.

We do not show the wireless connection in this chapter. For details on how you can configure the client workstation to connect to a wireless network, see Chapter 4, "Wireless Client" on page 107.

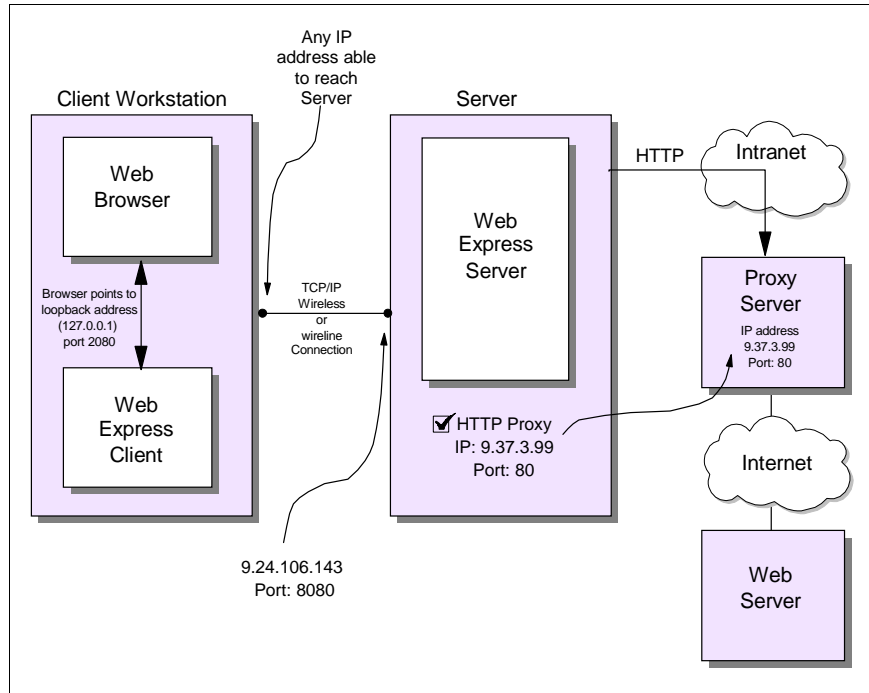


Figure 114. IBM eNetwork Web Express - Sample Scenario

As illustrated in Figure 114 on page 211, in this sample scenario, the Web Express server is configured to access the proxy server (IP address 9.37.3.99) and the Web Express server IP address is 9.24.106.143.

8.3.1 Web Express Server Basic Configuration - Windows NT

The configuration wizard is invoked when you create a new eNetwork Web Express server configuration profile and the basic configuration parameters should be entered. Figure 115 on page 212 shows the initial screen for the configuration wizard.

When creating a new configuration profile, the port number for the IP connection with the eNetwork Web Express clients, the HTTP proxy sever IP address and other related information should be configured. For information on how these values are configured see 8.3.2, "Web Express Advanced Configuration - Windows NT" on page 213.

The configuration wizard will also give you the option to select the advanced configuration option in case you want to change the default values initially provided for you. In the section we include a detailed explanation for the basic and advanced configuration parameters.

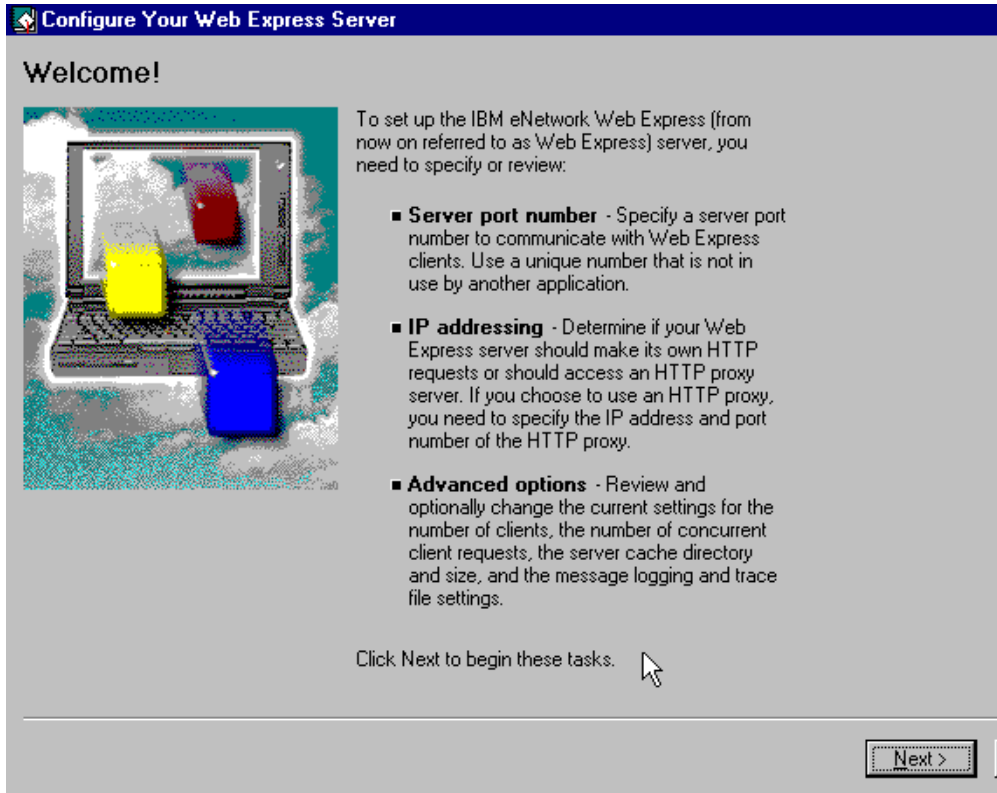


Figure 115. Web Express Basic Configuration

Figure 116 on page 212 shows the configuration summary for the sample scenario illustrated in Figure 114 on page 211.

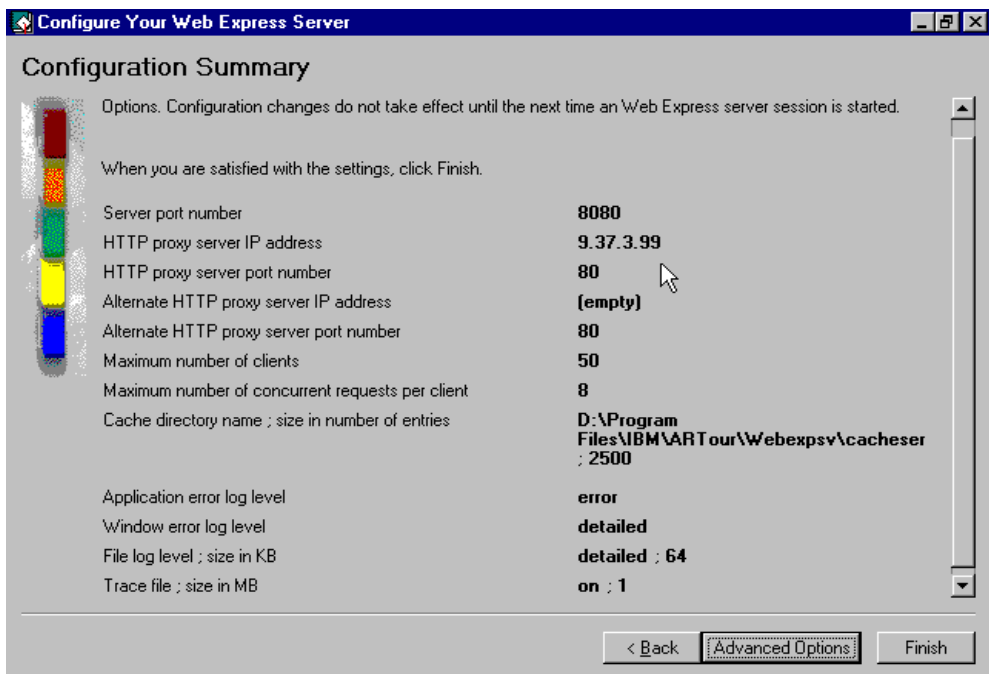


Figure 116. Web Express Server - Basic Configuration Summary

8.3.2 Web Express Advanced Configuration - Windows NT

If required, once you have created the configuration profile, the advanced configuration option can be invoked to configure properties. If this is the case, you will select **Configure Properties** from the installed Web Express server folder to start the advanced configuration process. You will then be required to configure the following screens:

1. Addresses
2. Cache
3. Logging
4. Advanced
5. Options

In the rest of this section, we describe the configuration parameters and options for our sample scenario illustrated in Figure 114 on page 211.

8.3.2.1 Addresses

In this panel, you configure the IP connections to the Web Express client and the Proxy server if you have one. In our scenario, port 8080 is used for the IP connection with the Web Express client as shown in Figure 117 on page 213.

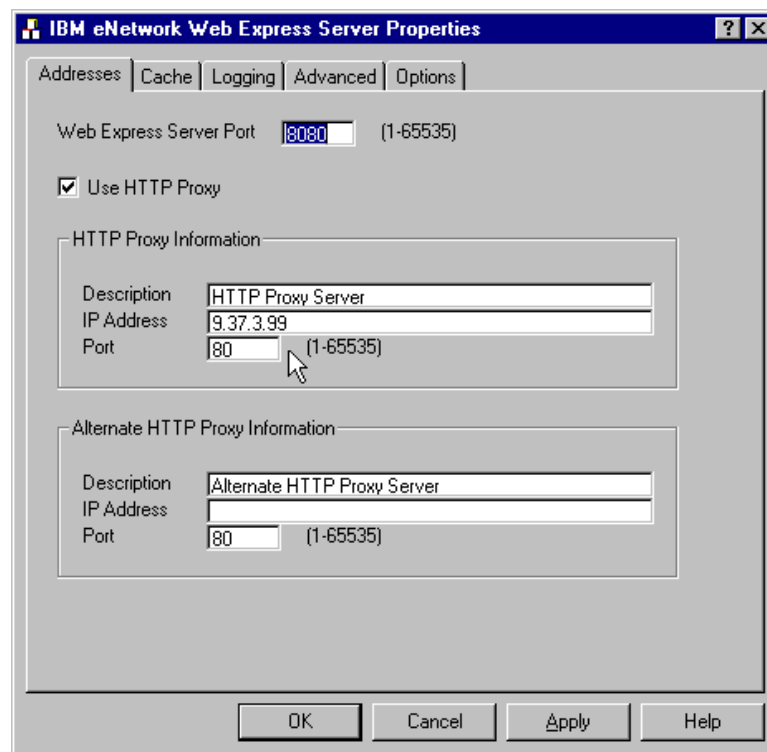


Figure 117. Web Express Server Properties - Addresses Configuration

If you are not required to use a Proxy server in your installation you may want to proceed to the next screen. However, in our scenario, we are required to use a Proxy server to access the Internet. Therefore, the "Use HTTP Proxy" box must be selected and the configuration for primary and alternate Proxy servers become available.

Note

Notice that Web Express server does not allow you to configure a Socks server in this release.

We configure the IP address (9.37.3.99) and port number (80) for the HTTP Proxy server. Since we are not using a backup Proxy server, we do not configure the alternate Proxy server.

8.3.2.2 Cache Configuration

In this panel you configure the name of the directory or subdirectory where cached files are stored. You must have full control permission to this directory. The default directory is created during installation. In this case we use the default value and it is D:\Program Files\IBM\ARTour\Webexpsv\cacheser as shown in Figure 118 on page 214.

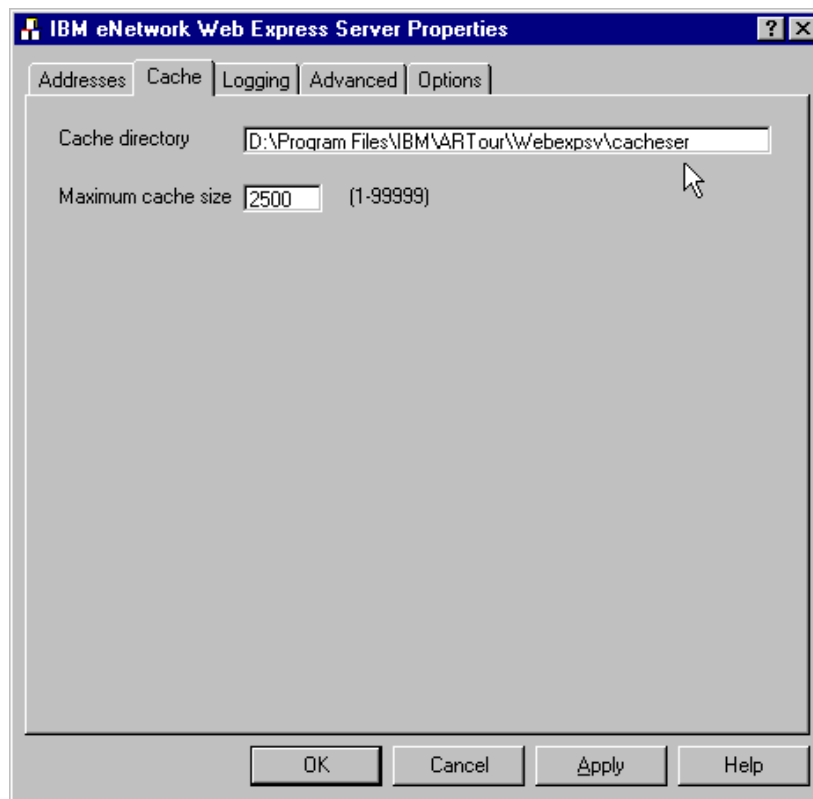


Figure 118. Web Express Server Properties - Cache Configuration

You can also specify the maximum number of text entries that can be cached. Non-text items (for example, graphics and applets) are not cached in the server. When the cache is full, the most-recently requested files are kept and the least-recently requested files are deleted.

In our configuration, we select the default value of 2500 entries which, in most of the cases, is an acceptable value for Web applications. The range can be from 1 entry to 99999 entries as seen in Figure 118 on page 214.

8.3.2.3 Logging Configuration

These are the configuration options for file logging, window logging and application logging. The default value is no logging for file and window logging and only application errors should be logged.

Use the default values for better Web Express Server performance, unless you need them for monitoring. See Figure 119 on page 215.

Note

Excessive logging may affect the performance of the Web Express server.

