SG24-4821-00

ELAN Management Using Nways Campus Manager for AIX

August 1997

International Technical Support Organization
Raleigh Center

IBM

International Technical Support Organization

SG24-4821-00

ELAN Management Using Nways Campus Manager for AIX

August 1997

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix C, "Special Notices" on page 249.

First Edition (August 1997)

This edition applies to the most recent version of Nways Campus Manager for 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

Contents

Preface

This redbook details how to use the Nways Campus Manager for AIX Suite of applications to provide network management of ATM devices configured for LAN Emulation and Classical IP services. The hardware devices used includes the IBM MSS, 8285, 8281 and 8282.

Using practical examples the book demonstrates how to explore an ATM environment and resolve what network components are performing what functions. Guidelines are also provided to assist in the configuration of the LAN Emulation elements.

In addition there are further examples showing how to define specific LAN Emulation services such as redundancy and security.

The redbook also covers how to install and customize each of the Nways Campus Manager applications and how these applications are integrated with each other and with the MSS configuration tools.

By reading this redbook you will become familiar with the ELAN environment and learn how to configure the IBM ATM devices.

This redbook is intended to supplement the standard product documentation regarding NetView for AIX and Nways Campus Manager for AIX.

Some knowledge of ATM, NetView for AIX and Network Management is assumed.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the Systems Management and Networking ITSO Center, Raleigh.

The authors of this redbook are:

Gerard Combes, IBM France

Peter Dominke, IBM France

Harril Levanen, IBM Finland

Hans-Georg Linder, IBM Germany

The advisors of this redbook are:

Paul Fearn
Aroldo Yuji Yai
Systems Management and Networking ITSO Center, Raleigh

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

John Parker
Volkert Kreuk
Systems Management and Networking ITSO Center, Raleigh

Steve Breese, IBM USA
Gilles Wozelka, IBM France
Shawn Clymer, IBM USA

The members of the Nways development teams in both Raleigh and La Gaude.

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 259 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

For Internet users	`http://www.redbooks.ibm.com`
For IBM Intranet users	`http://w3.itso.ibm.com`

- Send us a note at the following address:

  `redbook@vnet.ibm.com`

Chapter 1. Introduction to ELAN Management

Network management has mainly been involved with managing static entities such as routers, hubs and bridges. With the evolution of virtual LANs and switched networks there was a requirement for IBM to add new functionality to the Nways Manager for AIX applications.

These applications provide comprehensive management for the ATM and Forum-Compliant Emulated LANs (ELANs). This redbook concentrates mainly on the management of the ELAN components and the underlying ATM infrastructure.

IBM has a number of hardware devices that provide the ELAN capabilities. These devices are the IBM 8210 and 8285 Switch.

Our approach when writing this redbook was to define a simple procedure to assist in selecting the required Nways Manager for AIX management applications. The next stage was to install and configure each module. Once the software was installed and configured we explored our network using the management software.

These initial stages are performed on an existing network with the assumption that the management software will be implemented after the network has been installed. However, we do provide guidance on how the ATM devices are configured in the scenarios throughout this redbook.

We have made the assumption that the reader has prior knowledge of ATM and ELAN concepts, however we have included a brief overview of LANE in Appendix A, “ATM Forum-Compliant LAN Emulation” on page 215.

A good understanding of network management, SNMP and TME 10 NetView would also be beneficial.

1.1 The Managed Elements in an ELAN Network

The intention of this section is to present you with the elements that are manageable in an ELAN environment and which appropriate management software component is required. By doing this we made certain that we addressed all required management tasks and would prevent loading software that would not perform any useful management tasks and would save valuable resources on our Network Management Station.

Note: At the end of this section there is a completed matrix showing the managed components and the software required.

Before we selected the software components we decided to evaluate what components we actually wanted to manage. We did this by grouping the components into the following categories:

- ATM Devices and Connections
- Classical IP Elements
- Forum-Compliant LAN Emulation Elements

The sections below discuss the managed elements further.

1.2 ATM Devices

By working through this chapter, you get a better understanding of what managed components constitute an ELAN network.

The first managed element we identified was the actual hardware devices.

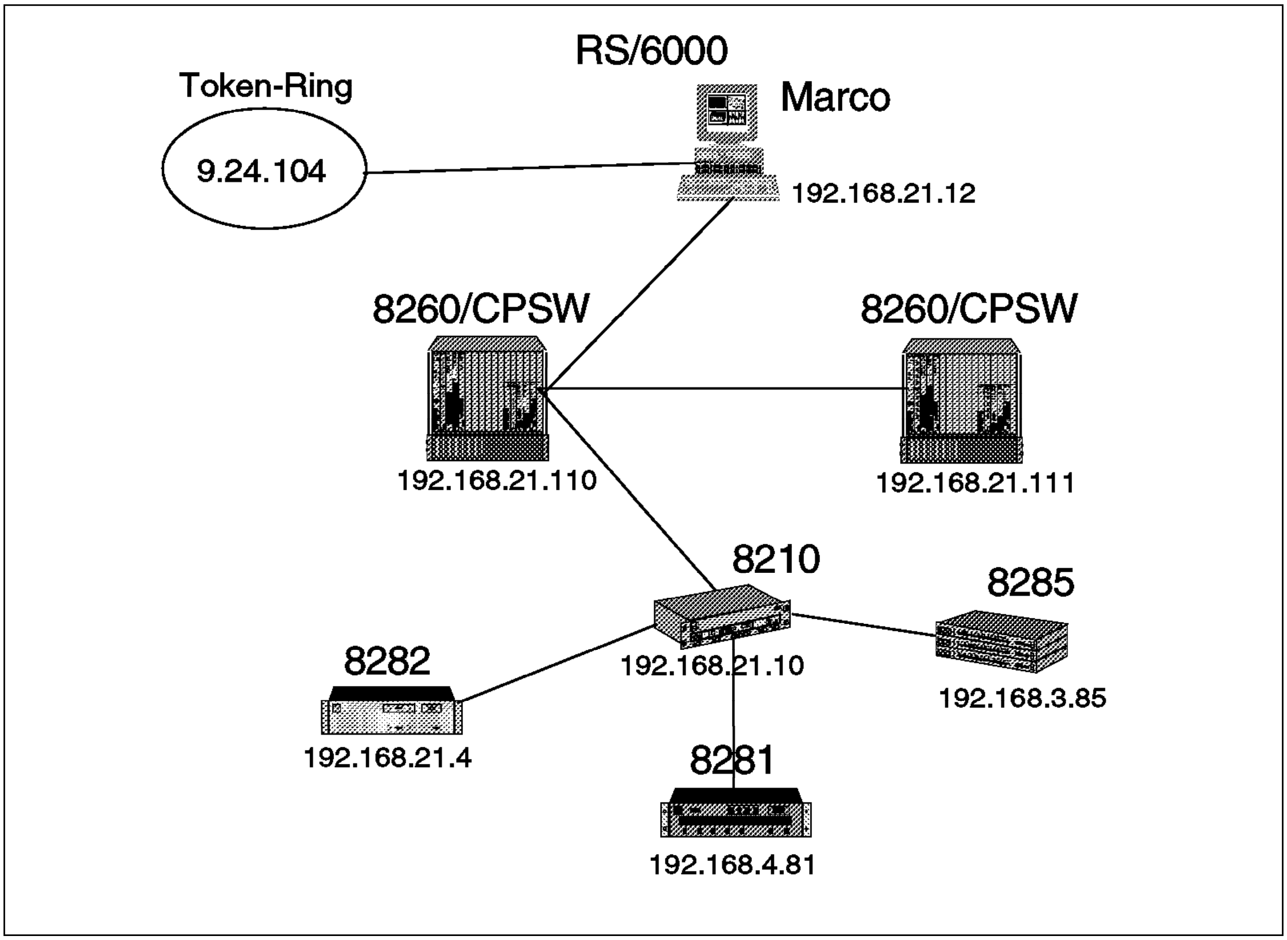

Figure 1. Hardware Devices

Figure 1 shows the physical network devices in our network. These are listed below:

The hardware entities that we deal with are listed below:

8260 8260 HUB with Control Point and Switch Module (CPSW)

8285 IBM 8285 Switch

8281 IBM 8281 Bridge

8282 IBM 8282 Concentrator

8210 Multiprotocol Switching Server (MSS)

Regardless of these devices being ATM devices they will also require some basic management of features such as overheat-condition detection or power supply failure.

The list is incomplete as far as a *real life* network is concerned, but since the main focus of this book is on LAN Emulation we have excluded the legacy LAN devices (for example, 8230).

1.3 ATM Network Structure and Connections

The following items define the underlying structure of an ATM network. Since it is this infrastructure, that the whole LAN emulation is based on it will also be dealt with in this redbook (although in not too much detail).

Clusters As the principle grouping of an ATM network so far. With the advent of PNNI phase one support, there will also be peer groups, but due to restraints in our network we could not reflect on these items as yet.

ATM end system interfaces ATM interfaces (UNI 3.0 and UNI 3.1) serve the purpose of attaching ATM end devices to an ATM network and setting up connections (SVCs) through it. Since ELAN devices have to establish these connections, they are of interest in this respect.

ATM network interfaces From the beginning of campus ATM networks the problem of connecting switches was solved by either proprietary interface definitions such as SSI or by the first releases of a public NNI (PNNI phase 0 alias IISP).

PVCs and SVCs Since these are the ″real″ connections that are established to eventually do the transport of data for an ELAN, their setup, maintenance and breakdown is of interest too.

1.4 Classical IP

Classical IP is included because we use this connection method for our Network Management Station. It proved to be a reliable and fairly simple method of connecting the Network Management Station to our ATM network. However, you should always keep in mind that *any* kind of IP connection will serve this purpose. And in addition, *one* such connection will do for all of these management tasks. There is never a need for more than one connection at time. We do show a number of established connections throughout this redbook.

The ATM host connection using Classical IP will connect to other hosts by being part of a logical IP subnet (LIS). This LIS will contain an ATM Address Resolution Protocol (ATMARP) server and a number of ATMARP clients. The ATMARP server is responsible for maintaining a table of ATM addresses and their corresponding IP address.

The Classical IP connected devices will be routed to other IP subnets in order to communicate with the LAN Emulation Clients.

Figure 2 on page 4 summarizes the different components of LAN Emulation. It is they and their management that this redbook is mainly concerned with.