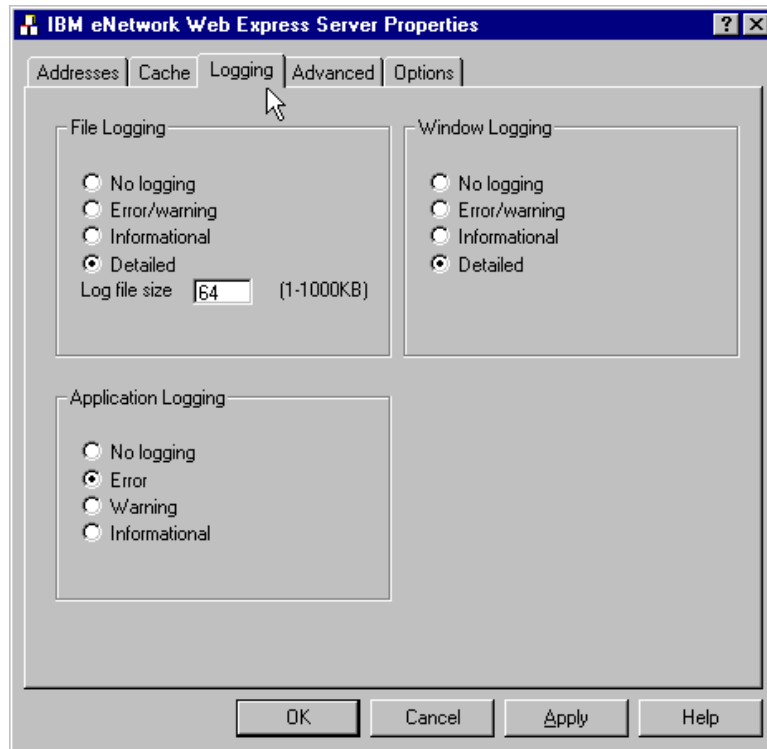


Figure 119. Web Express Server Properties - Logging Configuration

8.3.2.4 Advanced Configuration

You can direct real-time status information to a trace file while running the Web Express server. Located in the installation directory, the trace file is named `ssitrace.trc`.

Since tracing can impact performance, you should enable tracing only when requested to do so by service personnel. Each time a Web Express server session is started, the previous trace file is erased and trace information for the current session is recorded.

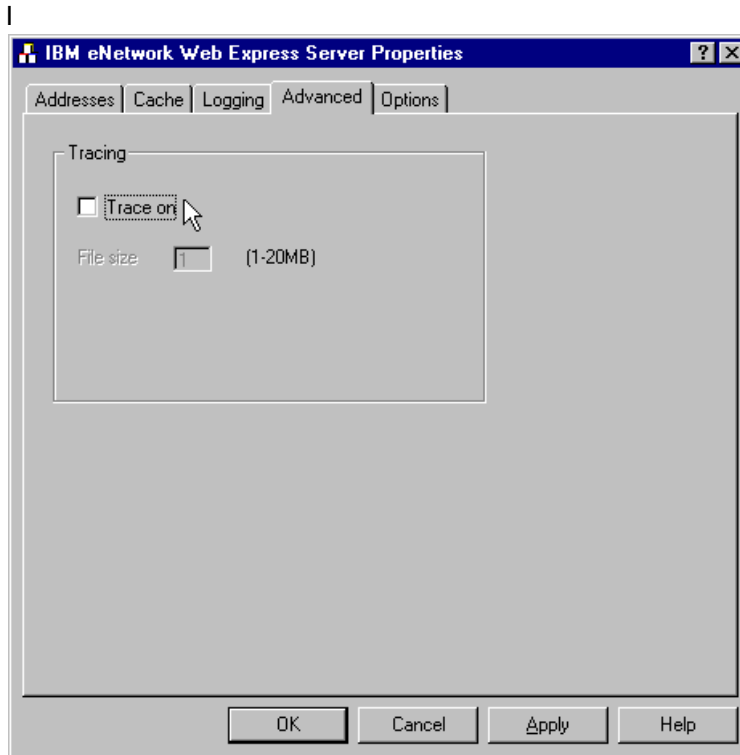


Figure 120. Web Express Server Properties - Advanced Configuration

If you have to set traces in the Web Express server, select the "Trace on" box and enter the trace file size if the default value of 1 MB is not large enough. See Figure 120 on page 216. A sample trace is included in Figure 121 on page 216.

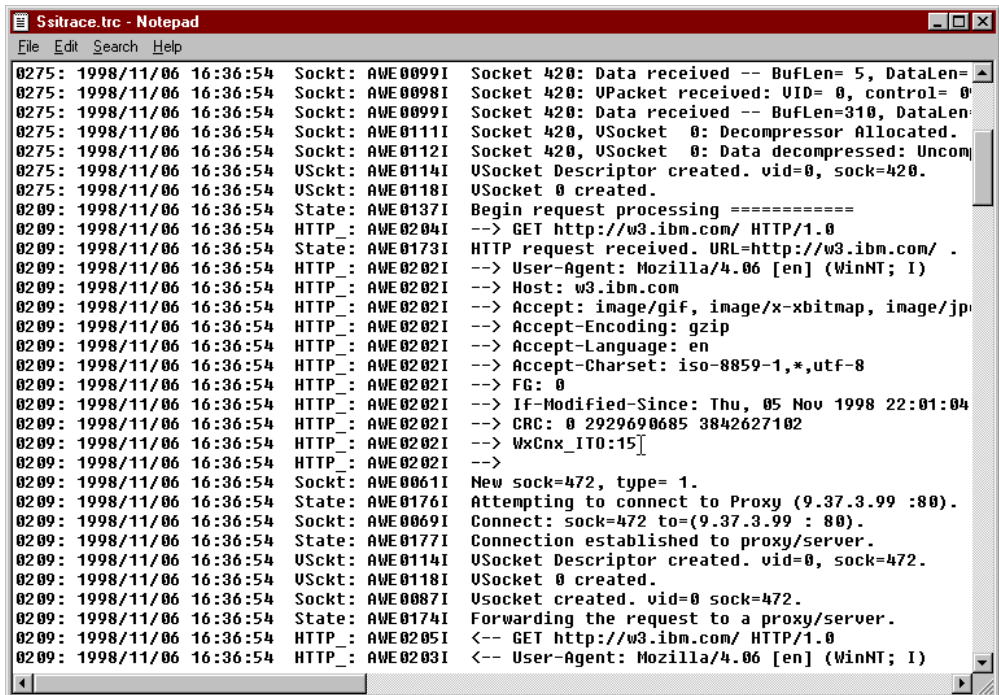


Figure 121. Web Express Server - Sample Trace

8.3.2.5 Options

These Web Express server configuration settings determine how much of your server machine's resources are used by Web Express. The maximum number of clients limits the number of clients that may connect to the Web Express server concurrently.

The maximum number of requests (threads) per client limits the number of concurrent requests the Web Express server accepts from each client.

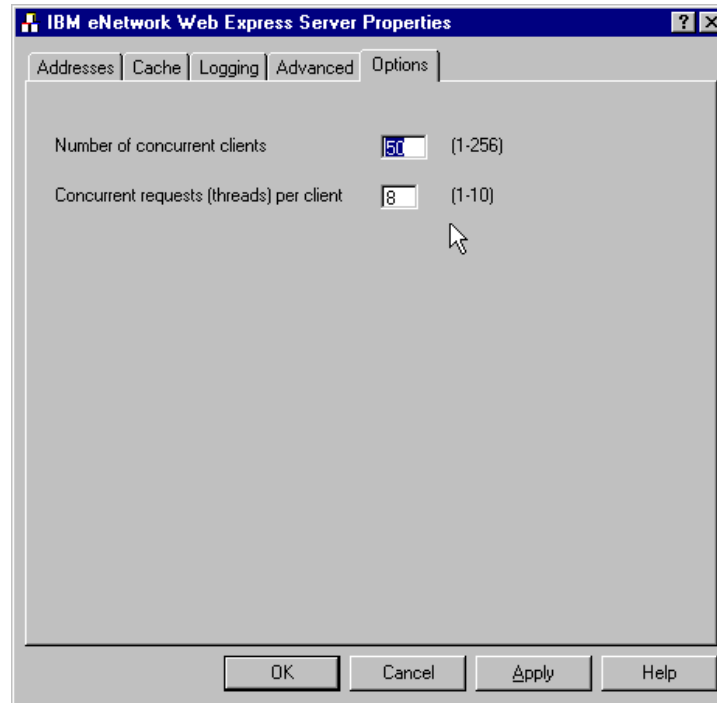


Figure 122. Web Express Server Properties - Options Configuration

The default value for the number of concurrent clients is 50 but it can be configured to a maximum number of 256 clients. The number of concurrent requests per client default value is 8 and it can be configured for a maximum of 10 threads per client as shown in Figure 122 on page 217.

Depending on the number of clients and the application traffic the Web Express server is handling, these values can be used to adjust and tune the performance of your Web Express server.

Increasing the number of concurrent clients and threads reduces serialization in the Web Express server. However, unless the server has enough resources, we do not recommend increasing these values to their maximum settings.

8.3.3 Web Express Server Configuration - AIX

In a similar way, Web Express server in AIX can be configured from smitty by selecting:

```
System Management->Communications Applications and Services and  
WebExpress->Configure WebExpress.
```

For example, a Web Express server for AIX can be configured as follows:

```

                                Configure WebExpress

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                [Entry Fields]
Server's IP address                    [9.67.131.119]
Server's IP port number                [8080]
Use HTTP Proxy                         ENABLED
- Proxy's IP address                   [9.37.3.99]
- Proxy's IP port number               [80]
- Proxy's address description          [Our Proxy Server]
- Alternate Proxy's IP address         []
- Alternate Proxy's IP port number     [80]
- Alternate Proxy's address description []
Cache directory                        [/var/webx]
Cache size                             [2500]

```

Server's IP address [9.67.131.119] means the host IP address where this Web Express resides. The server's IP port number [8080] is a unique port number in this server. This server port number will be used for the connection with the Web Express client. This is a default number.

Because the Web Express server will connect to an HTTP Proxy server, we enable the HTTP Proxy option. The default value is ENABLED.

The Proxy's IP address is the IP address of the HTTP Proxy server and it uses port number 80 for the connection with the Web Express server. In addition, any text can be entered as Proxy address description. You can also configure a backup or alternate Proxy server.

Cache directory is where the cached files will be stored and cache size is the maximum number of entries in the cache directory.

8.3.4 Web Express Client - Basic Configuration

The eNetwork Web Express Client runs on Windows 95, Windows 98 and Windows NT (workstation and server). It can be installed from CD-ROM or from diskettes.

To install the product, run "Setup" from diskette or the CD-ROM drive. You will then proceed to configure the connection to the Web Express server and the port number for the connection to the Web browser. See Figure 113 on page 207.

You will need to create a configuration profile to configure the Web Express client. You select "Create a New Profile", from the Web Express client folder, for the basic configuration and for further configuration, you select "Configure Profile" once the basic configuration has been entered.

8.3.4.1 Gathering Information

You are required to provide at least one configuration profile in order to start a Web Express session and when you create a new profile, you will need to provide the following information:

1. Connection characteristics. You provide information related to your network connection speed (slow, medium or high) and if you pay for your connection by the amount of data transferred when using this profile. These parameters

affect the behavior of the Web Express client (see “Advanced Configuration” on page 220).

2. Web Express server, HTTP Proxy server or no Proxy option. In this panel you configure which option you are using for this Web Express client. For example, it can communicate through a Web Express server, or an HTTP Proxy server, rather than communicating directly to the Web server.

Note

There are some limitations when the Web Express client is not connected to a Web Express server. For example, data compression and data reduction will not be available.

3. Web Express server or Proxy server addressing. If you selected the option to connect to a Web Express server or Proxy server, you will need to provide the IP address and port number for this connection. An alternate connection can also be configured.
4. Profile name and icon. Choose a profile name and an icon for this configuration.

8.3.4.2 Creating a Profile

When you create a profile the configuration wizard is invoked and you will enter the required parameters for the basic configuration. For more detailed information on the basic configuration parameters, see 8.3.5, “Advanced Configuration” on page 220.

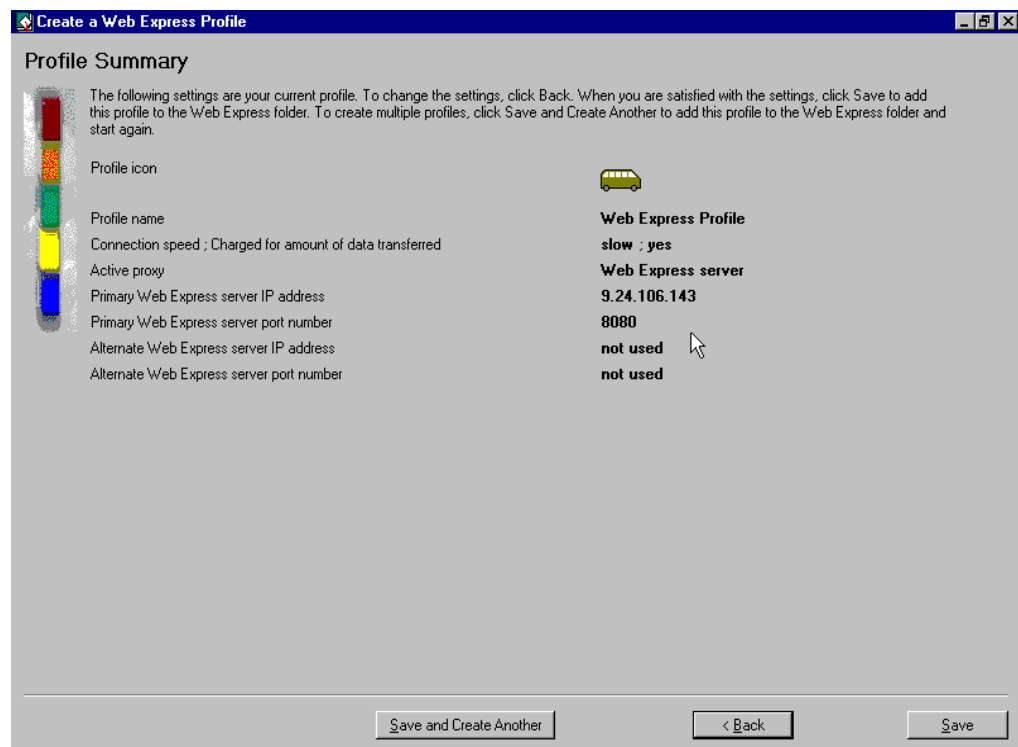


Figure 123. Web Express Client Configuration Profile - Summary

Figure 123 on page 219 illustrates a summary for the basic configuration options for our scenario. We have selected a slow speed network and we have also indicated that we are charged for the amount of data transferred. The Web Express client connects to a Web Express server (not to a Proxy server), so we provide the IP destination address (9.24.106.143) and port number (8080) for the connection to the Web Express server.

When you configure the profile, you have the option to change these parameters as well as provide more advanced configuration parameters that may affect the Web Express runtime process.

8.3.5 Advanced Configuration

Once you have created a configuration profile and provided the required parameters for your Web Express client configuration (see 8.3.4.1, “Gathering Information” on page 218), you can select the **Configure Profile** option from the Web Express client folder and change the basic parameters or reconfigure other advanced configuration defaults if needed. In this section, we provide a general overview of the configuration parameters you can add or change in the Web Express configuration profile.

8.3.5.1 Addresses

In this panel you configure or change the following options or parameters:

- Web Express client port. This is the port number for the IP connection between the Web Express client and the Web browser. In our scenario, we are using port number 2080 as seen in Figure 124 on page 221.
- Active Proxy. As indicated in 8.3.4.1, “Gathering Information” on page 218, the following options are available:
 - Web Express server. Indicates that you will connect to a Web Express server and all the optimization methods will be available. For example, caching, differencing, protocol reduction and header reduction. See 8.2.2, “eNetwork Web Express Optimization Methods” on page 208 for more details.
 - HTTP Proxy server. Indicates that a Web Express server is not used and the connection is to a Proxy server. Some optimization methods will not be available. See 8.3.4.1, “Gathering Information” on page 218 for details.
 - No Proxy. Indicates that neither, a Web Express server, nor a Proxy server will be used. In this case, the connection is directly to the Internet and some of the Web Express optimization methods will not be available. See 8.3.4.1, “Gathering Information” on page 218 for details.

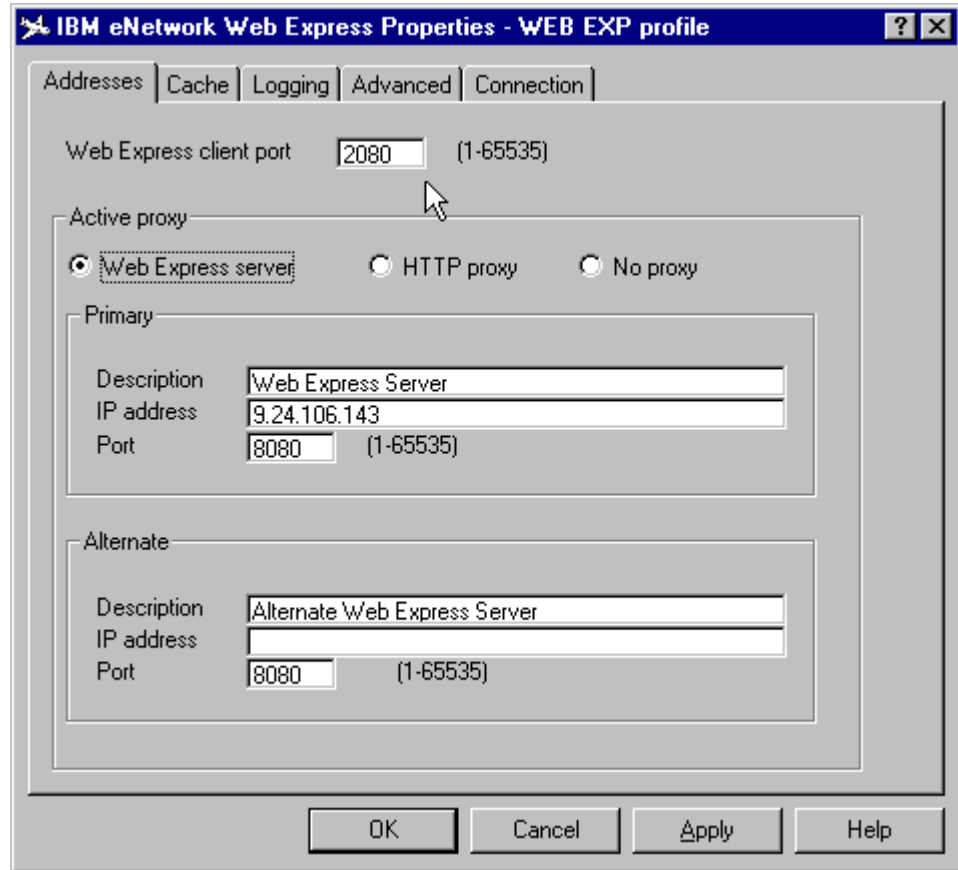


Figure 124. Web Express Client Properties - IP Addresses and Ports

Once the Active proxy option is selected, you will need to provide the IP address and port number for the either the Web Express server or the Proxy server. A backup or alternate server can also be configured. Figure 124 on page 221 illustrates the option for our scenario as stated in Figure 114 on page 211. That is, the Web Express client connects to a Web Express server taking advantage of all the provided optimization methods.

8.3.5.2 Cache Information

In this panel you configure the following parameters:

- Cache directory. The path for the cache directory. Figure 125 on page 222 shows the default value for this file.
- Maximum cache size. The maximum size for the cache directory. Default is 500 entries and up to 99999 entries can be configured. You will need to increase this number if you are running Web applications that use a large number of fields.
- Text entries refresh options. In this selection, you specify the option to never refresh the cache directory text entries, upon request refresh after a specified amount of time or always refresh. This option allows you to specify how often you want to update the text entries in the cache directory and therefore, adjust the frequency of update requests to the dynamics of your Web applications.
- Non-text entries refresh options. In this selection, you specify the option to never refresh the cache directory non-text entries, upon request refresh after a

specified amount of time or always refresh. This option allows you to specify how often you want to update the non-text entries in the cache directory and therefore, adjust the frequency of update requests to the dynamics of your Web applications.

Note

Notice that if you select the option to refresh after a specified amount of time or always refresh, the actual refresh does not take place unless there is a request for text or non-text entries.

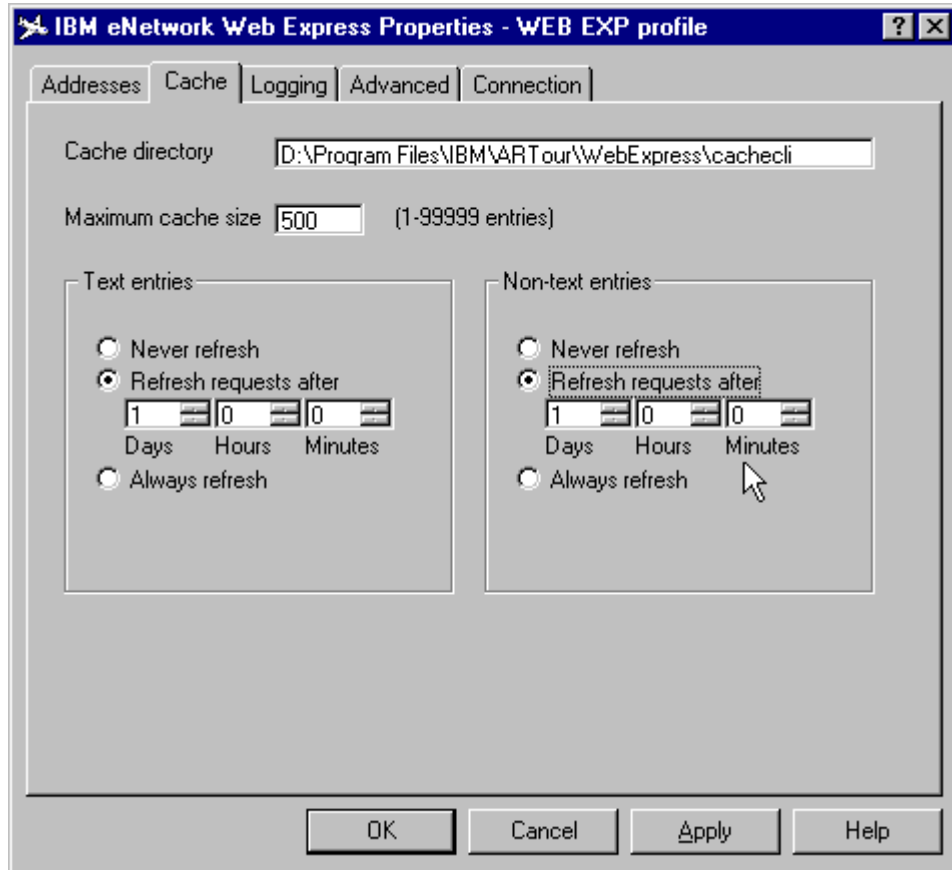


Figure 125. Web Express Client Properties - Cache Information

8.3.5.3 Logging

In this panel you can optionally configure the Web Express client logging facility configuration parameters. Select the option if you want no logging, error and warning logging, informational logging or detailed logging. A sample configuration panel is shown in Figure 126 on page 223. You can also specify the log file size (default value is 64 KB).

The name of the Web Express client log file is csilog.log. For a sample log file see Figure 136 on page 234.

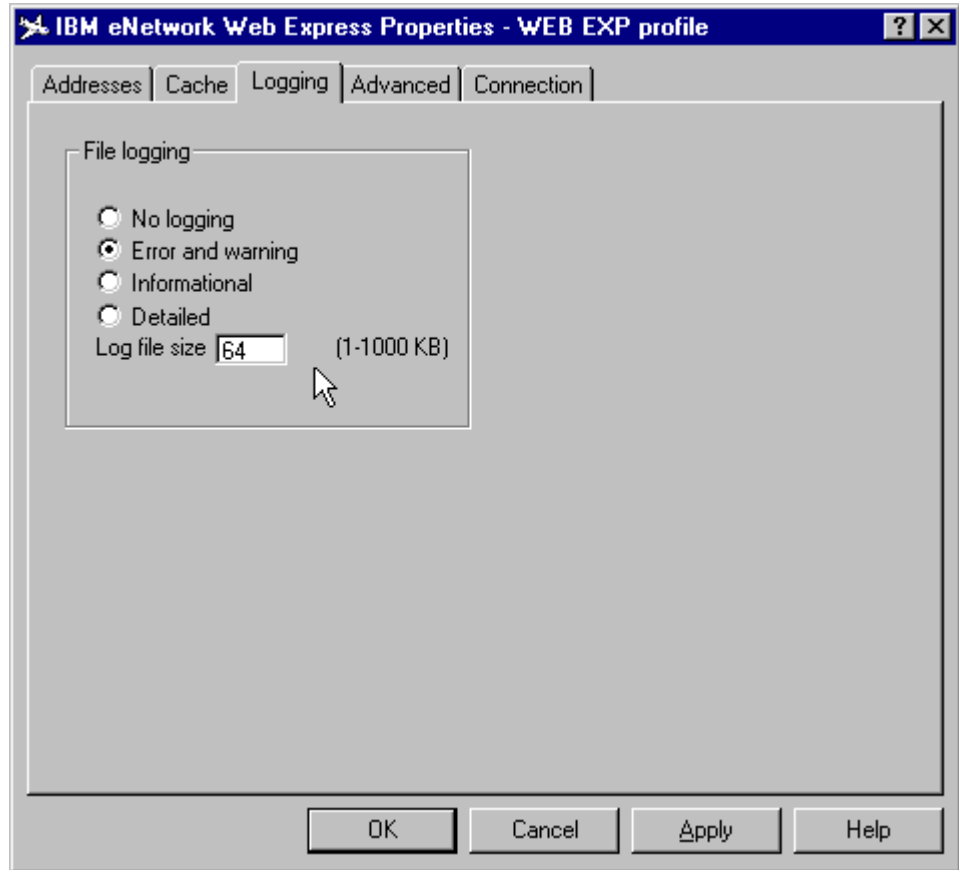


Figure 126. Web Express Client Properties - Logging Configuration

8.3.5.4 Advanced

In this panel you configure the following parameters if required:

- Concurrent browser connections. This is a performance option and specifies the maximum number of concurrent Web browser connections the Web Express client can handle. The maximum number is 10. Unless your workstation has enough resources, you should keep this value as low as possible.
- Trace options. In some circumstances when you are trying to troubleshoot a configuration problem or if you suspect there is a product defect, you will be required to run traces. Select the "Traces on" check box and the trace file size. The trace file size default is 1MB and you will need to increase this value when you run long traces; otherwise, the trace file will wrap around. For a sample trace file see Figure 139 on page 237. The name of the Web Express client trace file is csitrace.trc.