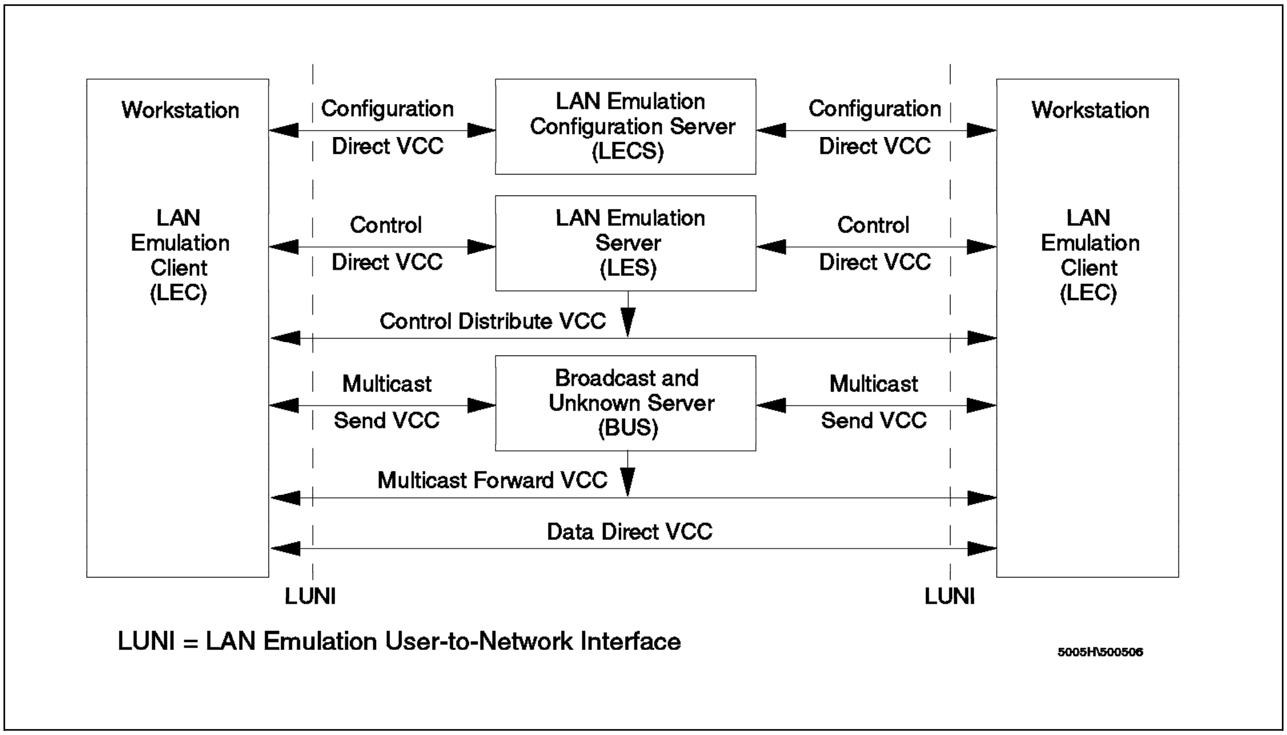

Figure 2. LAN Emulation Components

1. LAN Emulation Clients

   Users connect to the ELAN via LE clients, which request services through the LAN Emulation User-to-Network Interface (LUNI).

2. LAN Emulation Server (LES)

   The basic function of the LE server is to provide directory and address resolution services to the LECs of the emulated LAN. Each emulated LAN must have an LE server.

3. Broadcast and Unknown Server (BUS)

   The BUS is the element of LAN Emulation that permits broadcast messages on a connection-oriented network. On IBM devices LES and BUS show up in pairs, even sharing the same ATM address. Still they have separate functions.

4. LE Configuration Server (LECS)

   The LECS assigns the individual LE clients to the different virtual LANs that can exist in the ATM network. In addition to this, Nways Campus Manager ATM also considers them a focal point of ELAN administration, making it more than just an optional means of conveniently finding the proper LES/BUS pair.

The following are the additional functions (value add functions) that come included in the MSS functionality and are not included in the original definitions of the ATM Forum:

Security is enhanced by the security function of the server which disables a random LEC to join an ELAN unless complying with the policy regulations of its corresponding LECS. This feature can be managed from Nways Campus Manager ATM.

Bridging functionality with both transparent bridging and source route bridging combined in an adaptive source route transparent conversion bridging method (for NetBIOS and SNA).

Shortcuts can be introduced that establish a direct connection without interference of further intermediate LAN Emulation Clients serving as routers or bridges.

- Shortcut bridging
- IP cut-through
- NHRP

Redundancy enhancements based on the establishment of a heartbeat surveillance type of connection between redundant LES/BUS pairs. Redundancy can also be established for LECSs.

1.4.1 LAN Emulation VC Connections

Data transfer in the LE system (consisting of control messages and encapsulated LAN frames) uses a number of different ATM VCCs as illustrated in Figure 2 on page 4. In the 8260-based network these VCCs are realized by SVCs, which are established by the corresponding UNI interface of the ATM end systems involved. We can discriminate the following:

1. Control VCCs

   Control VCCs connect an LE client to the LE configuration server and the LE server, but they are never used for user data traffic. The following control VCCs are established:

   Configuration Direct VCC A bidirectional, point-to-point configuration direct VCC may be established between an LE client and the LECS to obtain configuration information (for example, the LE server′s ATM address).

   Control Direct VCC A bidirectional, point-to-point control direct VCC must be established (and kept active) between each LE client and the LE server. This is used for the exchange of control traffic (for example, address resolution) between the LE client and the LE server.

   Control Distribute VCC The LE server may optionally establish a unidirectional control distribute VCC to distribute control information (for example, query for an unregistered MAC address) to all LE clients connected to the ELAN.

2. Data Connections

   Data connections are direct VCCs from an LE client to another LE client or to the BUS. They are used to carry user data traffic and never carry control traffic (except for a flush message for cleanup).

   Data Direct VCC For unicast data transfer between end systems.

   Multicast Send VCC A point-to-point VCC from the LEC to the BUS. This VCC is used by the LEC to send broadcast and multicast data frames. It is also used by the LE clients for sending unicast frames until a data direct VCC is established between the LE client and its partner.

   Multicast Forward VCC A point-to-multipoint VCC from the BUS to the registered LECs used to forward data frames from the BUS to them.

Having introduced the elements that our management will be dealing with, let us briefly introduce the three different aspects of this management that we focus on.

1.5 Network Management Functions

Network management is normally subdivided into different aspects or categories. IBM historically differentiated between six such categories until with the advent of Tivoli this was reduced to just four. Our redbook concentrates on the following three aspects, which are best covered by the functionality of the Nways Campus Manager ATM software:

Configuration As the act of manipulating the controlling elements of a given hardware device in order to determine the flow of data and control through your network.

Problem Provides the ability to centrally monitor the managed components and report any faults to the network management station, and provides tools to perform problem diagnostics.

Performance Monitoring Addresses the performance of the managed components by collecting and graphing performance-related data, and having the ability to identify and network problems due to performance.

1.6 Software Elements of Nways Campus Manager

Table 1 on page 7 shows a list of the specific products you can choose from for management of our network elements. They are all contained in the Nways Campus Manager Version 1.1 package. Since this list may be outdated by the time of reading, refer to the latest announcement letters found at:

`www.networking.ibm.com`

Note: The installation instructions for each specific application are detailed in Chapter 2, "Installing and Configuring the Network Management Station" on page 11.

By using the elements we have defined the next stage as deciding what functions we need performed for each managed element.

The current Nways Manager for AIX software is divided up as follows:

LAN Network Manager Features SNMP-based management of token-ring networks including bridges, legacy and emulated segments. Full integration of RMON ring station information into network views. Links offered to ELAN management software component for detail exploration of emulated segments. Capable of showing (though not merging) information gathered by LLC-based LNM/2.

Router and Bridge Manager Version 2 SNMP-based gathering of information, control of threshold conditions, evaluation of incoming device traps. Graphical display of data over time.

ELAN Manager Management of ELAN domains, complete with all aspects concerning LECSs, LES/BUS pairs and LECs. Configuration, setup, and control of the complete Forum-Compliant LAN Emulation environment.

ATM Manager Visualization and control of all ATM-related connection elements. Monitoring of performance data.

LANReMon Full function access to all data collected by RMON agents in the network. This component is not covered in much detail by this publication.

Product-Specific Modules Graphical user interface access for most of the IBM networking devices. Provides configuration and status monitoring.

Nways Manager for AIX for AIX Version 1.1 comprises of the applications listed in the Table 1.

Table 1 (Page 1 of 2). Nways Campus Manager for AIX Version 1.1

Product Description	**Package Name**	**Version Number**
Management Application Transporter	mgtapptran.obj	2.1.0.0
Management Application Transporter books	mgtapptran.book.obj	2.1.0.0
ObjectStore Runtime 4.0.2 for AIX	ostore_runtime.base	4.0.2.0
8282 ATM Bridge Manager (PSM)	ahm6000.R8282s10.obj	3.2.0.0
8285 ATM Concentrator Manager (PSM)	ahm6000.R8285s10.obj	3.2.0.0
ATM Bridge Manager (PSM)	ahm6000.R8281s10.obj	3.2.0.0
ATM Manager and LAN Emulation Manager	ahm6000.base	3.2.0.0
Campus Manager - ATM HFC Manager	ahm6000.hfc	3.2.0.0
Campus Manager - ATM Web-Based Manager	ahm6000.atmweb	3.2.0.0
English/American DynaText books for Campus Manager - ATM	ahm6000.books.En_US.base	3.2.0.0
Nways MSS Server Manager (PSM)	ahm6000.R8210s10.obj	3.2.0.0
8224 Hub Manager (PSM)	cml.8224	3.2.0.0
8230 Hub Manager (PSM)	cml.8230	3.2.0.0
8235 DIALS Server (PSM)	cml.8235	3.2.0.0
8235-I40 IBM 8235 Model I40 DIALs Switch (PSM)	cml.8235-2	3.2.0.0
8238 Hub Manager (PSM)	cml.8238	3.2.0.0
8250 and 8260 Manager	cml.8250-60	3.2.0.0
8271-1 Nways Ethernet LAN Switch Manager (PSM)	cml.8271-1	3.2.0.0
8271-108 Nways Ethernet LAN Switch Manager (PSM)	cml.8271-108	3.2.0.0
8272 Token-Ring Switch Manager (PSM)	cml.8272	3.2.0.0
8273-74 Ethernet Route Switch/LAN Route Switch (PSM)	cml.8274	3.2.0.0
English/En_US Dynatext books	cml.books	3.2.0.0
FDDI Capability (LAN Network Manager)	cml.fddi	3.2.0.0