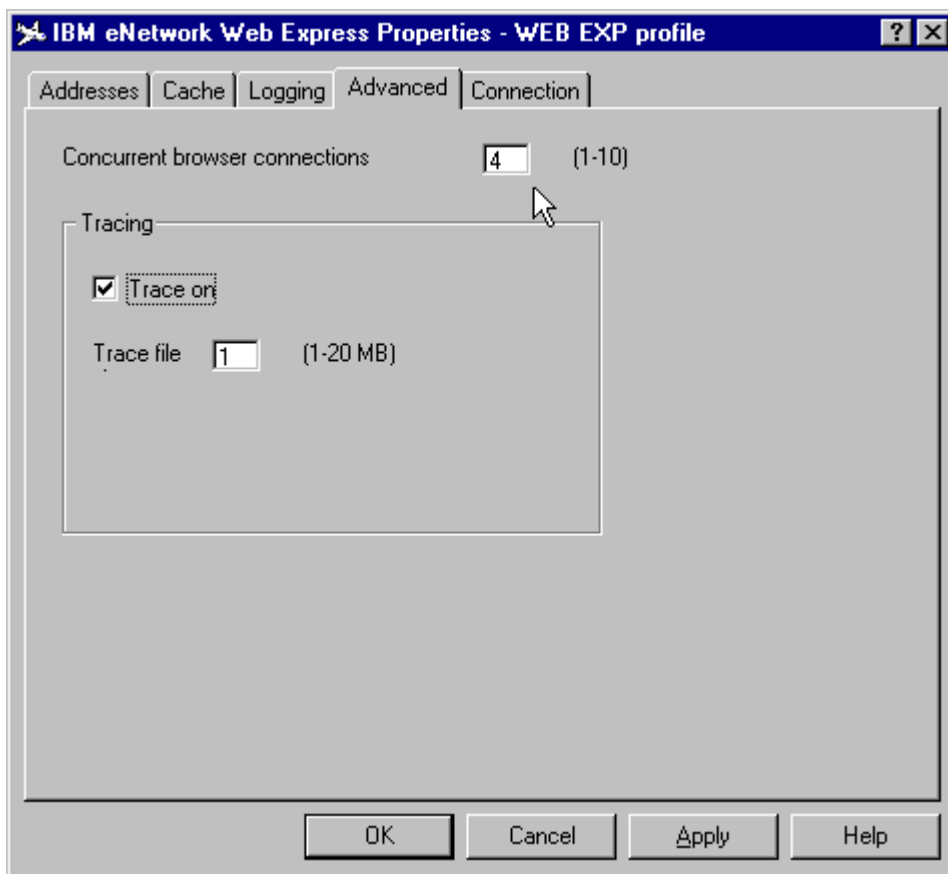


Figure 127. Web Express Client Properties - Advanced Configuration

8.3.5.5 Connection

In this panel you provide the Web Express connection characteristics. The following options can be configured:

- Data compression. It enables data compression for Web application traffic. In most cases, running multiple compression in your network is not so efficient for the performance of the Web application traffic. Therefore, you should only use this option when compression has not been turned on in other layers. For example, do not enable compression here if your wireless gateway is already doing it.
- Connection characteristics. These configuration options affect some of the initial default values in the profile for the Web Express client. The following options can be selected:
 1. Connection speed. The following speeds are available:
 - Slow. You will normally select a slow connection for wireless WANs, packet radio, and cellular phones.
 - Medium. Typical medium speed networks include CDPD, and dial networks such as PSTN, PCS, and GSM.
 - Fast. LAN networks are considered fast speed connections.
 2. Charge by the byte or packet option. Select this option if you are charged by the amount of traffic being transferred.

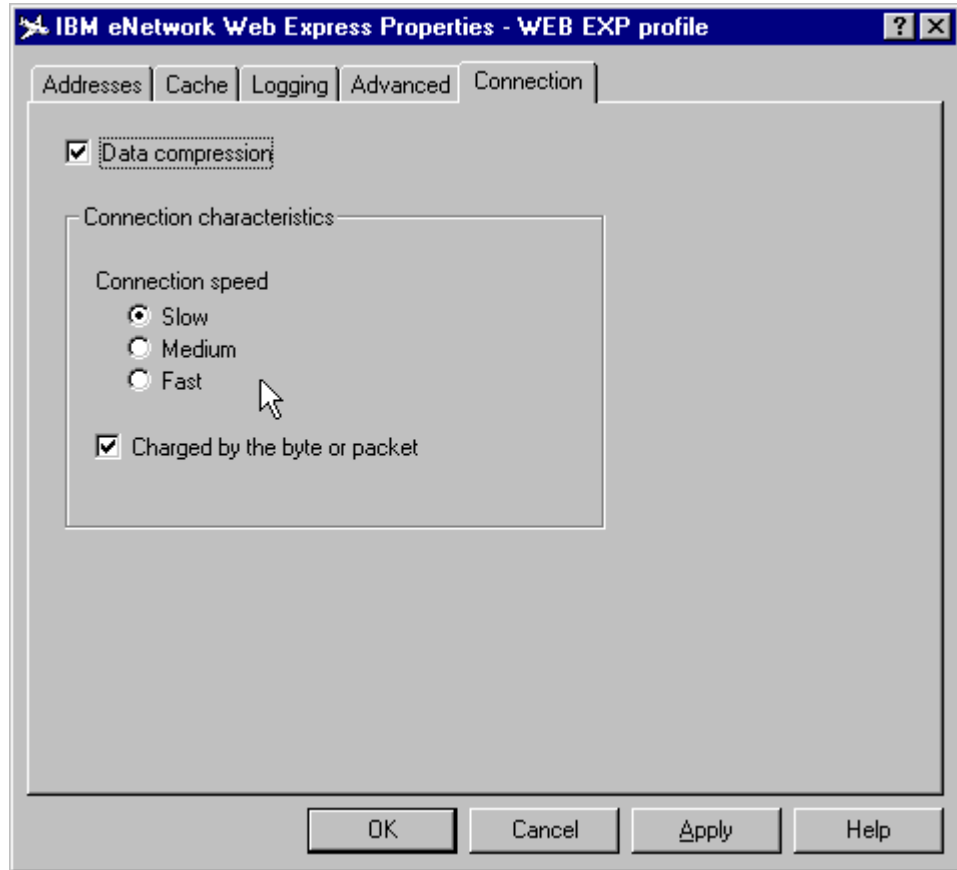


Figure 128. Web Express Client Properties - Connection Configuration

The connection options that you select will determine the initial default values for your Web Express client. However, you can always override these values by configuring the Properties of a profile after it is created. For example, see Figure 125 on page 222 where you can configure refresh intervals.

If you indicate that you are charged by the byte or packet, the initial default values shown in Table 8 on page 225 are selected.

Table 8. Charged by Amount of Data Transferred - Initial Default Values

Connection Speed	Slow	Medium	Fast
Refresh Interval ^a (text)	1 day	Always	Always
Refresh Interval ^a (non-text)	1 week	1 week	1 week
Download Images	Off	Off	Off
Number threads for background processing	2	4	6

a. Notice that the initial default values for the refresh interval (text and non-text entries) are only set when you create the configuration profile.

If you indicate that you are not charged by the byte or packet, the initial default values shown in Table 9 on page 226 are selected.

Table 9. Not Charged by Amount of Data Transferred - Initial Default Values

Connection Speed	Slow	Medium	Fast
Refresh Interval ^a (text)	1 day	Always	Always
Refresh Interval ^a (non-text)	1 week	1 day	Always
Download Images	Off	On	On
Number threads for background processing	2	4	6

a. Notice that the initial default values for the refresh interval (text and non-text entries) are only set when you create the configuration profile.

When downloading images is off, Web Express returns images, including graphics, multimedia clips, applets, and other embedded elements, from the cache to the browser. With downloading images off, Web Express will not transfer the images over the connection, even when the images in the cache are expired.

By default, most profiles prevent the downloading of images because these elements can be retrieved more quickly and less expensively from the cache. To make it probable that cached images are accurate and reliable, the value of downloading images and the value of the profile's non-text refresh interval are closely related. For profiles that are charged by the amount of data transferred, and which have slow speed connections, downloading images is less important since they may be too expensive and slow.

Note

By entering the proper connection speed, you select the number of threads used for multithreaded background downloads.

8.3.6 Web Browser Configuration

Since we have to access the Web-based application from the intranet or Internet, using a slow communication link such as wireless communication, the browser should connect to the Web Express client in the local machine. The Web Express client then connects to the Web Express server on the other end.

In general, there is no need for extra configuration in your Web browser as long as it runs in the same machine with the Web Express client. When the Web Express client is started, it will look for the default Web browser (for example, Netscape Navigator or Microsoft Internet Explorer) in your workstation and temporarily replace some of the Web browser configuration parameters in the registry. Specifically, it will include or replace the address and port number for the Web Express client acting as an HTTP proxy server as follows:

- HTTP Proxy server address: 127.0.0.1 (*localhost*)
- Port number: 2080

Note

For the Web browser, the Web Express client acts as an HTTP Proxy server.

When the Web Express client is terminated, it will then restore the Web browser configuration parameters in the registry. Therefore, based on this information, you should follow these rules:

1. Set your Web browser as the default browser in your system.
2. You should always start the Web Express client before the Web browser is started. This will allow the Web Express client to set the proper parameters in the Web browser configuration values in the registry.
3. You should always close the Web browser before the Web Express client is terminated. This will allow the Web Express client to restore the original Web browser configuration options in the registry.

If for any reason the Web Express client is terminated before the Web browser, you should be aware that some Web browsers may restore the configuration they have in memory. In this case, it will be the configuration values provided by the Web Express client in the registry. When this happens the Web Express client will try to restore the original Web browser configuration values.

In other words, when the Web Express client is called, it compares the value in the registry with its value (*localhost*). If they are same, the Web Express client assumes that it terminated before the Web browser and the browser erroneously restored the Web Express client values in the registry. For this reason, the Web Express client restores the original Web browser configuration values to allow the connection to the proper proxy server.

Note

For a clean shutdown, the Web browser should always be ended before the Web Express client.

8.4 Tivoli NetView Management

Tivoli NetView can be used to receive events (traps) generated by Web Express. In this section we show you how to install and configure the SNMP service in the Web Express server machine so that alerts can be sent to a Tivoli NetView console.

Note

It is not a requirement to install the Web Express management information base (MIB). However, it might be useful to load it in order to view the MIB structure when reading alerts.

8.4.1 SNMP Installation and Configuration - AIX

SNMP must be available in the AIX system to enable the SNMP trap function, so the TCP/IP SERVICES file must contain the following line:

snmp-trap 162/udp

This line may already exist in the file. Make sure that this line is not in the SERVICES file before adding it. To locate the SERVICES file, check your TCP/IP software documentation.

8.4.2 SNMP Installation and Configuration - Windows NT

If you want Web Express server to send events to a Tivoli NetView console in your network, you must install SNMP in the machine where Web Express server is running. In Windows NT, you select Network in the Control Panel to add the SNMP service if not already available. See Services tab in Figure 129 on page 228. If you need more details on how the SNMP service is installed and configured, see the proper documentation provided by Windows NT.

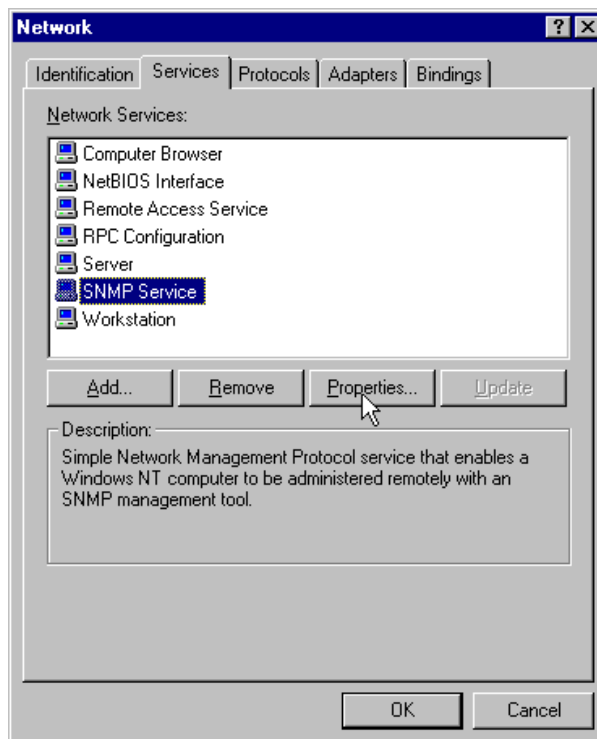


Figure 129. Windows NT - SNMP Service Installation

For a basic configuration, select Properties and enter the following parameters in the Traps tab as illustrated in Figure 130 on page 229:

- Add artour to the list of Community Names.
- Enter the IP address of the SNMP manager.

Note

If you uninstall the SNMP Service, the SNMP configuration for Web Express is also uninstalled.

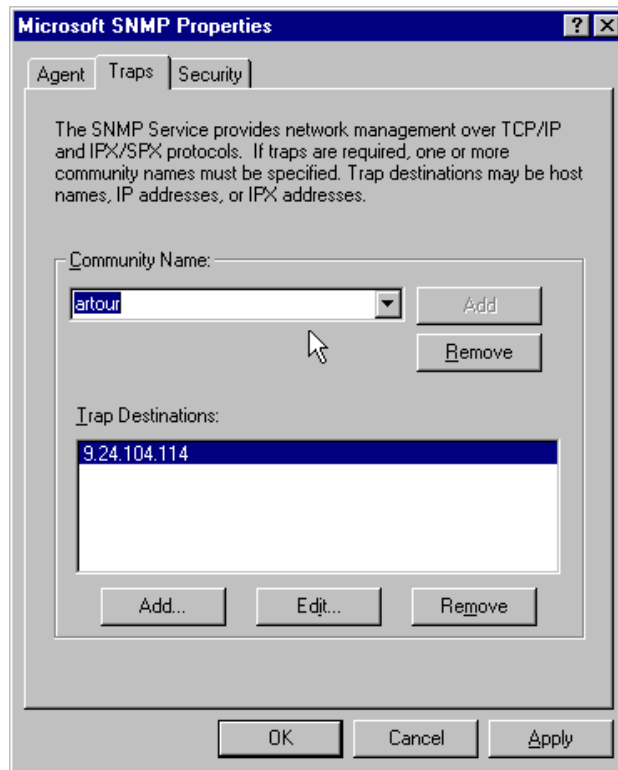


Figure 130. Windows NT SNMP Properties - Traps Configuration for Web Express

When the Web Express server is started you should see the message shown in Figure 131 on page 229. It indicates that an SNMP trap was sent to the configured Tivoli NetView console. Therefore, the Web Express server has established a successful connection with the SNMP service. IP address 9.24.104.114 is the address of the Tivoli NetView console.

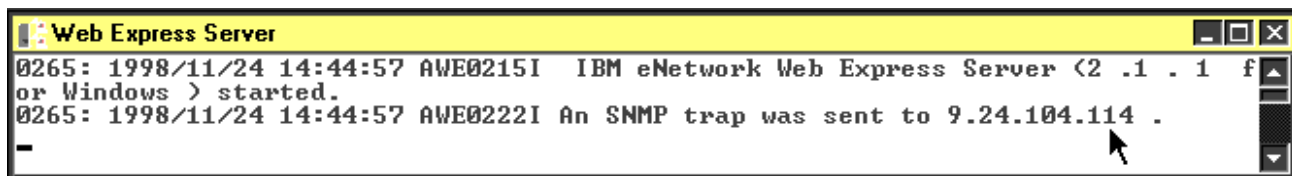


Figure 131. Web Express Initialization - SNMP Connection

8.4.2.1 Tivoli NetView Console - Event Browser

There are four situations that cause traps to be sent to the SNMP trap function:

1. The Web Express server started successfully (message AWE0215I). This alert is issued only after the configuration is loaded, resources needed for starting have been successfully accessed, and the server is waiting for a connection from the client.
2. The Web Express server startup failed. In this case, two alerts are sent. The first alert (message AWE0216E) which says Web Express Server startup failed, is paired with a second alert (message AWE0001E, AWE0059E, AWE0060E, AWE0223E, AWE0224E, AWE0226E, AWE0227E, or AWE0228E) that gives the reason for the failure.

3. The Web Express server ended (message AWE0210I). This alert is issued when the server ends normally.
4. The Web Express server ended abnormally. In this case two alerts are sent. The first alert (message AWE0217E) is paired with a second alert (message AWE0001E, AWE0015E, AWE0016E, AWE0108E, AWE0133E, AWE0168E, AWE0169E, AWE0181E, AWE0223E, AWE0224E, or AWE0236E) that gives the reason for termination.

A sample Tivoli NetView Event Browser screen is shown in Figure 132 on page 230. The entries (traps) from the Web Express server are for a node with computer name MUCHSIN.

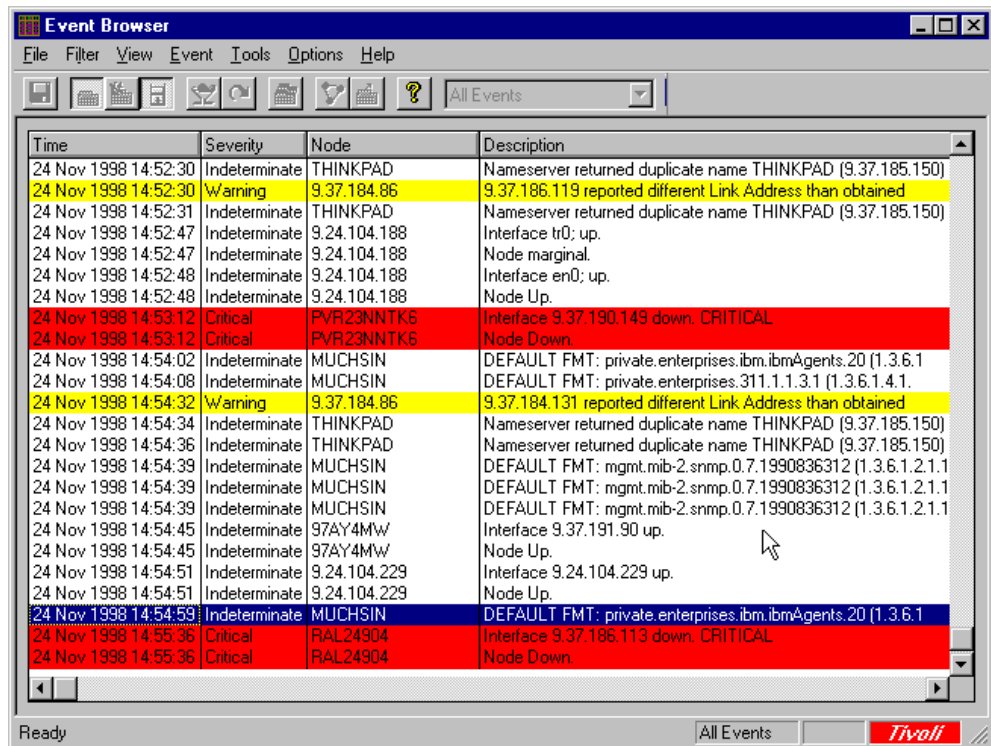


Figure 132. Tivoli NetView - Event Browser

For more information, you can also display the details of a specific entry as illustrated in Figure 133 on page 231.

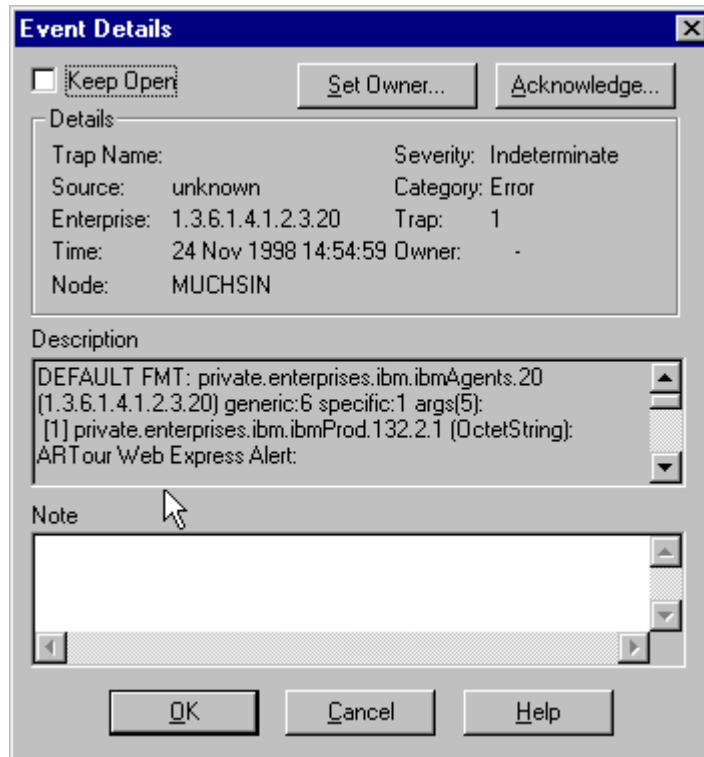


Figure 133. Tivoli NetView Event Browser - Web Express Event Details

8.5 Troubleshooting

In this section we show how you can troubleshoot configuration problems. It is always recommended that you review your configuration again and monitor the connections to make sure you are using the proper IP addresses, port numbers and other configuration parameters. However, if you do not know why you are not getting a Web Express connection, there are several things you can do to isolate the failure.

8.5.1 Monitoring Web Express

The first thing you should do if you are not getting a connection after reviewing your configuration is monitor the Web Express activity. Here we show where to look for information related to the Web Express connections. You can also monitor to verify your configuration options, IP addresses, ports and so on.

8.5.1.1 Web Express Client Problems

If the Web Express client could not connect to the Web Express server for whatever reason, a display similar to the one shown in Figure 134 on page 232 will be displayed on your Web browser screen.

In order to isolate the problem, we recommend you go through the following steps:

- Look at the activity display to see if your Web browser has connected to the Web Express client.

- In your Web browser issue the following command to see if there is a connection between the Web Express client and the Web Express server:
<http://artour.web.express/ssiping>
 This command is a quick variation of the IP ping program.

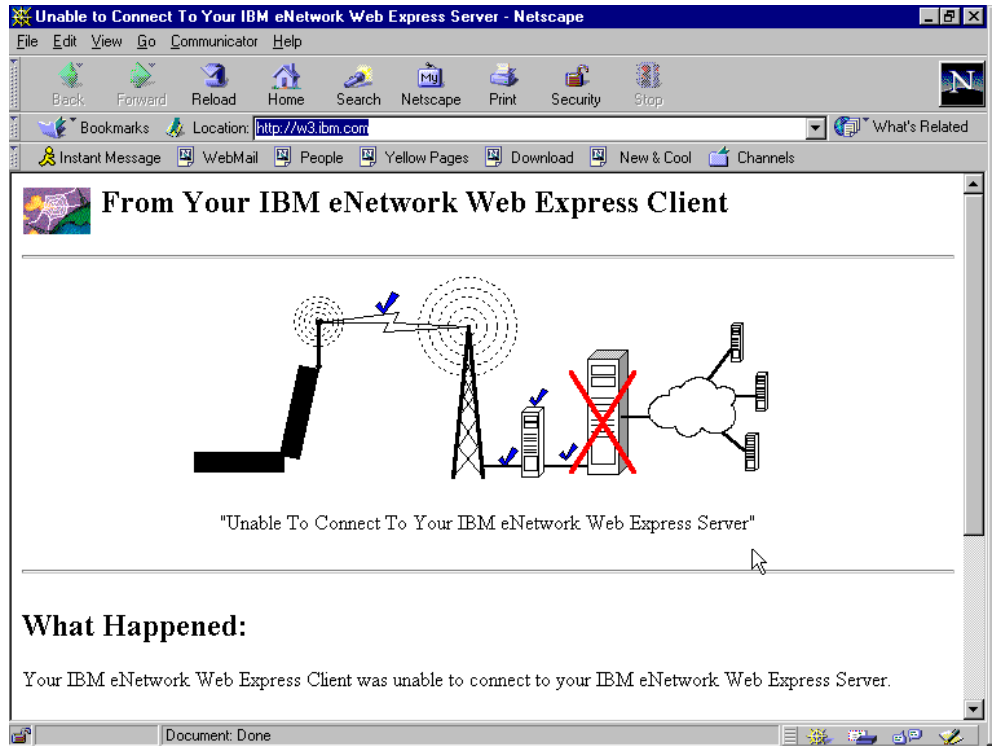


Figure 134. Web Express Client - Problems

For example, Figure 134 on page 232 indicates that the wireless or wireline connection was established but the Web Express client could not contact the Web Express server and you will take appropriate action as suggested in the display.

8.5.1.2 Monitoring Web Express Server

When you start Web Express server, it will display activity information based on your configuration options. Figure 135 on page 233 illustrates detailed information on the Web Express server console.

For information on how to configure the message types you want displayed, see Figure 119 on page 215.


```

Web Express Server
0233: 1998/11/05 16:59:14 AHED202I -->
0233: 1998/11/05 16:59:15 AHED180I Response received from proxy/server.
0233: 1998/11/05 16:59:17 AHED184I Returning response to IBM eNetwork Web Express Client.
0233: 1998/11/05 16:59:17 AHED207I <-- HTTP/1.0 200 OK
0233: 1998/11/05 16:59:17 AHED203I <-- Server: Domino-Go-Webserver/4.6.2.5
0233: 1998/11/05 16:59:17 AHED203I <-- Date: Thu, 05 Nov 1998 21:53:52 GMT
0233: 1998/11/05 16:59:17 AHED203I <-- Accept-Ranges: bytes
0233: 1998/11/05 16:59:17 AHED203I <-- Content-Type: text/html
0233: 1998/11/05 16:59:17 AHED203I <-- Last-Modified: Thu, 05 Nov 1998 21:53:52 GMT
0233: 1998/11/05 16:59:17 AHED203I <-- Via: HTTP/1.1 proxy.raleigh.ibm.com (IBM-HTE)
0233: 1998/11/05 16:59:17 AHED203I <-- CRC: 2929690685
0233: 1998/11/05 16:59:17 AHED203I <-- Content-Length: 18605
0233: 1998/11/05 16:59:17 AHED203I <--
0233: 1998/11/05 16:59:17 AHED207I <-- HTTP/1.0 200 OK
0233: 1998/11/05 16:59:17 AHED203I <-- Server: Domino-Go-Webserver/4.6.2.5
0233: 1998/11/05 16:59:17 AHED203I <-- Date: Thu, 05 Nov 1998 21:53:52 GMT
0233: 1998/11/05 16:59:17 AHED203I <-- Accept-Ranges: bytes
0233: 1998/11/05 16:59:17 AHED203I <-- Content-Type: text/html
0233: 1998/11/05 16:59:17 AHED203I <-- Last-Modified: Thu, 05 Nov 1998 21:53:52 GMT
0233: 1998/11/05 16:59:17 AHED203I <-- Via: HTTP/1.1 proxy.raleigh.ibm.com (IBM-HTE)
0233: 1998/11/05 16:59:17 AHED203I <-- CRC: 258090516
0233: 1998/11/05 16:59:17 AHED203I <-- Content-Length: 66
0233: 1998/11/05 16:59:17 AHED203I <--
0233: 1998/11/05 16:59:17 AHED170I Processing complete for URL=http://u3.ibm.com/ .

```

Figure 135. Web Express Server - Monitoring

8.5.2 Viewing the Log Files

Web Express implements a log facility that you can browse when required. You will find log files for both, the Web Express client and server. In this section we provide some information about how you can browse these files when looking for information about problems or simply when you just want to monitor the Web Express logged events.

8.5.2.1 Web Express Client - Log File

The Web Express client log file name is csilog.log. This file is dynamically updated when the Web Express client is running.

Note

Web Express client must be started before you start any communications with the Web browser clients.

Figure 136 on page 234 illustrates a portion of the log file. The file contains entries related to the Web Express client activity.

In this log file you will find informational messages as well as warning and error messages. For information on how to configure the message types you want logged, see Figure 126 on page 223.

```

Csilog - Notepad
File Edit Search Help
**000005246
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=896 errno=10038 ( Socket operation
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=896, errno=10038. Closed!
0749: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=1176 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=1176, errno=10038. Closed!
0738: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=1028 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=1028, errno=10038. Closed!
0509: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=1056 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=1056, errno=10038. Closed!
0495: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=1192 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=1192, errno=10038. Closed!
0749: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0738: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=984 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=984, errno=10038. Closed!
0509: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=1200 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=1200, errno=10038. Closed!
0495: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=1184 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=1184, errno=10038. Closed!
0749: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=1188 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=1188, errno=10038. Closed!
0738: 1998/11/06 10:27:06 AWE0018W Your IBM eNetwork Web Express Client did not retrieve URI
0711: 1998/11/06 10:27:06 AWE0076W SetErrNo: (recv ) sock=1196 errno=10038 ( Socket operati
0711: 1998/11/06 10:27:06 AWE0091W Bad receive on simplex socket=1196, errno=10038. Closed!