Product Description	Package Name	Version Number
Fast Ethernet Stackable Hub (PSM)	cml.8225	3.2.0.0
Multiprotocol Routers (PSM)	cml.2210	3.2.0.0
Network Processor (PSM)	cml.6611	3.2.0.0
OS/2 Agent Capability (LAN Network Manager)	cml.lnme	3.2.0.0
Required Common Part for PSMs (2210 & 6611)	cml.ibmr	3.2.0.0
Required Common Part for PSMs (8271-1-8827282818285821082)	cml.COMM	3.2.0.0
Required Common Part of Campus Manager (except for PSMs)	cml.base	3.2.0.0
Required Common Part of LAN Network Manager	cml.baseLAN	3.2.0.0
SNMP Bridge Capability (LAN Network Manager)	cml.br	3.2.0.0
Token-Ring Capability (LAN Network Manager)	cml.tr	3.2.0.0
IBM Nways Campus Manager / Remote Monitor En_US Acrobat b	lanReMon.En_US.books	2.0.0.0
IBM Nways Campus Manager / Remote Monitor advanced	lanReMon.advance.obj	2.0.0.0
IBM Nways Campus Manager / Remote Monitor basic	lanReMon.base.obj	2.0.0.0
IBM Router and Bridge Manager Server	rabm.obj	2.2.0.0
(For NetView for AIX) IBM AIX APPN Topology Application/6	rabmappn.obj	1.3.0.0
IBM Router and Bridge Manager Client	rabmclt.obj	2.2.0.0
(For NetView for AIX) IBM AIX DLSw Topology Application/6	rabmdlsw.obj	1.3.0.0
IBM AIX Router and Bridge Manager/6000 Publications	rabmbook.obj	2.2.0.0
IBM Systems Monitor for AIX (CFG)	smcfg.eui.obj	2.3.1.0
IBM Systems Monitor for AIX (CFG) DynaText - En_US	smcfg.dtext.En_US.eui.obj	2.3.1.0
IBM Systems Monitor for AIX (MLM)	smmlm.subagent.obj	2.3.1.0
DynaText Browser	dtext.brwsr.obj	2.3.0.2
IBM Nways Campus Manager / Traffic Monitor Basic	TrafficMon.traffic_mon	1.1.0.0
(For NetView for AIX) IBM AIX Alert Manager	alertman.obj	1.2.6.1

Table 1 (Page 2 of 2). Nways Campus Manager for AIX Version 1.1

An IBM Web page that contains the product descriptions is located at http://www.networking.ibm.com/cms/cmsprod.html.

1.7 Selecting the Specific Software Components

Now, what should you choose from the above to actually manage the elements and devices in your network? Simply installing them all may seriously impact the overall performance of your Network Management Station. The following matrix contains the names of the applications that will perform the required management functions for our ELAN network.

Table 2. ATMC Product Selection

Managed Element	Configuration	Problem	Performance
8260 Chassis	cml.8250-60	NetView	-
8260 CPSW	telnet	NetView	-
8285	8285 PSM	NetView RABM	-
8282	8282 PSM	NetView RABM	-
8210	8210 PSM MSS Web Browser	NetView ATMC	ATMC
8281	8281 PSM	NetView RABM	-
ATM clusters	ATMC Telnet	-	-
ATM end system interfaces	ATMC	NetView	-
ATM network interfaces	ATMC	NetView RABM	ATMC
PVCs and SVCs	ATMC	NetView/RABM RABM	ATMC
Classical IP ARP servers/clients	telnet	-	-
ELAN FC elements (LECS, LES/BUS pairs, LEC)	ATMC	NetView ATMC	ATMC
ELAN value add functions	ELS	MSS Web Browser Telnet	-
ELAN VC connections	ATMC	ELS	ATMC

Notes:

1. NetView - NetView for AIX Version 4
2. PSM - Product Specific Module
3. ATMC - NWAYS ATM Campus Manager
4. RABM - Router and Bridge Manager
5. ELS - MSS Event Logging System

Table 2 is included to provide a basic template to assist in the design of your management framework.

1.8 Components to Install

Using Table 2 on page 9 we can construct a list of the specific applications required to manager our ELAN network.

There are a number of pre-requisites to consider when installing the Nways software. These are as follows:

- mgtapptran must be installed prior to installing the the PSM modules.
- The Object Store must be installed before the ATMC applications and/or before installing Router and Bridge Manager.
- The PSMs modules require the relevant base application either CML or ATM.

We installed the application components in the following order.

Note: AIX Version 4.2 was already installed on our network management station.

1. NetView for AIX Version 4.1
2. NetView PTF
3. mgtapptran transporter (contained within the NetView PTF)
4. Object Store database
5. Campus Manager LAN base (cmlbase)
6. Campus Manager Common part for PSMs
7. Campus Manager ATM (atmbase) including PSM modules
8. Mid-Level Manager
9. Router and Bridge Manager

The next chapter describes our installation process.

Chapter 2. Installing and Configuring the Network Management Station

This chapter describes the installation procedure for the Network Management Station software detailing each of the installation stages. Also we describe how the Network Management Station was connected to the ATM network and explain the what options exist for connecting the Network Management Station to the network.

The chapter is divided into the following sections:

- Server hardware configuration
- Connecting the Network Management Station to the ATM network
- Installing the Nways Manager for AIX software

2.1 Server Hardware Configuration

We defined our Network Management Station with the host name of marco and was installed with two network cards, one token-ring card and one ATM card.

Marco was configured with the following hardware components:

```
+ hdisk0           00-00-0S-0,0      1.0 GB SCSI Disk Drive
+ hdisk1           00-00-0S-1,0      1.0 GB SCSI Disk Drive
+ tok0             00-02             Token-Ring High-Performance Adapter
* atm0             00-03             100 Mbps ATM Adapter
+ ppr0             00-04             POWER Gt4e Graphics Adapter
+ mem0             00-0B             128 MB Memory Card
```

Typically with the RS/6000 the more memory that is installed the more efficient the software will perform. However we have listed the minimum disk requirements for the Nways Manager for AIX applications.

- 38 MB with Nways Campus Manager RMON
- 42 MB with Nways Campus Manager ATM
- 98 MB with Nways Campus Manager LAN without RABM and LNM
- 110 MB with Nways Campus Manager LAN without RABM
- 201 MB with Nways Campus Manager LAN with LNM
- 215 MB with Nways Campus Manager LAN with RABM and LNM
- 295 MB with Nways Campus Manager for AIX V1.1

The RAM requirements depend on how many actual devices will be managed by NetView and Nways Manager for AIX. We had 128 MB of RAM installed on our Network Management Station and quite often we saw some slow response times and heavy paging activity.

The latest resource requirements are normally located in the relevant release notes for each application.

Also check that there is enough available free disk space for both the Object Store and Router and Bridge Manager applications to add their file systems. The installation of these products will fail if there is not enough disk space. To check your disk space key in the command:


```
lspv hdisk0
```

Check the line shown below:

```
FREE PPs:          16 (64 megabytes)
```

We had 64 MB free, which is adequate for our environment. This of course depends on the size of the network you want to manage.

We also recommend that you allocate at least twice the amount of your physical memory in paging space. This can be monitored using the command:

```
lsps -a
```

In addition, the AIX vmstat command will show the the active paging space activity.

Given less memory and a lot of paging, the software will still work reliably, but you may see effects such as windows taking a long time to display.

2.2 Connection the Network Management Station to the ATM Network

We connected the Network Management Station to the ATM network using a Classical IP connection to the IBM 8210 Server. To access the ATM network and devices we assigned the ATM card the IP address of 192.168.21.10. The network 192.168 is our ATM subnet. The token-ring card was assigned 9.24.104.12 to provide connectivity to the legacy token-ring network. The IBM 8210 was configured as an ARP server and marco defined as an ARP client (see Figure 1 on page 2).

Figure 3 shows the ATM card configuration for marco; use the command smit inet. Then select **Change/Show Characteristics of a Network Card**.

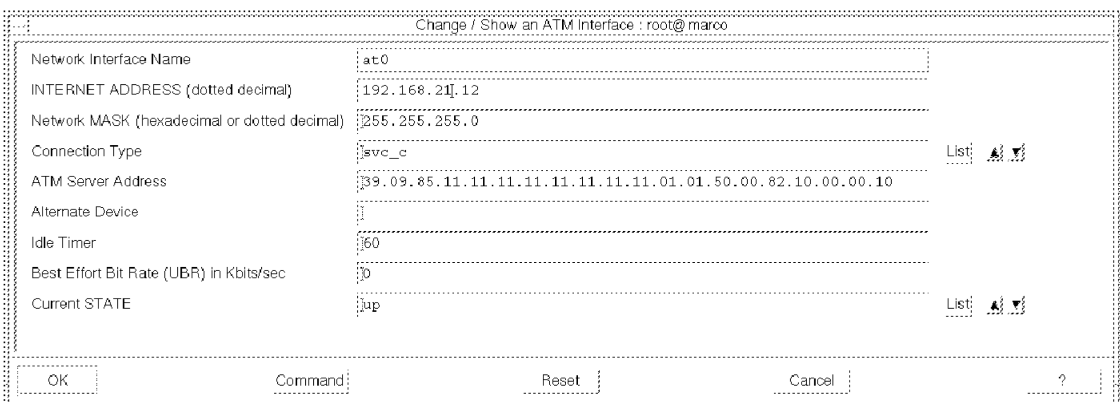

Figure 3. ATM Network Card Parameters

The ATM server address is the ATM ARP address configured in the IBM 8210 device.

We also tested the LAN Emulation Client software for AIX Version 4.2. This provided the facility to configure marco as an LEC by defining a policy rule based on the ELAN name for marco. This code is beta form, so we did not include any documentation in this redbook. However, you may want to be aware that this feature exists for RS/6000.

If the RS/6000 does not have the an ATM card installed, then the Network Management Station could be connected to the ATM network via a gateway. We also tested this method.

All the connection methods provided us with exactly the same function from a management perspective.

2.3 Installing the Nways Manager for AIX Software

The software installation process is described below.

The Network Management Station was installed with AIX Version 4.2. Before installing the NetView for AIX software we disabled the ATM card to allow the NetView software to install using the network information relating to the legacy LAN. This was to reduce the possibility of NetView becoming confused as to which subnet it will use to create its configuration files.

Once the NetView software was installed we re-enabled the ATM card and performed a demand-poll on marco.

Note: All the packages where installed using standard smit install screens.