```

Figure 136. Web Express Client -Log File

8.5.2.2 Web Express Server - Log File

The Web Express server log file name is ssllog.log. This file is dynamically updated when the Web Express server is running.

```

Ssilog - Notepad
File Edit Search Help
**0000052295
0273: 1998/11/08 22:24:15 AWE0170I Processing complete for URL=http://207.82.250.251/null.h
0209: 1998/11/08 22:24:15 AWE0206I --> HTTP/1.0 200 OK
0209: 1998/11/08 22:24:15 AWE0202I --> Date: Mon, 09 Nov 1998 03:18:19 GMT
0209: 1998/11/08 22:24:15 AWE0202I --> Server: Apache/1.2.1
0209: 1998/11/08 22:24:16 AWE0202I --> Content-Type: text/html
0209: 1998/11/08 22:24:16 AWE0202I --> Via: HTTP/1.1 proxy.raleigh.ibm.com (IBM-WTE)
0209: 1998/11/08 22:24:16 AWE0202I -->
0209: 1998/11/08 22:24:16 AWE0180I Response received from proxy/server.
0209: 1998/11/08 22:24:16 AWE0184I Returning response to IBM eNetwork Web Express Client.
0209: 1998/11/08 22:24:16 AWE0207I <-- HTTP/1.0 200 OK
0209: 1998/11/08 22:24:16 AWE0203I <-- Date: Mon, 09 Nov 1998 03:18:19 GMT
0209: 1998/11/08 22:24:16 AWE0203I <-- Server: Apache/1.2.1
0209: 1998/11/08 22:24:16 AWE0203I <-- Content-Type: text/html
0209: 1998/11/08 22:24:16 AWE0203I <-- Via: HTTP/1.1 proxy.raleigh.ibm.com (IBM-WTE)
0209: 1998/11/08 22:24:16 AWE0203I <-- CRC: 4229528492
0209: 1998/11/08 22:24:16 AWE0203I <-- Content-Length: 8221
0209: 1998/11/08 22:24:16 AWE0203I <--
0209: 1998/11/08 22:24:16 AWE0170I Processing complete for URL=http://207.82.250.251/cgi-bin
0273: 1998/11/08 22:29:08 AWE0137I Begin request processing =====
0273: 1998/11/08 22:29:08 AWE0204I --> POST http://207.82.250.251/cgi-bin/premail/m_anzib/2
0273: 1998/11/08 22:29:08 AWE0202I --> Referer: http://207.82.250.251/cgi-bin/compose?disk=
0273: 1998/11/08 22:29:08 AWE0202I --> Host: 207.82.250.251
0273: 1998/11/08 22:29:08 AWE0202I --> Accept-Encoding: gzip
0273: 1998/11/08 22:29:08 AWE0202I --> Accept-Language: en
0273: 1998/11/08 22:29:08 AWE0202I --> Accept-Charset: iso-8859-1,*,utf-8
0273: 1998/11/08 22:29:08 AWE0202I --> Cookie: ID=95785c9a7475e5d0
0273: 1998/11/08 22:29:08 AWE0202I --> Content-type: application/x-www-form-urlencoded
0273: 1998/11/08 22:29:08 AWE0202I --> FG: 0
0273: 1998/11/08 22:29:08 AWE0202I --> CRC: 1440 * *
0273: 1998/11/08 22:29:08 AWE0202I --> WxCnx_IT0:15

```

Figure 137. Web Express Server - Log File

When troubleshooting for configuration problems, the Web Express server provides valuable information in the log file. In our scenario, the log file contains entries related to the connection activity. For example, it shows URL processing details and information about the connection with the HTTP Proxy server.

Note

Web Express server must be started before you attempt any connections with Web Express clients.

In this log file you will find informational messages as well as warning and error messages. For information on how to configure the message types you want to be logged, see Figure 119 on page 215.

You will find the following entry types in the log file:

1. Error and warning messages.
2. Informational. Requests and responses are logged.
3. Detailed entries, for example, progress messages and HTTP headers.

Also notice that the first column refers to the thread number sending the log message and it can be used to identify the log entries for a particular client or process. Log messages are displayed in national language.

You should also note that the eNetwork Web Express log files can be used for statistical analysis of traffic. For example, using spreadsheet tools.

8.5.3 Web Express Traces

A trace facility has been implemented in the Web Express client and server. In this section we provide a sample of the trace files.

Note

Running traces in Web Express will always create an extra overhead. You should only enable traces when specifically required.

8.5.3.1 Web Express Client - Trace File

If the Web Express client log file does not give you enough information to troubleshoot a potential problem, your last resort is to run traces. You will also be required to run traces if you think there is a potential product defect.

```

Csitrace.trc - Notepad
File Edit Search Help
0202: 1998/11/16 16:43:45 Sockt: AWE0061I New sock=348, type= 2.
0202: 1998/11/16 16:43:45 Sockt: AWE0068I Bind: sock=348, addr=(127.0.0.1 : 0).
0202: 1998/11/16 16:43:45 Sockt: AWE0061I New sock=352, type= 2.
0202: 1998/11/16 16:43:45 Sockt: AWE0069I Connect: sock=352 to=(127.0.0.1 :1076).
0200: 1998/11/16 16:43:45 Sockt: AWE0061I New sock=892, type= 1.
0200: 1998/11/16 16:43:45 USckt: AWE0114I USocket Descriptor created. vid=0, sock=892.
0200: 1998/11/16 16:43:45 USckt: AWE0118I USocket 0 created.
0202: 1998/11/16 16:43:45 Sockt: AWE0061I New sock=940, type= 1.
0202: 1998/11/16 16:43:45 Sockt: AWE0061I New sock=912, type= 1.
0202: 1998/11/16 16:43:45 Sockt: AWE0068I Bind: sock=912, addr=(0.0.0.0 :2080).
0202: 1998/11/16 16:43:45 Sockt: AWE0071I Listen: sock=912.
0202: 1998/11/16 16:43:45 State: AWE0229I IBM eNetwork Web Express Client (2 .1 . 1 for W
0204: 1998/11/16 16:43:45 Sockt: AWE0068I Bind: sock=940, addr=(0.0.0.0 :2622).
0204: 1998/11/16 16:43:45 Sockt: AWE0305I Applet command listening on port 2622.
0204: 1998/11/16 16:43:45 Sockt: AWE0071I Listen: sock=940.
0204: 1998/11/16 16:43:45 Sockt: AWE0061I New sock=936, type= 1.
0116: 1998/11/16 16:43:45 Sockt: AWE0061I New sock=960, type= 1.
0116: 1998/11/16 16:43:45 Sockt: AWE0068I Bind: sock=960, addr=(0.0.0.0 :2621).
0116: 1998/11/16 16:43:45 Sockt: AWE0304I Applet event channel listening on port 2621.
0116: 1998/11/16 16:43:45 Sockt: AWE0071I Listen: sock=960.
0202: 1998/11/16 16:44:01 Sockt: AWE0067I Accept: sock=912, new sock=984, peer=(127.0.0.1
0202: 1998/11/16 16:44:01 Sockt: AWE0064I Reference2 to sock=984 created.
0202: 1998/11/16 16:44:01 USckt: AWE0114I USocket Descriptor created. vid=0, sock=984.
0202: 1998/11/16 16:44:01 USckt: AWE0118I USocket 0 created.
0202: 1998/11/16 16:44:01 Sockt: AWE0087I USocket created. vid=0 sock=984.
0219: 1998/11/16 16:44:01 State: AWE0137I Begin request processing =====
0219: 1998/11/16 16:44:01 Sockt: AWE0124I USelect: wait on event.
0202: 1998/11/16 16:44:01 Sockt: AWE0099I Socket 984: Data received -- BufLen=2048, DataLe
0202: 1998/11/16 16:44:01 Sockt: AWE0099I Socket 984: Data received -- BufLen=2048, DataLe
0219: 1998/11/16 16:44:01 HTTP_: AWE0204I --> GET http://w3.ibm.com/ HTTP/1.0
0219: 1998/11/16 16:44:01 State: AWE0148I Processing HTTP request.

```

Figure 138. Web Express Client - Trace File

A sample of a Web Express client trace is shown in Figure 138 on page 236. It contains trace entries such as the product version number, IP addresses, ports and HTTP traffic. The name of the Web Express client trace file is csitrace.trc.

Trace file entries cannot be seen in a national language as they are only displayed in English.

8.5.3.2 Web Express Server - Trace File

In a similar way, the Web Express server trace facility can be invoked to trace the server activity. Traces are set in the Web Express server advanced configuration. For details on how you can set these traces, see Figure 120 on page 216.

```

Sstrace.trc - Notepad
File Edit Search Help
0183: 1998/11/16 16:42:02 Sockt: AWE0061I New sock=340, type= 2.
0183: 1998/11/16 16:42:02 Sockt: AWE0068I Bind: sock=340, addr=(127.0.0.1 : 0).
0183: 1998/11/16 16:42:02 Sockt: AWE0061I New sock=348, type= 2.
0183: 1998/11/16 16:42:02 Sockt: AWE0069I Connect: sock=348 to=(127.0.0.1 :1030).
0183: 1998/11/16 16:42:02 Sockt: AWE0061I New sock=464, type= 1.
0183: 1998/11/16 16:42:02 Sockt: AWE0068I Bind: sock=464, addr=(0.0.0.0 :8080).
0183: 1998/11/16 16:42:02 Sockt: AWE0071I Listen: sock=464.
0183: 1998/11/16 16:42:02 State: AWE0215I IBH eNetwork Web Express Server (2 .1 . 1 for W
0183: 1998/11/16 16:42:02 Error: AWE0221W SNMP agent service could not open the manager li
0183: 1998/11/16 16:42:32 Sockt: AWE0067I Accept: sock=464, new sock=504, peer=(9.24.106.1
0183: 1998/11/16 16:42:32 State: AWE0259I IP Address 9.24.106.144 connected at Mon Nov 16
0183: 1998/11/16 16:42:32 Sockt: AWE0064I Reference2 to sock=504 created.
0183: 1998/11/16 16:42:32 State: AWE0240I Sending capabilities: Version=3.
0183: 1998/11/16 16:42:32 Sockt: AWE0099I Socket 504: Data received -- BufLen= 5, DataLen=
0183: 1998/11/16 16:42:32 Sockt: AWE0098I Socket 504: UPacket received: UID=-1, control= 0
0183: 1998/11/16 16:42:32 Sockt: AWE0099I Socket 504: Data received -- BufLen= 6, DataLen=
0183: 1998/11/16 16:42:32 Sockt: AWE0103I Socket 504: Capability Packet received: Length =
0183: 1998/11/16 16:42:32 Sockt: AWE0104I Socket 504: VersionReleaseCode found at offset
0183: 1998/11/16 16:42:32 Sockt: AWE0105I Socket 504: CompressionLevel found at offset 3;
0183: 1998/11/16 16:42:32 Sockt: AWE0099I Socket 504: Data received -- BufLen= 5, DataLen=
0183: 1998/11/16 16:42:32 Sockt: AWE0098I Socket 504: UPacket received: UID= 0, control= 0
0183: 1998/11/16 16:42:32 Sockt: AWE0099I Socket 504: Data received -- BufLen=310, DataLen=
0183: 1998/11/16 16:42:32 Sockt: AWE0111I Socket 504, USocket 0: Decompressor Allocated.
0183: 1998/11/16 16:42:32 Sockt: AWE0112I Socket 504, USocket 0: Data decompressed: Uncomp
0183: 1998/11/16 16:42:32 USckt: AWE0114I USocket Descriptor created. vid=0, sock=504.
0183: 1998/11/16 16:42:32 USckt: AWE0118I USocket 0 created.
0151: 1998/11/16 16:42:32 State: AWE0137I Begin request processing =====
0151: 1998/11/16 16:42:32 HTTP_: AWE0204I --> GET http://w3.ibm.com/ HTTP/1.0
0151: 1998/11/16 16:42:32 State: AWE0173I HTTP request received. URL=http://w3.ibm.com/ .
0151: 1998/11/16 16:42:32 HTTP_: AWE0202I --> User-Agent: Mozilla/4.06 [en] (WinNT; I)
0151: 1998/11/16 16:42:32 HTTP_: AWE0202I --> Host: w3.ibm.com

```

Figure 139. Web Express Server - Trace File

The name of the trace file in the Web Express server is sstrace.trc. Figure 139 on page 237 illustrates a sample trace with entries related to the server activity. For example, request processing, sockets, product version number, IP addresses and so on.

Hint

Since the trace file wraps around, you may want to look for the "end of trace" entry in the trace file in order to locate the beginning of the trace records.

Trace file entries cannot be seen in a national language as they are only displayed in English.

Part 4. Appendixes

This part contains useful information you may require when deploying wireless networks using the eNetwork Wireless Gateway and Client, eNetwork Emulator Express and the eNetwork Web Express products. It includes information such as system requirements, documentation, URLs, and related publications.

Appendix A. System Requirements

This part gives the system requirements for eNetwork Wireless implementation. The system requirements are for the eNetwork Wireless Gateway and Client Hardware and software including Emulator Express, Web Express, emulation software and Web browser software.

Requirements Reminder

- The information below represents the minimum hardware requirements. Please make sure that you have enough capacity to run other applications.
- It is a good idea to follow the instructions in the READ.ME file, since it contains the latest information.

eNetwork Wireless Gateway

Hardware and software requirements:

- RS/6000, PowerPC, or SP2 systems.
- Additional hardware requirements vary according to the wireless network.
- AIX, Version 4.1.5, 4.2, or 4.3 . With AIX 4.3 use the C++ Library Version 3.0 shipped with the operating system.

eNetwork Wireless Client

Hardware requirements

- A 486 microprocessor with 16 MB of RAM
- A modem

Operating system requirements are one of the following:

- Operating System/2 Warp
- Windows 3.1, or higher, with a TCP/IP stack that supports an NDIS 2 driver
- Windows 95 or NT Client or Server Version 4.0 or higher

The operating system should have the following features:

- Microsoft Windows Version 3.1 (or later) and TCP/IP networking software that supports NDIS Version 2 device drivers.
- Microsoft Windows 95
 - You must have Microsoft TCP/IP networking support installed on your computer.
- Microsoft Windows NT Version 4.0 or later
 - You must have Microsoft TCP/IP networking support installed on your computer.
- OS/2 Warp version 3, Warp Connect or Warp Version 4
 - Internet Access Kit from the Warp Version 3 Bonus Pack, TCP/IP 2.1, TCP/IP 3.0 included in Warp Connect, or TCP/IP Version 5.1 included in Warp 4.

eNetwork Emulator Express

- eNetwork Emulator Express Server

Hardware and operating system requirements on RISC/6000 systems:

- RS/6000, PowerPC, or SP2 system with 64 MB of RAM, a 2 GB hard drive, and a LAN connection
- AIX, Version 4.1 or higher

Hardware and operating system requirements on Intel-based systems:

- Pentium 166 microprocessor, or equivalent, with 64 MB of RAM, a 2 GB hard drive, and a LAN connection
- Windows NT Server 4.1
- eNetwork Emulator Express Client

Hardware and operating system requirements on Intel-based systems:

- A 486 microprocessor with 16 MB of RAM and;
- A modem
- OS/2 Warp, Windows 95 or NT 4.0 or higher
- Telnet 5250 or 3270 software such as IBM Personal Communication Software

eNetwork Web Express

- eNetwork Web Express Server

Hardware and operating system requirements on RISC/6000 systems:

- RS/6000, PowerPC, or SP2 system with 64 MB of RAM, a 2 GB hard drive, and a LAN connection
- AIX, Version 4.1 or higher

Hardware and operating system requirements on Intel-based systems:

- Pentium 166 microprocessor, or equivalent, with 64 MB of RAM, a 2 GB hard drive, and a LAN connection
- Windows NT Server 4.1
- eNetwork Web Express Client

Hardware and operating system requirements on Intel-based systems:

- A 486 microprocessor with 16 MB of RAM
- A modem
- Windows 95

One of the following browsers:

- Netscape Navigator with JVM 1.02, or higher
- Internet Explorer with JVM 1.02, or higher

Product Support

The eNetwork products described herein are fully supported in all countries in which they are available in accordance with local IBM support procedures.