We installed NetView (base and feature package) and the latest PTF level U447036. The output of lslpp -ah after this should look as follows:

```
# lslpp -ah "nv*.obj"
  Fileset         Level     Action      Status      Date        Time
  -----------------------------------------------------------------------
Path: /usr/lib/objrepos
  nv6000.base.obj
                  4.1.2.0   COMMIT      COMPLETE    05/01/97    15:56:
                  4.1.2.0   APPLY       COMPLETE    05/01/97    15:56:
          4.1.2.0.U440147   (U447036)
          4.1.2.0.U441259   (U447036)
          4.1.2.0.U441840   (U447036)
          4.1.2.0.U444912   (U447036)
          4.1.2.0.U446444   (U447036)
          4.1.2.0.U447036   COMMIT      COMPLETE    05/01/97    16:59:
          4.1.2.0.U447036   APPLY       COMPLETE    05/01/97    16:48:

  nv6000.features.obj
                  4.1.2.0   COMMIT      COMPLETE    05/01/97    15:56:
                  4.1.2.0   APPLY       COMPLETE    05/01/97    15:56:
          4.1.2.0.U440147   (U447036)
          4.1.2.0.U441259   (U447036)
          4.1.2.0.U441840   (U447036)
          4.1.2.0.U444912   (U447036)
          4.1.2.0.U446444   (U447036)
          4.1.2.0.U447036   COMMIT      COMPLETE    05/01/97    16:59:
          4.1.2.0.U447036   APPLY       COMPLETE    05/01/97    16:48:
```

After installing NetView, it is convenient to install Management Application Transporter, since the latest version of this code is delivered on the same tape as the NetView PTF. Management Application Transporter (MAT) is required for all the Product Specific Modules (PSMs) that come with the Nways Campus Manager software. There is a more detailed description of it available in the book *Campus ATM Network Manager Guidelines*, SG24-5006-00 but we also cover some aspects of it in this publication. You should install the following parts of it:

```
# lslpp -ah "*mgtapptran*"
  Fileset         Level     Action       Status       Date         Time
  ----------------------------------------------------------------------
Path: /usr/lib/objrepos
  mgtapptran.book.obj
                  2.1.0.0   COMMIT       COMPLETE     05/01/97     16:44:
                  2.1.0.0   APPLY        COMPLETE     05/01/97     16:44:

  mgtapptran.obj
                  2.1.0.0   COMMIT       COMPLETE     05/01/97     16:44:
                  2.1.0.0   APPLY        COMPLETE     05/01/97     16:44:
```

2.3.1 Removing Previous Versions of Nways Manager for AIX

Any step taken so far could of course be based on an existing version of your network management too. For all the steps taken from here onwards it appears that there is no simple and easy transition from an existing management configuration under Nways Campus Manager Version 2 to the new Nways Campus Manager Version 3. If there are any components installed so far, it is recommended to first uninstall them completely, before proceeding with the installation of the new version.

This is partly because of the newly introduced usage of the Object Store database, which was not common to the modules used under Version 2. In addition, it appears advisable to give a complicated software setup a completely new start. Moreover, some of the new software products such as Router and Bridge Manager are very different in function and setup.

In case you had a preliminary version of Object Store installed, make sure to remove this as well. Check the output of the command /usr/lpp/ODI/OS4.0/cset/bin/osversion. If the output is not similar to: `Object Store Release 4.0.2 for AIX/C Set ++.`, remove it together with all the other components mentioned below.

Remove all old PSMs if you are installing a new version of cml.COMM. To find out the current version of cml.COMM issue the command lslpp -l | grep cml. The output is similar to: `cml.COMM   2.10.0.0 COMMITTED`.

From an AIX command line, type `smitty` then select the following choices one by one as they become available:

- Software installation and maintenance
- Maintain installed software
- Remove software products

Now make sure that the focus is in the Software name field. Press F4 to get the list of available software for removal. Select each component using F7, for example:

```
F4: Software name.  When you
  Select with F7, a '>' will appear
  in front of the selected item.

  > ahm6000.base
  > ahm6000.R8210s10.obj
  > ahm6000.R8281s10.obj
  > ahm6000.R8282s10.obj
  > ahm6000.R8285s10.obj
  > ahm6000.R8285s10.obj
  > cml.COMM
  > cml.8250-60
  > cml.base
  > cml.baseLAN
  > cml.br
```

After you have selected all the components you wish to remove, press Enter. Now you are given several choices to complete the options you wish to remove (see Figure 4, which shows the software removal parameters).

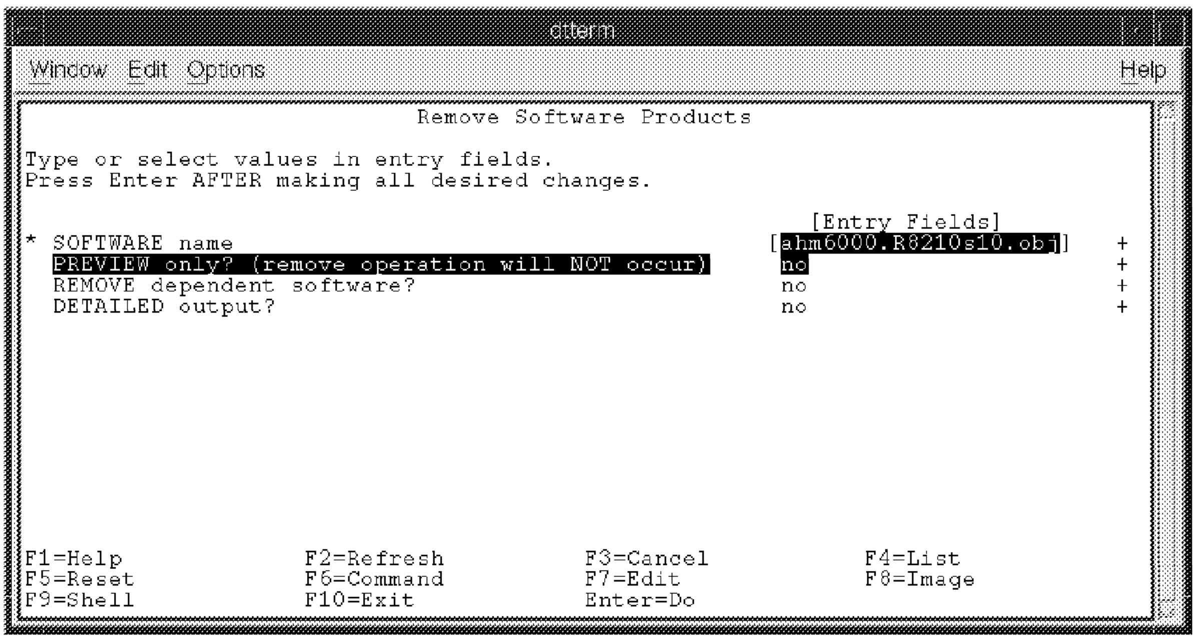

Figure 4. Removing Software Products

Remember to set the following:

- PREVIEW only to no
- REMOVE dependent software to no

During the removal of the components, TME 10 NetView will be re-started a number of times. It is advisable to close down all NetView interfaces before continuing with this operation.

The installation summary section will display SUCCESS after each component is removed. You can also search for error or warning strings in the file to see if any of the subcomponents failed to be removed.

After removing all the previously installed Nways Campus Manager software you can now install the latest version.

2.3.2 The Installation Process

From the list of software applications that we included in our table, we installed these products in a specific order.

The first part of these components is the Object Store database.

2.3.3 Installing Object Store (ODI Database)

As said before, the new version of the code stores much of the information retrieved from the network (notably the ATM information) in the new Object Store database. So, before installing the components of Nways Campus Manager Suite you need to install the latest version of the Object Store. You will find the code delivered to you on the same media as the Nways Campus Manager software.

In the installation handbook that accompanies the deliverables the installation of Object Store is described in the back of the book. Nevertheless this has to be done first.

Using smit we installed the Object Store option. The image name is ostore_runtime.image. After Object Store is successfully installed, the directory /usr/lpp/ODI/OS4.0/cset/bin is created. It contains the Object Store commands. The documentation can be found in the directory /usr/lpp/ODI/OS4.0/doc.

Once the installation has completed you need to check the install log:

```
/usr/lpp/ODI/OS4.0/install_log
```

If this is the first time Object Store is installed on the machine you *must* configure it before continuing with the Nways Manager for AIX installation. The following lines show the output of our configuration process.

```
root@marco:/usr/lpp/ODI/OS4.0/cset/bin# osconfig server
The default copy of ObjectStore to configure is in
/usr/lpp/ODI/OS4.0/cset.
Is this the copy that you want to configure?  yes

ObjectStore includes shared libraries. For ObjectStore applications
and utilities to work, the dynamic linker must be able to find them.
The recommended arrangement is to have symbolic links
in /usr/lib to the shared libraries.
If you choose not to make these links, then you will
have to instruct all ObjectStore users to add
/usr/lpp/ODI/OS4.0/cset/lib
to their LIBPATH environment variable.

WARNING: ObjectStore libraries already exist in /usr/lib.
If you choose not to make links in /usr/lib for the
new libraries, ObjectStore users may incorrectly link with
old libraries.

Do you want to create links to ObjectStore libraries in /usr/lib?  yes
Since you have requested a File-database configuration,
you must give a pathname for the transaction log file.
Where do you want to put the transaction log?
/usr/lpp/ostore_runtime/transaction.log
You have configured this machine to run an ObjectStore server.
The server′s transaction log is in /usr/lpp/ostore_runtime/transaction.log.

Do you want to proceed?  yes
Writing configuration files and initializing the server, please wait...
970515 092503 ObjectStore Release 4.0.2 Database Server
The ObjectStore server is running.

ObjectStore includes a server daemon which must be running
for any application to access an ObjectStore database.
It is recommended that you auto-start the daemon via commands
in your operating system startup scripts. If you do not configure
automatic startup, you will have to start the server daemon by hand,
or re-run this utility to configure auto-start.

Would you like to configure automatic server startup and shutdown?  yes
The ObjectStore Server daemon process is accessible.
Schema databases are accessible.

The cache manager launcher for release 4 (/usr/lpp/ODI/OS4.0/cset/lib/oscminit)
has correct modes and ownership.
ObjectStore configuration completed.
```

To see the state of Object Store in /usr/lpp/ODI/OS4.0/cset/bin, use the following commands:

- osversion
- ossvrping -v hostname (where hostname is the Network Management Station)
- ossvrstat

2.3.4 Configuring Object Store (ODI Database)

Once the Object Store is installed it must be configured. From the AIX command line issue the command:

```
cd /usr/lpp/ODI/OS4.0/cset/bin
```

In our case, osconfig server was /usr/lpp/ostore_runtime/transactionlog.

Further information relating to the Object Store can be found in the files listed below:

- /usr/lpp/ODI/OS4.0/doc/ascii (ASCII format)
- /usr/lpp/ODI/OS4.0/doc/html (HTML format)

The Object Store stores files in the directory /tmp/ostore and contains some error logging and socket information. The required space is about 10k.

Note: The default directory for the sockets configuration is set to /tmp/ostore. If the contents of /tmp is removed, the Object Store application will not function correctly.