Appendix B. Special Notices

This publication is intended to help network specialists and administrators to install, configure and monitor nodes running IBM eNetwork Wireless Gateway and Client, IBM eNetwork Emulator Express and IBM eNetwork Web Express products. The information in this publication is not intended as the specification of any programming interfaces that are provided by these products. See the PUBLICATIONS section of the IBM Programming Announcement for IBM eNetwork Wireless Gateway for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering 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 the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

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

AIX	APPN
AS/400	AT
BookManager	CT
eNetwork	IBM
Language Environment	NetView
Operating System/2	OS/2
OS/400	RS/6000
SP	SP2
ThinkPad	VTAM
XT	400

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

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

Other company, product, and service names may be trademarks or service marks of others.

Appendix C. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How to Get ITSO Redbooks" on page 247.

- *An Introduction to Wireless Technology*, SG24-4465-01
- *IBM eNetwork Communications Server For Windows NT, Version 6.0 Enhancements*, SG24-5232

C.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

C.3 Other Publications

These publications are also relevant as further information sources:

For the eNetwork Wireless Software the following product documentation is available:

- *eNetwork Wireless Technical Overview*, GC31-8630
- *eNetwork Wireless Gateway and Client V4R1 Administrator's Guide*, GC31-8633
- *ARTour Emulator Express Server and Client Administrator's Guide*, GC31-8636
- *eNetwork Web Express Version 2 Release 1 Administrator's Guide*, GC31-8634

Further information can be found under the following URL which internally is available to all IBM employees: <http://wireless.raleigh.ibm.com>

The external link to eNetwork Wireless Software is:
<http://www.ibm.com/software/enetwork/mobile/>

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** <http://www.redbooks.ibm.com/>

Search for, view, download or order hardcopy/CD-ROM redbooks from the redbooks web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this redbooks site.

Redpieces are redbooks in progress; not all redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

Send orders via e-mail including information from the redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the "How to Order" section at this site: http://www.elink.ibm.link.ibm.com/pbl/pbl/

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the "How to Order" section at this site: http://www.elink.ibm.link.ibm.com/pbl/pbl/

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the "How to Order" section at this site: http://www.elink.ibm.link.ibm.com/pbl/pbl/

This information was current at the time of publication, but is continually subject to change. The latest information for customer may be found at <http://www.redbooks.ibm.com/> and for IBM employees at <http://w3.itso.ibm.com/>.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and redbooks by accessing the IBM Intranet Web site at <http://w3.itso.ibm.com/> and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may also view redbook, residency, and workshop announcements at <http://inews.ibm.com/>.

Index

Symbols

/etc/ARTour.route 75
/etc/emexpsrv.cfg 182
/portmap 71
/usr/lpp/emexpress 178
/usr/OV/bitmaps/C 74
/usr/OV/fields/C 74
/usr/OV/registration/C 74
/usr/OV/symbols/C 74
/var Directory 59
/var/emexpress 185

Numerics

2PKDP 165
3270 and 5250 applications 174
3270/5250 sessions 5
3270/5250 terminal emulator 173
3-tier model 12

A

Accessing the Wireless Network 143
ACCOUNT LOCKED 90
Activating
 a Modem through the Network Provider 110
Active Proxy 220
Add a Mobile Client Connection. 91
Add a Mobile Client Panel 91
Add a Mobile Network Interface 78
Add a PSTN Connection 93
Add an X.25 Device Driver for Each X.25 Adapter Card.
62
Adding
 Profile 130
Adding a PSTN Modem Type 69
Addresses 213, 220
Advanced 223
Advanced Configuration 190, 215
Advanced Mobile Telephone System (AMPS) 34
Agent 12
AIX 7
AIX configuration database 45
AIX operating system 164
AIX V4.1 54
AIX workstation 167
AIXLink 1.1.3.0 55
AIXlink/X.25
 Application Development Toolkit - COMIO Support 55
 COMIO Compatibility Support & Applications 55
 NPI 55
 Runtime Environment 55
 Server Support 55
Alcatel 35
All Connections 105
ALP 48
American Mobile ARDIS 163
Amount of Data Transferred 225, 226

AMPS cellular service 31
ampx0 62
ampx1 62
An Overview of the eNetwork Wireless Software 3
Analog Cellular Phone Systems (AMPS) 34
Analog or digital telephone networks 21
Analog PSTN Systems 33
application specific terminal 12
APPN 199
ARDIS 22
ARDIS Connection 80
ARDIS Gateway 92
Ardis Maximum Transmission Unit 162
artgw 72
artgw.msg.En_US 72
artgw.msg.en_US 72
artnwm 72
ARTour Link Protocol 48
ARTour Link Protocol (ALP) 46
ARTour Version 2.X 75
artour_devinfo 73
artour_devsearch 73
ARTouracct 154
artourmgr 73
artourmgr.fields 74
artourmgr.reg 74
artourmgr.symbols 74
AS/400 6
AS/400 host system 192
ASCII-console 45
Asynchronous I/O Processing Parameters 66
authentication 47
Authentication required flag 103
authorization 47
autobauding 37
Automatic Layout 100
Autostart Applications 128
Available Space in the /var Directory 59

B

background knowledge 4
bandwidth 10
Base Operating System, level 4.1.4.0 54
base station 19
Base station Data Link Controller (BDLC) 40
basic components of wireless data communication 19
Basic Configuration 178
basic rate interfaces (BRI) 40
Battery Information 136
Bell Laboratories 34
BellSouth Wireless Data 163
Benchmarking Application 156
bisynchronous 3270 23
Bisynchronous point-to-pont 23
bitmaps/* 74
bos.net.tcp.client 55
bos.net.tcp.server 55

brick 27
Broadcast Messages 52

C

C
Program FilesIBMeNetwork Emulator Express Client.
190
Program FilesIBMeNetwork Emulator Express Serv-
er. 181
CAC 181
CACH 184
Cache 181, 184
Cache Configuration 214
Cache director 221
cache file 182
Cache Information 221
cachesize 512 183
Caching 208
CardPhones 36
Category of Problem 141
CDMF 48
CDPD 7
CDPD Connection 87
CDPD modems 32
CDPD Protocol Architecture 32
CDPD Wireless Network Controllers 32
Cellular Digital Packet Data (CDPD) 31
Cellular radio network 19
CGI 7
Change / Show Security Defaults 90
Changing Device Labels 106
chdev 76, 77
Check Connection 105
Check Connection->Ping. 105
chfs 59
CID 28
Client Configuration 189
Client Toolbar 136
CLNT 181, 184
CNFG 181, 184
COM port 27
COMMON-ISDN-API (CAPI) 40
communication delays 10
Communication Problem overview 141
Communications Server 192
Communications Server Tel net Sessions 198
COMP 184
Compression 181
compression 48, 162
Compression/Decompression 184
Concurrent browser connections 223
Configure 181, 184
Configure Profile 220
Configuring 75
eNetwork Wireless Client for CDPD Network 125
eNetwork Wireless Client for IBM ARDIS Modem 122
eNetwork Wireless Client for Mobitex Network 124
eNetwork Wireless Gateway and Client Network Man-
agement 98
eNetwork Wireless Gateway with ARDIS Connection

80
eNetwork Wireless Gateway with CDPD Connection
87
eNetwork Wireless Gateway with Mobitex Connection
82
Telnet Emulator to Use Emulator Express 191
Confirmed 51
Connect status 104
CONNECTED 17
Connecting to Analog Wireline Networks 38
Connecting to Digital Wireline Networks (ISDN) 39
Connection 224
Connection characteristics 224
connection oriented 21
Connection speed 224
Connections over PSTN networks 33
Connections via X.25 41
Contained Devices 105
Controller 181, 184
costs per byte transmitted 10
Country Code 83
Create Segment 106
Creating a New Profile 218
Creating an Icon to start connection 127
Creating eNetwork Wireless Mobile Network Interface 77
CTRL 181, 184
Current STATE 95, 97

D

data circuit asynchronous 37
Data compression 224
Data Reduction Process 175
Data Transmission Techniques 46
DataCard 36
Dataradio 40
Dataradio Multiplex Protocol (DMP) 41
DATARADIO network 54
DataTAC 4, 21, 23
DataTAC (ARDIS) modem 27
DataTAC 4000 22
DataTAC 5000 22
DataTAC 6000 22
DataTAC ARDIS Network Problem 147
DataTAC Network Architecture 23
DataTAC networks over TCP 168
DataTAC Transmission Parameters for Motorola PMR 51
DataTAC(ARDIS) 27
DCS1800 35
DCS1900 35
Defining X.25 Reset Delay Timer Interval 76
Delete Segment 106
Deleting existing Profile 131
Deleting or Revising
existing Wireless Client Profile 130
DES 48
Determining the Disk Space Needed 58
Determining the Virtual Storage Needed 58
Device Info 103
Device Information 102
Device Label 106

df /var 59
DHCP 195
dial-up access 7
Differencing 208
Digital Communications System 1800 Standard (DCS1800) 35
digital user channels 39
Disconnect Information 136
DISCONNECTED 17
Disk Space 58
Displaying the ARTour Log 146
DLUR PU 199
dotted decimal notation 26
dual homed IP 167

E

EBCDIC 176
EC 34
echo \$LANG 57
echo nodes 144
Edit->Modify/Describe->Object. 106
Edit->Modify/Describe->Submap 106
Edit->Modify/Describe->Symbol. 106
EID 21
Electronic ID 21
Electronic Serial Number (ESN) 21
emexpcl.trc 190
emexpcl2.trc 190
emexpress 178
emexpsr2.trc 181
Emulation Express
 Client Configuration for Windows 95/NT 189
Emulator Express 6
 Client Configuration for Windows 95/NT 189
 Client for Windows 95/NT Configuration 189
 Client Installation 188
 Client Sessions 197
 Log File - Client 200
 Log File - Server 201
 Server - Log File 201
 Server for AIX Configuration 182
 Server for Windows NT Configuration 178
 Server Installation 176
 Server Sessions 197
 Servers and Clients 174
 Trace File - Client 202
 Trace File - Server 203
Emulator Express Client Sessions 197
Emulator Express Log File - Client 200
Emulator Express Log File - Server 201
Emulator Express Server 6
Emulator Express Trace File - Client 202
encapsulation 46
encrypt 166
encryption 46, 47, 167
eNetwork Emulator Express 3, 5, 173
 3270 File Transfer 176
 Architecture 174
 Caching 175
 Components 174

Data Compression 175
Data Reduction Process 175
Protocol Reduction 175
Server Configuration 178
eNetwork Emulator Express Configuration 6
eNetwork Gateway Application Down 149
eNetwork Personal Communicaton 5, 9
eNetwork Web Express 3, 6, 7, 205
eNetwork Wireless
 Components 142
 Gateway action 148
eNetwork wireless
 Client action 147
eNetwork Wireless Client statistics 156
eNetwork Wireless Clients 4
eNetwork Wireless Gateway and Client 4
eNetwork Wireless Gateway and Client Configuration 5
eNetwork Wireless Gateway and Client Network Management 97
eNetwork Wireless Gateway Architecture 45
eNetwork Wireless Gateway Inside a Firewall 167
eNetwork Wireless Gateway Outside a Firewall 169
eNetwork Wireless Gateway Product Files 72
eNetwork Wireless Gateway Software Architecture 45
eNetwork Wireless Interface 160
eNetwork Wireless Layer 45
eNetwork Wireless layer 9
eNetwork Wireless Scales 162
eNetwork Wireless Software 3
eNetwork Wireless Software components 3
Ericsson 35
Ericsson Mobile Communications AB 29
Error Message 147
Error Messages on the eNetwork Wireless Client 149
ESD 32
ESN 21
ETC 34
Ethernet 70
Ethernet card 21
ETHERNET LAN 28
ETSI GSM 07.05 37
ETSI GSM 07.07 37
European Telecommunications Standards Institute (ETSI) 35
Express family 10
Extended Addressing 26
Extended Addressing Scheme 25

F

filepath 185
FILT 181, 184
Filter 181, 184
filtering all traffic 169
firewall 166
Fixed Routing 24
Fleet Connectivity 24
For This Submap 100
full screen-oriented 6

G

- Gateway Connected to the Internet 166
- Gateway information panel 138
- Gateway locks the user 152
- General 181, 184
- General Configuration 98
- General Packet Radio Service (GPRS) 35
- German Modacom 24
- GIF 7
- global connection parameters 80
- Global System for Mobile Communication (GSM) 35
- graphical user interface 5
- Grouping Mobile Devices 106
- GSM 35
- GSM subscription 36
- GSM via GSM-ISDN 38