The following variables must be defined in the file /etc/environment:

- export OS_CACHE_DIR=/usr/CML/OStore/cache
- export OS_COMMSEG_DIR=/usr/CML/OStore/cache
- export OS_ROOTDIR=/usr/lpp/ODI/OS4.0/cset
- export LIBPATH=/usr/lpp/ODI/OS4.0/cset/lib
- export OS_AS_START=0x70000000

The binary files for the Object Store are located in the directory $OS_ROOTDIR and contain the following:

To clean up the Object Store environment issue the command:

```
$OS_ROOTDIR/bin/oscmrf
```

To stop the cache manager process, issue the command:

```
$OS_ROOTDIR/bin/oscmshtd
```

To stop the server process, issue:

```
$OS_ROOTDIR/bin/ossvrshtd hostname
```

After any modifications are made to the Object Store configuration the server must be re-started, so that the changes will come into account. To restart the server, issue: `/etc/rc.objectstoreserv`.

2.3.5 Object Store Troubleshooting

To see if the server is running and accessible issue the command: `$OS_ROOTDIR/bin/ossvrping marco` (where marco is the hostname).

If everything is running satisfactory, the Object Store server on host marco will respond with `Server marco is alive`.

If Object Store is not alive, we need to check that it has been configured correctly:

- Verify that the transaction log file is correctly created in the directory you entered during the osconfig process. We used the directory /usr/lpp/ostore_runtime/transactionlog.
- Verify that the sockets are created in the directory /tmp/ostore.

In the /tmp/ostore directory there are three types of files:

1. The cache files: Data transferred from server to Object Store client will be stored inside these cache files. Each process using Object Store API is a client, so will have its own cache file.
2. The Commseg files: Data control files to manage cache files (for example, locking).
3. The third type of file is defined as socket used by the cache manager process and server process. The file /etc/ports is updated during installation to include these entries.

2.3.6 Product Installation

Remember our recommendation that only the required modules should be installed in order to save space and memory. For our environment we proceeded with the following choices:

```
                              SOFTWARE to install                           x
                                                                            x
     Move cursor to desired item and press F7. Use arrow keys to scroll.   x
         ONE OR MORE items can be selected.                                 x
     Press Enter AFTER making all selections.                               x
                                                                            x
      MORE...8                                                              x
                                                                            x
       cml                                                              ALL x
        + 3.2.0.0  2210 Multiprotocol Routers (PSM)                         x
        + 3.2.0.0  6611 Network Processor (PSM)                             x
        + 3.2.0.0  8224 Hub Manager (PSM)                                   x
        + 3.2.0.0  8225 Fast Ethernet Stackable Hub(PSM)                    x
        + 3.2.0.0  8230 Hub Manager (PSM)                                   x
        + 3.2.0.0  8235 DIALS Server (PSM)                                  x
        + 3.2.0.0  8235-I40 IBM 8235 Model I40 DIALs Switch (PSM)           x
        + 3.2.0.0  8237 10baseT Ethernet Stackable Hub                      x
        + 3.2.0.0  8238 Hub Manager (PSM)                                   x
     >  + 3.2.0.0  8250 and 8260 Manager                                    x
        + 3.2.0.0  8271-1 Nways Ethernet LAN Switch Manager (PSM)           x
        + 3.2.0.0  8271-108 Nways Ethernet LAN Switch Manager (PSM)         x
        + 3.2.0.0  8272 Token Ring Switch Manager (PSM)                     x
        + 3.2.0.0  8273-74 Ethernet RouteSwitch/LAN RouteSwitch (PSM)       x
     >  + 3.2.0.0  English/En_US books for Campus Manager - LAN             x
        + 3.2.0.0  FDDI capability (LAN Network Manager)                    x
     >  + 1.1.0.0  IBM Nways Campus Manager - Switching Modules Management  x
        + 3.2.0.0  OS/2 Agent capability (LAN Network Manager)              x
        + 3.2.0.0  Required common part for PSMs (2210 & 6611)              x
     >  + 3.2.0.0  Required common part for PSMs (8271-1-8,8272,8281,8285,821 x
     >  + 3.2.0.0  Required common part of Campus Manager (except for PSMs) x
     >  + 3.2.0.0  Required common part of LAN Network Manager              x
     >  + 3.2.0.0  SNMP Bridge capability (LAN Network Manager)             x
     >  + 3.2.0.0  Token-Ring capability (LAN Network Manager)              x
      BOTTOM                                                                x
                                                                            x
```

It may be interesting to know how much space our installation consumed. Here is the file system usage before the installation:

```
root@marco:/tmp/ostore#df -k
Filesystem    1024-blocks      Free %Used    Iused %Iused Mounted on
/dev/hd4             8192      2572   69%     1409    35% /
/dev/hd2          1257472    335044   74%    29002    10% /usr
/dev/hd9var         20480      2192   90%      908    18% /var
/dev/hd3            53248     48780    9%      144     2% /tmp
/dev/hd1             4096      1672   60%      301    30% /home
/dev/lv00          303104    121856   60%       62     1% /code
```

The file system usage after intallation was:

```
Filesystem    1024-blocks      Free %Used    Iused %Iused Mounted on
/dev/hd4             8192      2568   69%     1412    35% /
/dev/hd2          1257472    139928   89%    35227    12% /usr
/dev/hd9var         20480      2212   90%      908    18% /var
/dev/hd3            53248     48760    9%      159     2% /tmp
/dev/hd1             4096      1664   60%      301    30% /home
/dev/lv00          303104    121856   60%       62     1% /code
/dev/lv01           24576     20576   17%       21     1% /usr/CML/OStore/c
```

The installation should indicate success for all of your installed items. Here is the output from smit:

```
cml.COMM                    3.2.0.0         USR         APPLY       SUCCESS
cml.8272                    3.2.0.0         USR         APPLY       SUCCESS
cml.8238                    3.2.0.0         USR         APPLY       SUCCESS
cml.8230                    3.2.0.0         USR         APPLY       SUCCESS
cml.smm                     1.1.0.0         USR         APPLY       SUCCESS
cml.base                    3.2.0.0         USR         APPLY       SUCCESS
cml.books                   3.2.0.0         USR         APPLY       SUCCESS
cml.baseLAN                 3.2.0.0         USR         APPLY       SUCCESS
cml.tr                      3.2.0.0         USR         APPLY       SUCCESS
cml.br                      3.2.0.0         USR         APPLY       SUCCESS
cml.8250-60                 3.2.0.0         USR         APPLY       SUCCESS
```

After the installation you will find a new file system mounted. It is /usr/CML/OStore/cache and holds the cache data for the Object Store database clients. Your clients should be visible via the oscmstat command.

To view the clients issue the command:

```
oscmstat marco
```

Our output is shown below:

```
ObjectStore Release 4.0.2 Cache Manager Status: Cache Manager Version 8.2.
Process ID 12136.  Executable is /usr/lpp/ODI/OS4.0/cset/lib/oscmgr4.
Host "marco".  Started at Thu May 15 11:21:18 1997
Soft Allocation Limit 0, Hard Allocation Limit 0.
Allocated: free 0, used 3239984.
Server host:       Client process ID:     Status for this host:
       marco       0                      Initializing: constructor finished
       marco       0                      Initializing: constructor finished

There are 2 clients currently running on this host:
  54856       0       search process v10.0 0x30020000
  46666       0              unknown v10.0 0x30000000
Free files (cache):
   NONE
In-use files (cache):
  /usr/CML/OStore/cache/objectstore_4_marco_cache_7 (1998848)
  /usr/CML/OStore/cache/objectstore_4_marco_cache_6 (999424)
Free files (commseg):
   NONE
In-use files (commseg):
  /usr/CML/OStore/cache/objectstore_4_marco_commseg_5 (131104)
  /usr/CML/OStore/cache/objectstore_4_marco_commseg_2 (110608)
Call Back Queue: Empty
```

We then continued with the installation of the Nways Campus Manager for ATM components. This is what we selected.

```
                              SOFTWARE to install                            x
                                                                             x
    Move cursor to desired item and press F7. Use arrow keys to scroll.      x
        ONE OR MORE items can be selected.                                   x
    Press Enter AFTER making all selections.                                 x
                                                                             x
      #--------------------------------------------------------------------- x
      #                                                                      x
      # KEY:                                                                 x
      #   + = No license password required                                   x
      #                                                                      x
      #--------------------------------------------------------------------- x
                                                                             x
    > ahm6000                                                            ALL x
       + 3.2.0.0  8282 ATM Concentrator (PSM)                                x
       + 3.2.0.0  8285 ATM Workgroup Switch (PSM)                            x
       + 3.2.0.0  ATM Bridge Manager (PSM)                                   x
       + 3.2.0.0  ATM Manager and LAN Emulation Manager                      x
       + 3.2.0.0  Campus Manager - ATM HFC Manager                           x
       + 3.2.0.0  Campus Manager - ATM Web-Based Manager                     x
       + 3.2.0.0  English/American DynaText books for Campus Manager - ATM   x
       + 3.2.0.0  Nways MSS Server Manager (PSM)                             x
                                                                             x
```

After successful installation it should show the following modules installed:

```
ahm6000.hfc                 3.2.0.0        USR        APPLY       SUCCESS
ahm6000.books.En_US.base    3.2.0.0        USR        APPLY       SUCCESS
ahm6000.base                3.2.0.0        USR        APPLY       SUCCESS
ahm6000.atmweb              3.2.0.0        USR        APPLY       SUCCESS
```

The list below shows the complete list of software products installed:

Using the lslpp -l command we can verify our installed product list.

```
mgtapptran.book.obj        2.1.0.0  COMMITTED  Management Application
mgtapptran.obj             2.1.0.0  COMMITTED  Management Application
ostore_runtime.base        4.0.2.0  COMMITTED  ObjectStore runtime 4.0.
cml.8230                   3.2.0.0  COMMITTED  8230 Hub Manager (PSM)
cml.8238                   3.2.0.0  COMMITTED  8238 Hub Manager (PSM)
cml.8250-60                3.2.0.0  COMMITTED  8250 and 8260 Manager
cml.8272                   3.2.0.0  COMMITTED  8272 Token Ring Switch M
cml.COMM                   3.2.0.0  COMMITTED  Required common part for
cml.base                   3.2.0.0  COMMITTED  Required common part of
cml.baseLAN                3.2.0.0  COMMITTED  Required common part of
cml.books                  3.2.0.0  COMMITTED  English/En_US books for
cml.br                     3.2.0.0  COMMITTED  SNMP Bridge capability (
cml.smm                    1.1.0.0  COMMITTED  IBM Nways Campus Manager
cml.tr                     3.2.0.0  COMMITTED  Token-Ring capability (L
ahm6000.R8210s10.obj       3.2.0.0  COMMITTED  Nways MSS Server Manager
ahm6000.R8281s10.obj       3.2.0.0  COMMITTED  ATM Bridge Manager (PSM)
ahm6000.R8282s10.obj       3.2.0.0  COMMITTED  8282 ATM Concentrator (P
ahm6000.R8285s10.obj       3.2.0.0  COMMITTED  8285 ATM Workgroup Switc
ahm6000.atmweb             3.2.0.0  COMMITTED  Campus Manager - ATM Web
ahm6000.base               3.2.0.0  COMMITTED  ATM Manager and LAN Emul
ahm6000.books.En_US.base   3.2.0.0  COMMITTED  English/American DynaTex
ahm6000.hfc                3.2.0.0  COMMITTED  Campus Manager - ATM HFC
```

There are a number of log files maintained during the installation of the Nways Campus Manager ATM products. These log files are created in the directory:

/usr/CML/install_log

Also to verify the installation was successful we used the ps and ovstatus commands to check the status.