H

- handoff 20
- Hardware Requirement 54
- Header reduction 208
- higher latency 10
- HOD 5
- homing network provider 20
- Host On-Demand 5
- Host On-Demand (HOD) 176
- hosting network provider 20
- HTML 7
- http
 - //wireless.raleigh.ibm.com 245
 - //www.capi.org/ 40
 - //www.gsmdata.com 35
 - //www.software.ibm.com/enetwork/mobile/ 246
- HTTP protocols 7
- HTTP Proxy server 218, 220
- HTTP proxy server 7, 8

I

- IBM eNetwork Wireless Gateway Requirement 53
- IBM mainframe 6
- Icon to start connection 127
- Identifying Mobile Devices and Subscribers 36
- idle time 182
- idletime 25 183
- IEEE 802.3 70
- if_MNU_drive.Snd.GSM.tty0 96
- if_MNU-drive 96
- if_MNU-drive.Acct 96
- if_MNU-drive.BcMc 96
- if_MNU-drive.CfgMgr 96
- if_MNU-drive.ChPw 96
- if_MNU-drive.Log 96
- if_MNU-drive.Rcv.IO 96
- if_MNU-drive.SmuxD 96
- if_MNU-drive.Trace 96
- in coverage 20
- IND\$FILE protocol 176
- independent signalling channel 39
- inside the firewall 167

Installing

- Emulator Express Client for Windows 95/NT 188
- Emulator Express Server for AIX 177
- Emulator Express Server for Windows NT 176
- Installing and Configuring Serial Line Support 65
- Installing and Removing eNetwork Wireless Gateway Product Files 72
- Installing eNetwork Wireless Gateway Product Files. 72
- Installing/Uninstalling and Configuring
 - Wireless Client on OS/2 116
- Integrated Services Digital Network 39
- interconnection 8
- Interface to AIX TCP/IP 45
- Internet Protocol (IP) 173
- Internet Service Provider (ISP) 167
- interval_value 77
- Introduction to Wireless Technology 19
- IP Addressing in the eNetwork Wireless Gateway and Client 46
- IP Addressing with eNetwork Wireless 46
- IP Packet Filtering and Mapping 50
- IP protocols 5
- IP stack 162
- IP transit traffic 167
- ISDN Basic Access 40
- ISDN Standard 39

J

- Java based 5

L

- LAN 11
- Language Environment 57
- listen 182
- Listing All Mobile Devices in a Structure 105
- local 10
- Local Command Mode 27
- Local MAN 93
- local PSTN address 87
- Locating Devices and Connections 104
- Log Level 99
- Logging 200, 222
- Logging Configuration 215
- Logical Link Identifier (LLI) 25
- lsattr 76
- lsps -a 58
- Lucent 35

M

- MASC 31
- MASC frames 31
- MASC protocol 31
- Maximum cache size 221
- Maximum IP Packet Size 162
- maximum number of emulator sessions 182
- Maximum Transmission Unit (MTU) 159
- maxsessions 185
- MCA-bus 54

- Measuring Performance 153
- message oriented wireless network 23
- Message Switch 23
- Messaging 24
- MHX 31
- Microsoft Network Explorer 9
- mn0 46
- mni 77
- MNP-10 34
- MOBILE 17
- Mobile
 - User Reports Problem 145
- Mobile Client 12
- Mobile Client Configuration 90
- Mobile Client Status 152
- Mobile Clients 46
- Mobile Devices 46
- Mobile Network Connections layer 45
- Mobile Network Interface 46
- Mobile Subnet 46
- mobile switching centers 20
- Mobile Versus Wireless 17
- Mobitex 4, 29
- Mobitex Access Number (MAN) 30
- Mobitex architecture 29
- Mobitex Connection 82
- Mobitex gateway 93
- Mobitex MOX 30
- Mobitex Network Architecture 29
- Mobitex X.25 Adapter interface. 83
- Modem Identifier 146
- Modem Information 137
- Modem Pools in Analog Cellular Networks 34
- Modem Pools in Digital Cellular Networks 38
- Monitoring 196
- Monitoring the eNetwork Wireless Gateway and Client Network 100
- Monitoring the Progress from Client Toolbar 136
- Monitoring Web Express 231
- Monitoring Web Express Server 232
- Motorola 21, 35
- Motorola InfoTAC 27
- Motorola PMR 54
- Motorola Private Mobile Radio (PMR) 27
- Motorola Private Mobile Radio Architecture 28
- Motorola RNC3000 controller 27
- Motorola VRM 600 27
- MOX over X.25 links 30
- MPAKs 31
- MSC 20
- MTU sizes 153
- Multi Site Controller (MSC) 41
- multi-site controller (MSC) 54

N

- narrowband wireless links 10
- Native Command Language (NCL) 27
- Native Mode 27
- NCL interface 31
- Negative Entitlement 26

- Netscape 9
- Netscape Navigator 227
- NetView/6000 45
- Network Management Console 72
- network management station (NMS) 72
- Network nodes 98
- New Object Holding Area 100
- No Proxy 220
- Nokia 35
- Non-text 221
- non-transparent mode 37
- Nortel, 35
- notebook 174
- number of minutes 182
- nv6000 99

O

- ODM 45
- ODM database 75
- Off for This Submap. 100
- Online Mode 27
- Optimization Techniques 48
- optimizes IP communication 11
- Optimizing IP MTU Sizes 159
- Options 99
- OS/2 4, 128
- other private 64
- other public 64
- outside the firewall 167

P

- packet filtering 50
- Packet Mapping 51
- packet oriented 21
- PAD (Packet Assembly/Disassembly unit) 42
- Password 103
- Password expired flag 103
- PBX 33
- PC card 21
- PCMCIA 21
- PCOMM 5, 9, 176, 195
 - Telnet 3270 Configuration 195
 - Telnet Client Configuration - Target IP Address 196
- PCOMM Telnet 3270 192
- PCOMM Telnet 5250 192
- peer-to-peer connection 11
- Pentium Processor 36
- performance 153
- Permanent Virtual Circuits (PVC) 42
- Personal Communications Networks (PCN) 35
- Personal Communications Services (PCS) 35
- physical acces 165
- Physical Unit (PU) 199
- ping 157
- Plug and Play Operating System 134
- point-to-point connection 49
- Portmap Daemon 71
- Portmap Daemon for Automatic Startup 71
- Preparing and Running the eNetwork Wireless Client 133

- PREVIEW only 75
- Primary Rate Access 40
- primary rate interfaces (PRI) 40
- Primary-Access Equipment Modem Pools 34
- Problem Scenario 146
- Product Support 242
- Protocol and Encapsulation Hierarchie of eNetwork Wireless 48
- Protocol reduction 208
- Proxy 12
- PRPQ 48
- PSTN 7, 33
 - Area Code 83
 - Company Code 83
 - Personal Code 83
- PSTN Area Prefix 84
- PSTN Connection 83
- PSTN CountryPrefix 84
- PSTN General Prefix 84
- Public Switched Telephone Network (PSTN) 34
- Putting It All Together 8

R

- Radio Data-Link Access Procedure 22
- Radio modems 21
- Radio Network Gateway 23
- radio packet data network technology 21
- RD-LAP 22
- README file 188
- rectangles 100
- reduces unnecessary retransmissions 11
- reduction 49
- redundancy 49
- Registering eNetwork Wireless Client. 88
- regular permission 164
- Re-installing
 - Emulator Express Client for Windows 95/NT 189
 - Emulator Express Server for Windows NT 177
- Re-installing Emulator Express Client for Windows 95/NT 189
- Remote MAN 93
- Renaming Structures 106
- Response times 157
- Retransmission Optimization 49
- Revising the existing configuration 131
- RF/NCP 23
- RFC 1144 49
- ring speed 70
- RNC3000 Maximum Transmission Unit 52
- RNG 23
- roamed mobile device 20
- roaming agreement 20
- round trip times (RTT) 153
- RS/6000 54
- RTT 153
- Running the Wireless Client 116

S

- SA-bus 54

- Sample Scenario 192, 210
- sARTour 97, 145
- SCR 24
- secure tunneling 48
- Secure Tunneling Protocol 48
- Security Issues 164
- Selecting Events to Trace 181
- Selection of Wireless Networks 44
- SERV 181, 184
- session key 47
- Set as Home 99
- Set Home Submaps 99
- Setting
 - Idle Timeout 180, 183
 - the Cache Size 179, 182
 - the Maximum Number of Emulator Sessions 185
 - the Maximum Number of Sessions 180
 - the Server (Listen) Port Number 182
 - the Trace File Size 184
- share one communication channel 22
- shared media access 22
- Short Hold Mode 50
- Short Message Service (SMS) 35
- shut down 168
- Siemens 35
- Signal Information 136
- SIM 21
- Slot Addressing Scheme 25
- Slot Identifier 26
- Slot Number 25
- Slot Prefix 26
- small firewall 169
- smart card 21
- SMIT 53
- smit chinetARTour 79
- smit chlang 57
- smit chps 58
- smit commodev 60, 61
- smit inetARTour 78
- smit mktcpip 70
- SMITTY 53
- SMUX Daemon 98
- SNA host 174
- SNA LU6.2 23
- SNA3270 23
- SNMP 164
- SNMP Installation and Configuration - AIX 227
- SNMP Installation and Configuration - Windows NT 228
- snmp-trap 228
- Software Requirement. 54
- special protocol 165
- Specify the directory 182
- Specifying
 - a Directory for the Trace, Log, and Cache Files 185
- standard computer symbols 100
- Standard Context Routing 24
- Start SMUX Daemon 98
- Starting a Trace 183
- Starting the eNetwork Wireless Gateway 95
- startsrc -s portmap 72

STATIONARY 17
statistics 156
Stopping the eNetwork Wireless Gateway 97
submap IP Internet 99
Subscriber Identity Module (SIM) 36
Subscriber Unit Identifier 92
Subscriber Unit Identifier (SUI) 25
support procedures 242
Supported Platforms 209
Switched Virtual Channel (SVC) 25, 30
sx25.adt.comio 55
sx25.comio 55
sx25.npi 55
sx25.rte 55
sx25.server 55
Synchronize 106

T

tail -f /val/adm/ARTour.log 146
TCP Header Reduction 49
TCP packets 11
TCP protocol 11
TCP/IP 4
TCP/IP Client 55
TCP/IP networks 21
TCP/IP products 4
TCP/IP protocols 165
TCP/IP Server 55
Technical Basics of Wireless Communicatio 17
Telnet 181, 185
Telnet 3270 clients 176
Telnet 3270/5250 server 174
Telnet-3270 5
Telnet-3270/5250 5
Telnet-5250 5
Text entries 221
ThinkPad 174
Tivoli NetView
 Console - Event Browser 229
 Event Browser 230
 Event Browser - Web Express Event Details 231
 Management 227
Tivoli NetView - Event Browser 230
Tivoli NetView Management 227
TIVOLI network management 45
Tivoli TME 10 NetView 72
Tivoli TME 10 NetView for AIX Version 3 Release 1.2 55
TN3270E server 192
TNPR 182, 185
token ring 70
Token-Ring 21
trace 0 183
trace 1 183
Trace flag 104
Trace Options 184
Trace options 223
traceopts 185
Traces 202
tracesize 10 184
tracing 182

Tracing packets 158
traffic 195
TRAN 182, 185
transmission characteristics 11
Transmission Statistics 138
transmitted independently 10
transparent mode 37
Transport 182, 185
Trap Generation 99
Troubleshooting 141, 196, 231
trusted network 166
TTY Connection Parameters for Each User 66
twd0 63
Two Party Key Distribution Protocol (2PKDP) 165
TX-CEL 34

U

UDP Ports
 8888 94, 117, 130
 8889 94, 117, 130
UDP traffic 169
Unconfirmed 51
Uninstalling
 Emulator Express for Windows 95/NT 189
Uninstalling Emulator Express Server for Windows NT 177
untrusted network 166
User Segments 106
Using 183
 a Trace File 180

V

V.110 37, 40
V.110 protocol 54
V.32 37
V.42bis compression 35
Van-Jacobson reduction algorithm 49
vi /etc/rc.tcpip 71
View 100
Viewing and Setting Device Information 102
Viewing the Log Files 233
Virtual Storage 58
VTAM system 194

W

Web browser 6
Web Browser Configuration 226
Web Express
 Client - Log File 233
 Client - Trace File 235
 Client Configuration 218
 client port 220
 Client Problems 231
 Client Properties - Advanced Configuration 224
 Client Properties - Cache Information 222
 Client Properties - Connection Configuration 225
 Client Properties - IP Addresses and Ports 221
 Client Properties - Logging Configuration 223

- Components 207
- Implementation 206
- Optimization Methods 208
- server 220
- Server - Log File 234
- Server - Trace File 236
- Server Configuration - AIX 217
- Server Configuration - Windows NT 211
- Server Installation - AIX 209
- Server Installation - Windows NT 209
- Server Properties - Cache Configuration 214
- Server Properties - Options Configuration 217
- Solution Highlights 208
- Traces 235
- Web Express Client 8
- Web Express Server 7
- Web Serve 6
- Web-based Applications 205
- What You Need to Communicate 35
- wide area networks 10
- Windows 3.1 4, 7
- Windows 95 4, 7
- Windows NT 4, 7
- WIRED 17
- WIRELESS 17
- Wireless Client
 - Installation on NT 4.0 115
 - Installation on Windows 95 113
- wireless device 8
- Wireless Mobile Network Technologies 19
- Wireless Network Transmission Parameters 153
- wireline device 8
- World Wide Web 8
- wrapping small pieces of data 11

X

- X server 154
- X.25 23
- X.25 Adapter Software 55
- X.25 CoProcessor/1 55
- X.25 Coprocessor/2 55
- X.25 CoProcessor/2 or Multiport/2 62
- X.25 Device Driver 62
- X.25 device driver 60
- X.25 mobile originated 24
- X.25 mobile terminated 24
- X.25 networks 21
- X.25 node 21
- X.25 packet 21
- X.25 Problems 144
- X.25 Reset Delay Timer Interval 76
- X.31 protocol 42
- x25resetdelay 76
- XTERM window 154

Y

- ynchronizing TME 10 NetView and the Wireless Gateway 106

ITSO Redbook Evaluation

Mobile Computing: The eNetwork Wireless Solution
SG24-5299-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at <http://www.redbooks.ibm.com>
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?

Customer **Business Partner** **Solution Developer** **IBM employee**
 None of the above

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

What other redbooks would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

SG24-5299-00

Printed in the U.S.A.