Finally we rebooted our machine and started up NetView.

2.3.7 Controlling the Nways Campus Manager ATM Daemons

The majority of daemons can be controlled directly from the TME 10 NetView interface.

Now we can check to see of the correct daemons are running. For the Campus Manager daemons issue the command:

/usr/CML/bin/cmlstatus

When NetView is started using the command nv6000 the following daemons become active:

```
Application Transporter Request Broker V.2 R.0 Port No 2485
Application Transporter System Startup: ..
Starting application: Rnvgate
Starting application: Rnvch
Starting application: Rwatch
Starting application: Rsph
Starting application: Rmibs2
Starting application: Rcomms10
Starting application: R8285s10
Common Manager for AIX V1.0.2
Starting application: R8282s10
8285 Manager for AIX V2.1.0
Starting application: R8281s10
8282 Manager for AIX V1.0.2
Starting application: Rpimserv
8281 Manager for AIX V1.0.6
Starting application: R8210s10
Nways MSS Server Manager for AIX V1.0.1
```

We also verified the management application transporter was up and running by issuing the command ps -ef | grep mgtappatran.

2.3.8 Clearing the Topology Database

There was a number of times we had to clear the Object Store database, for example, when we modified the IBM 8210 configuration. From the TME 10 NetView interface do the following:

1. Type `smit cml6k_Maint` from the AIX command line.
2. Select **Campus Manager->ATM Maintenance**.
3. From this panel select the option **Clear the Campus Manager ATM-topology**.

   This will remove the ATM topology database. We had to re-start the ATM topology daemon using the command /usr/CML/bin/cmlstart ahmtopod.
4. Next we installed Router and Bridge Manager and Mid-Level Manager.

2.4 Installing Router and Bridge Manager Version 2

This chapter describes the pre-installation requirements (including Mid-Level Manager), installation, and configuration procedures to run Router and Bridge Manager.

Router and Bridge Manager has the following disk space requirements:

- At least 60 MB of disk space for database files
- At least 30 MB of disk space for program files for the server
- At least 16 MB of disk space for Object Store cache files

Note: Although Router and Bridge Manager has been enabled to run with the client/server component of the NetView for AIX Version 4 software for our purpose we installed only the server component as we did not need to run the client software.

2.4.1 Router and Bridge Manager Installation Process

We decided to install the Mid-Level Manager component prior to installing Router and Bridge Manager due to Router and Bridge Manager installation script updating some of the Mid-Level Manager configuration parameters.

For Mid-Level Manager the package names are:

```
smcfg.eui.obj
smcfg.dtext.En_US.eui.obj
smmlm.subagent.obj.
```

When installed the daemon midmand should be running.

Now we can install Router and Bridge Manager by selecting the following package:

```
rabm                            ALL
 @ 2.2.0.0  IBM Router and Bridge Manager Server
```

The installation log file is /tmp/RabmServer.log. Also the Object Store daemon must be running and no NetView windows should be active.

For RABM you can check the processes are active by running ovstatus and looking for:

```
 object manager name: NCMPserver
 behavior:            OVs_NON_WELL_BEHAVED
 state:               RUNNING
 PID:                 46366
 exit status:         -

 object manager name: rabmEventServer
 behavior:            OVs_NON_WELL_BEHAVED
 state:               RUNNING
 PID:                 43574
 exit status:         -
```

The customization of this product is discussed in chapter Chapter 7, “Using Router and Bridge Manager Version 2.2” on page 149.

After installing Router and Bridge Manager a new SMIT entry will be generated under the Communications Applications and Services menu item. This entry name is misleading because it is called Mid-Level Manager (MLM) Definition Configuration.

2.5 MIB Definitions

The Nways Campus management applications require SNMP MIBS in order to manager the components. The sections below explain what MIBs are used.

The following MIB definition files can be found in the directory /usr/OV/snmp_mibs. We installed the MIB definitions using the command /usr/OV/bin/xnmloadmib. We loaded the MIBs below:

```
af-FORUM-TC.mib
af0044-LEC.mib
af1129-BUS.mib
af1129-ELANLECS.mib
af1129-LES.mib
af0417v40-ILMI.mib
```

These MIBs were installed to allow us to use the TME 10 NetView MIB browser on our managed ATM devices.

2.6 Additional Management Tools

In addition to the Nways Manager for AIX applications the following are two additional tools that will assist in managing our ELAN environment:

- IBM 8210 Configuration Program
- IBM 8210 Web Browser

The sections below provide a brief description of these tools.

2.6.1 IBM 8210 Configuration Program

This software can be downloaded from the Internet Web page http://www.networking.ibm.com/nes/nesswitc.htm#8210v11.

The software requires seven formatted diskettes. The instructions are also at the same location.

These tools are integrated with TME 10 NetView using smit to amend the contents of the file /usr/CML/conf/mss_profile. This file defines the locations for both the Web browser and the configuration utility.

This file should not be directly amended. To apply personal requirements to this file, issue the command:

```
smit ahm6k
```

Then select **Set MSS Server Management Tools Preferences**.

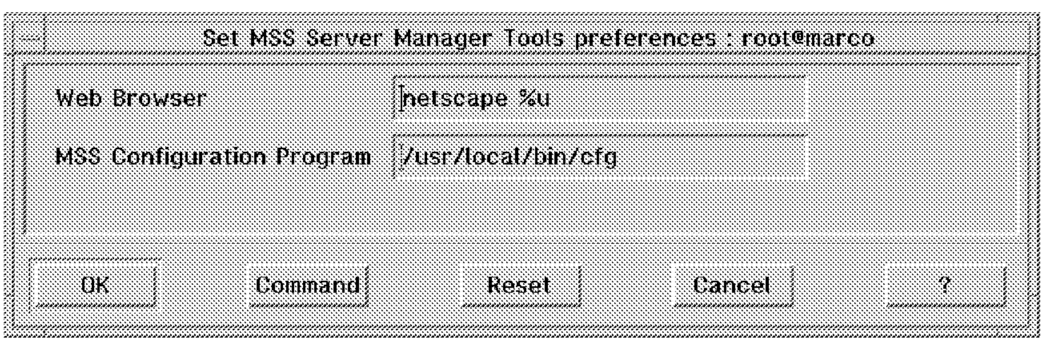

Figure 5. Set MSS Server Manager Tools Preferences

After the configuration with SMIT has been done, a file called mss_profile will be created.

To execute the tools from the NetView interface you can double-click on the **IBM 8210 PSM** icon (see Figure 6 on page 26).

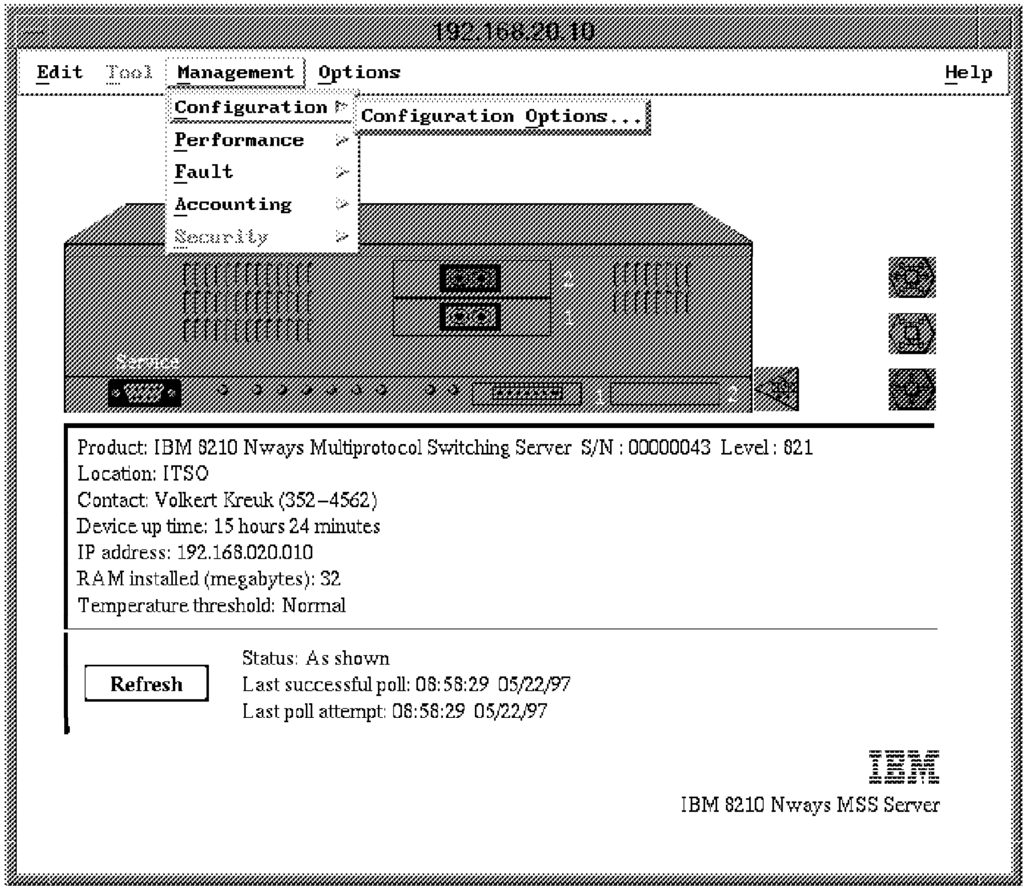

Figure 6. IBM 8210 PSM

From here you can select **Management->Configuration->Configuration Options** and Figure 7 on page 27 will appear.

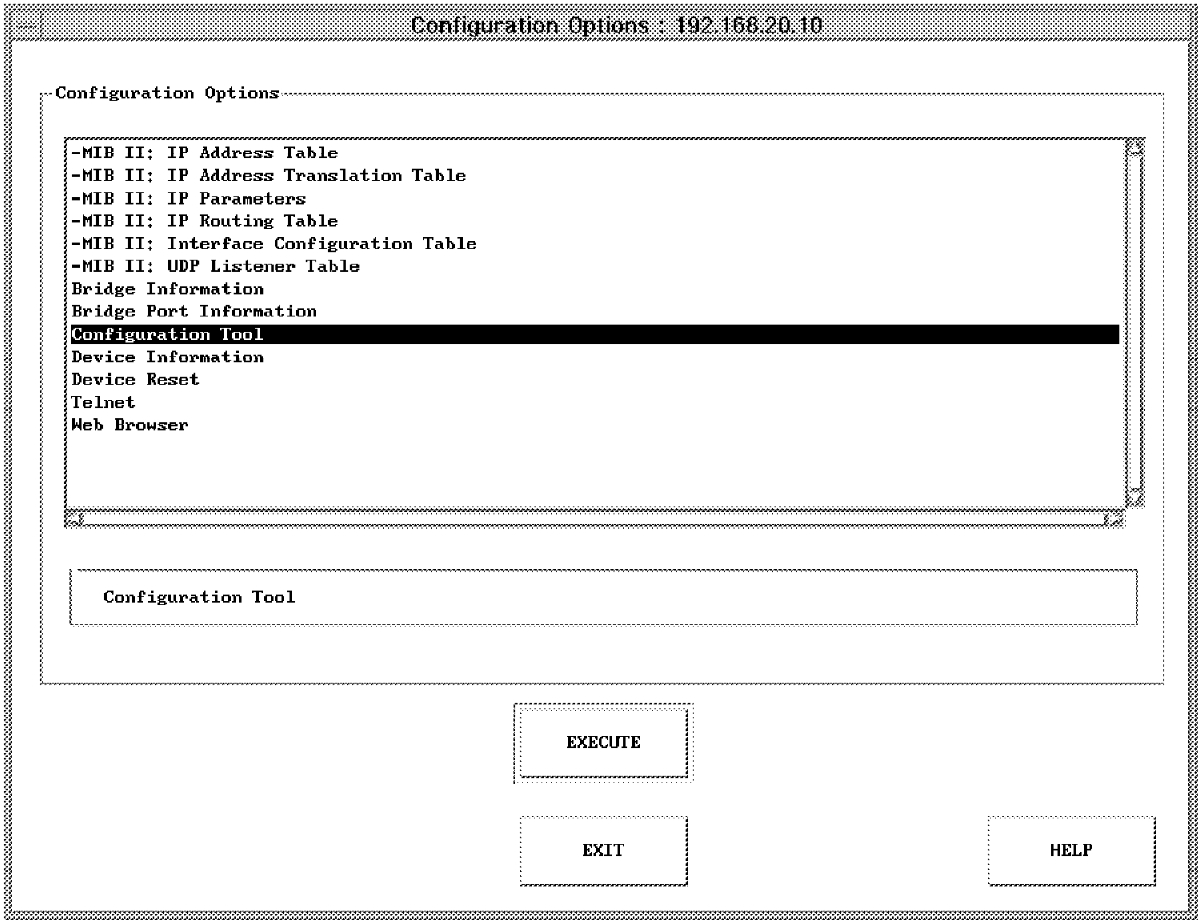

Figure 7. Executing the MSS Configuration Tool

From this screen you can select **Configuration Tool** and click on **Execute**.

2.6.2 Using the Configuration Utility

The IBM 8210 configuration must be retrieved from the device. Once retrieved, a screen similar to Figure 8 on page 28 will appear.

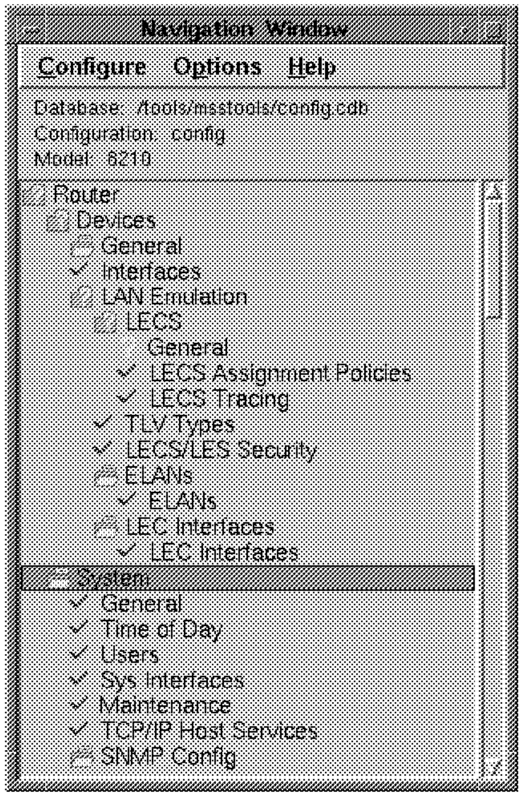

Figure 8. 8210 Configuration

If any question marks are displayed along side the items list, this means that there is a problem with the configuration (for instance a configuration field is missing).

A green check mark means that this item has been configured correctly as far as the Configuration Utility is able to check.

This indication by different icons and colors allows you to get a status overview of the configuration you are working on.

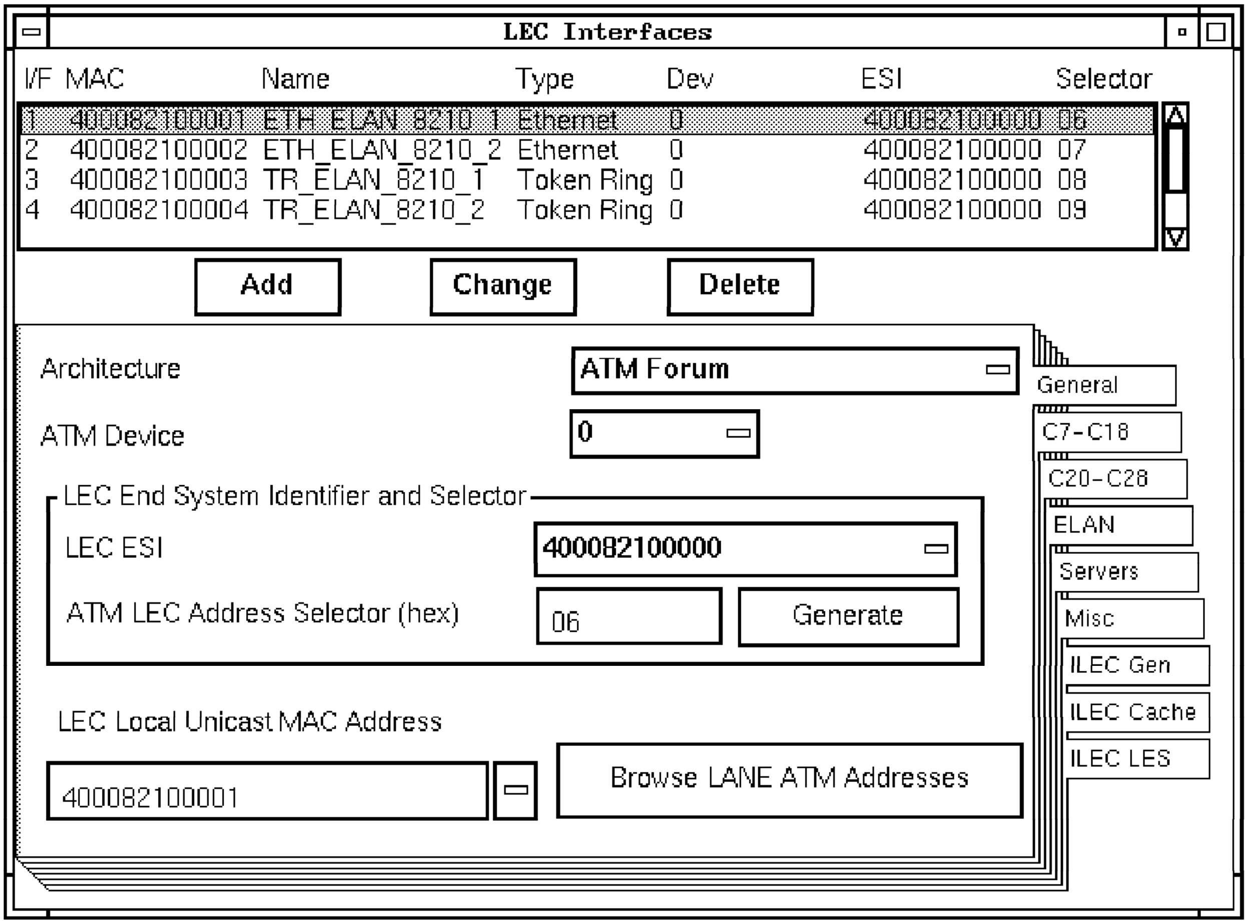

Figure 9. LEC Interface Definition for the IBM 8210

Figure 9 shows the defined LEC interfaces and their associated ESIs and selector byte values.

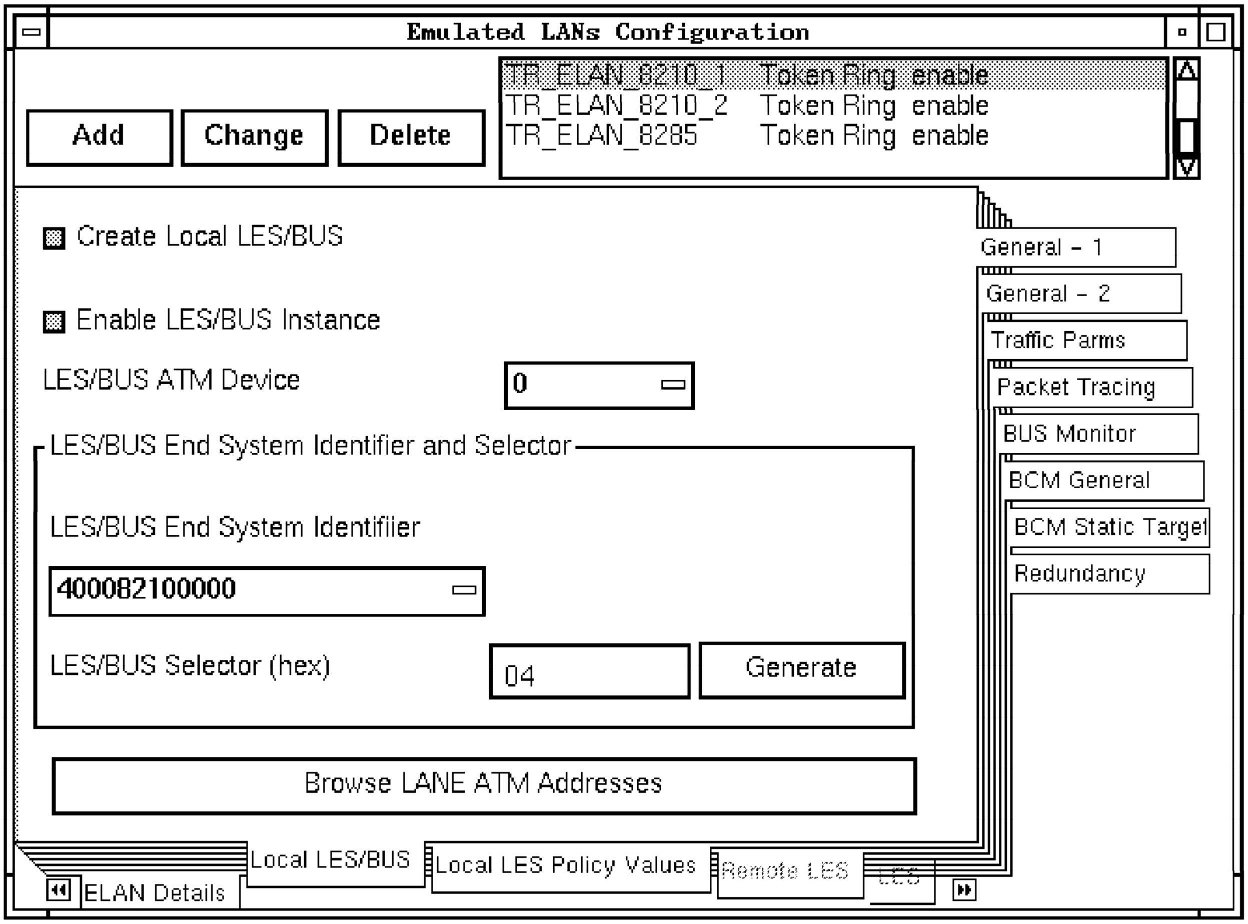

Figure 10. Emulated LAN Configuration

Figure 10 displays the defined ELAN configuration.

2.6.3 Using the Web Browser for the 8210

The Web browser interface can be accessed using Netscape from marco.

When starting the Web browser we disabled the proxy. The location is the IP address of the IBM 8210. In our case we entered `http://192.168.21.10` and then pressed Enter. This will open a window similar to Figure 11 on page 31.

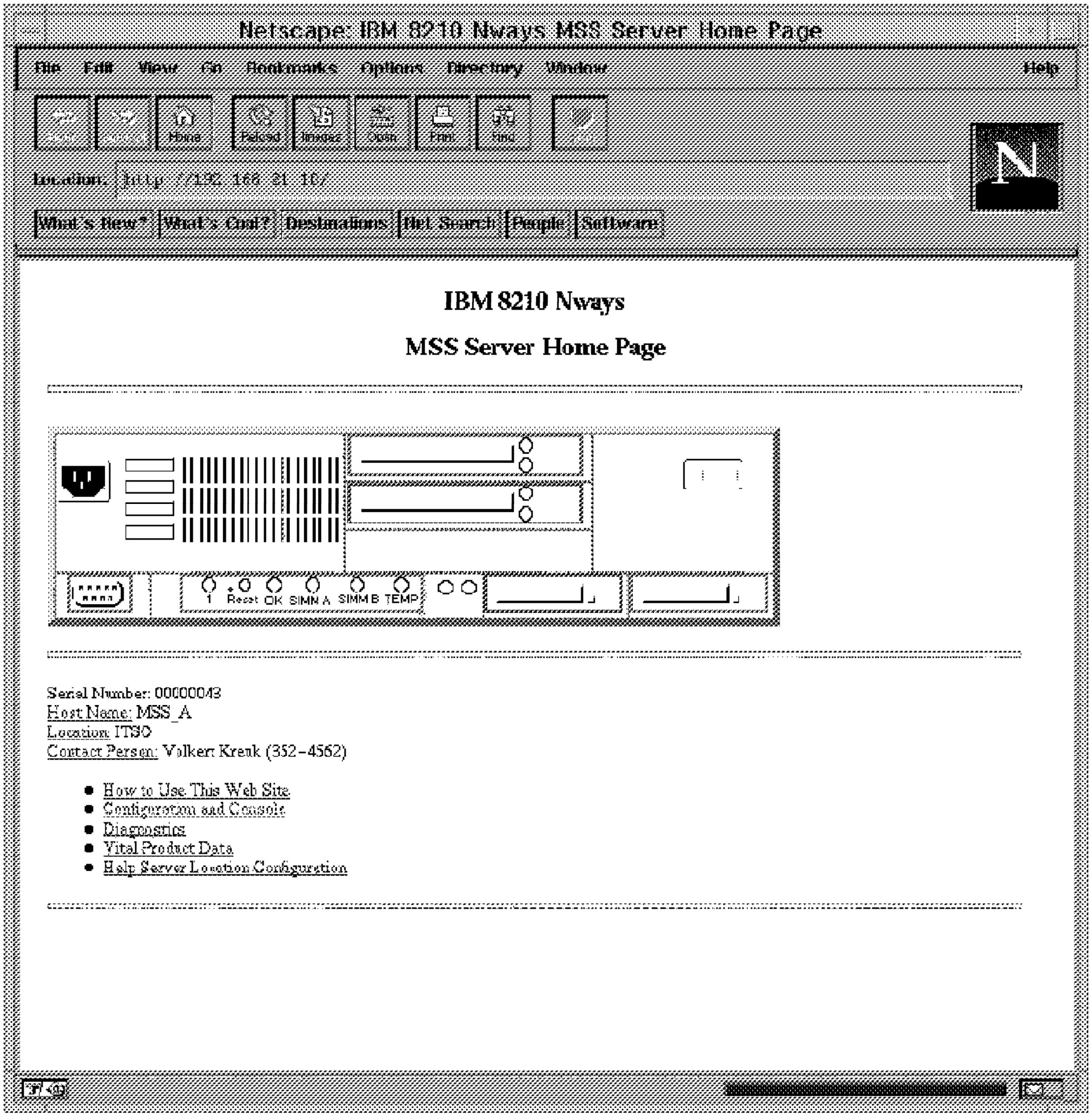

Figure 11. 8210 Web Server

For our initial configuration of the ELAN network we used the Quick Configuration option. The initial page looks like Figure 12 on page 32.

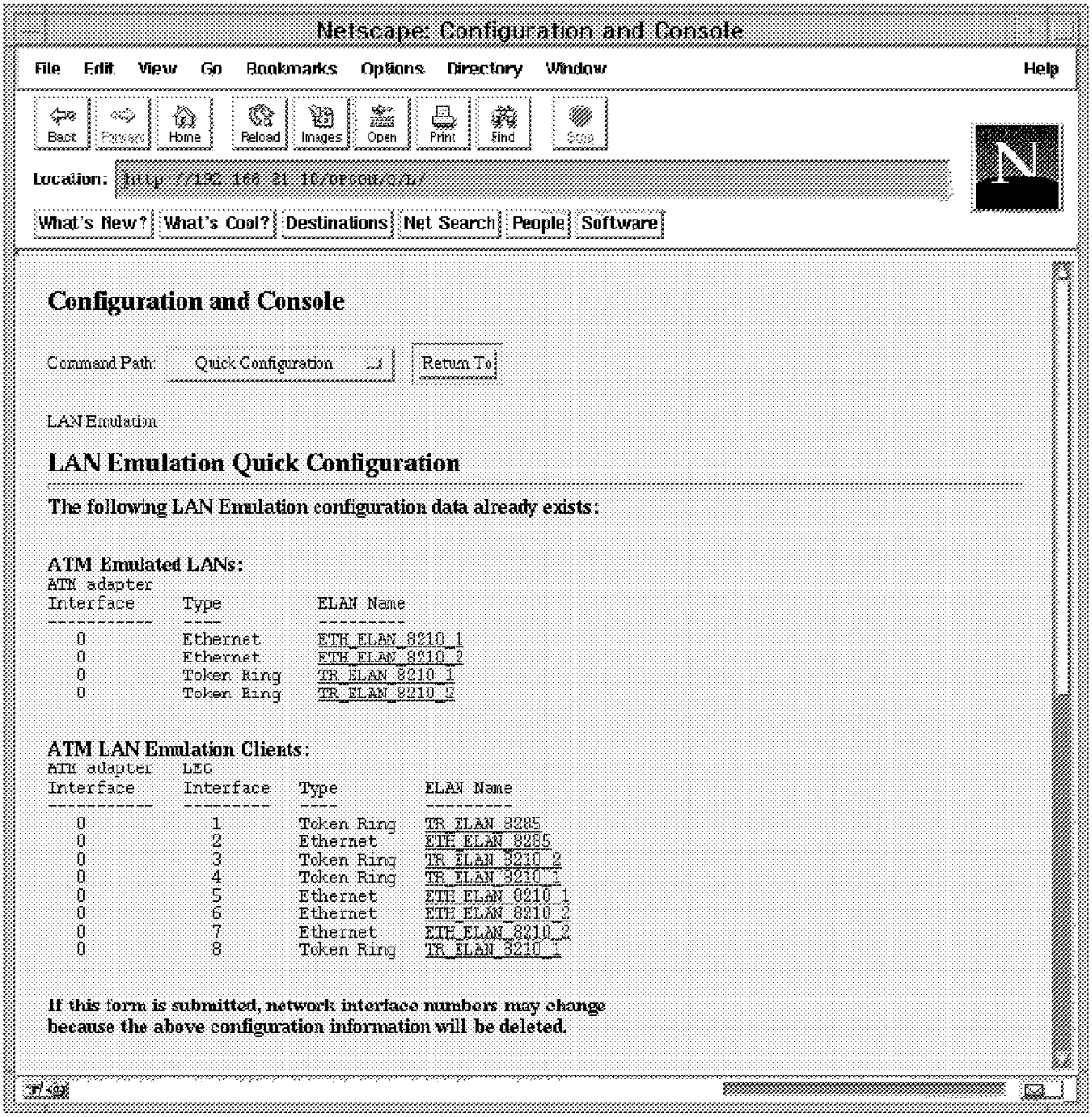

Figure 12. Quick Configuration for the IBM 8210

It is advisable to familiarize yourself with the Web browser as we found it a very useful tool for configuring the IBM 8210.

Figure 13 on page 33 shows the event logging system. We found this useful for identifying LAN Emulation problems in our configuration.

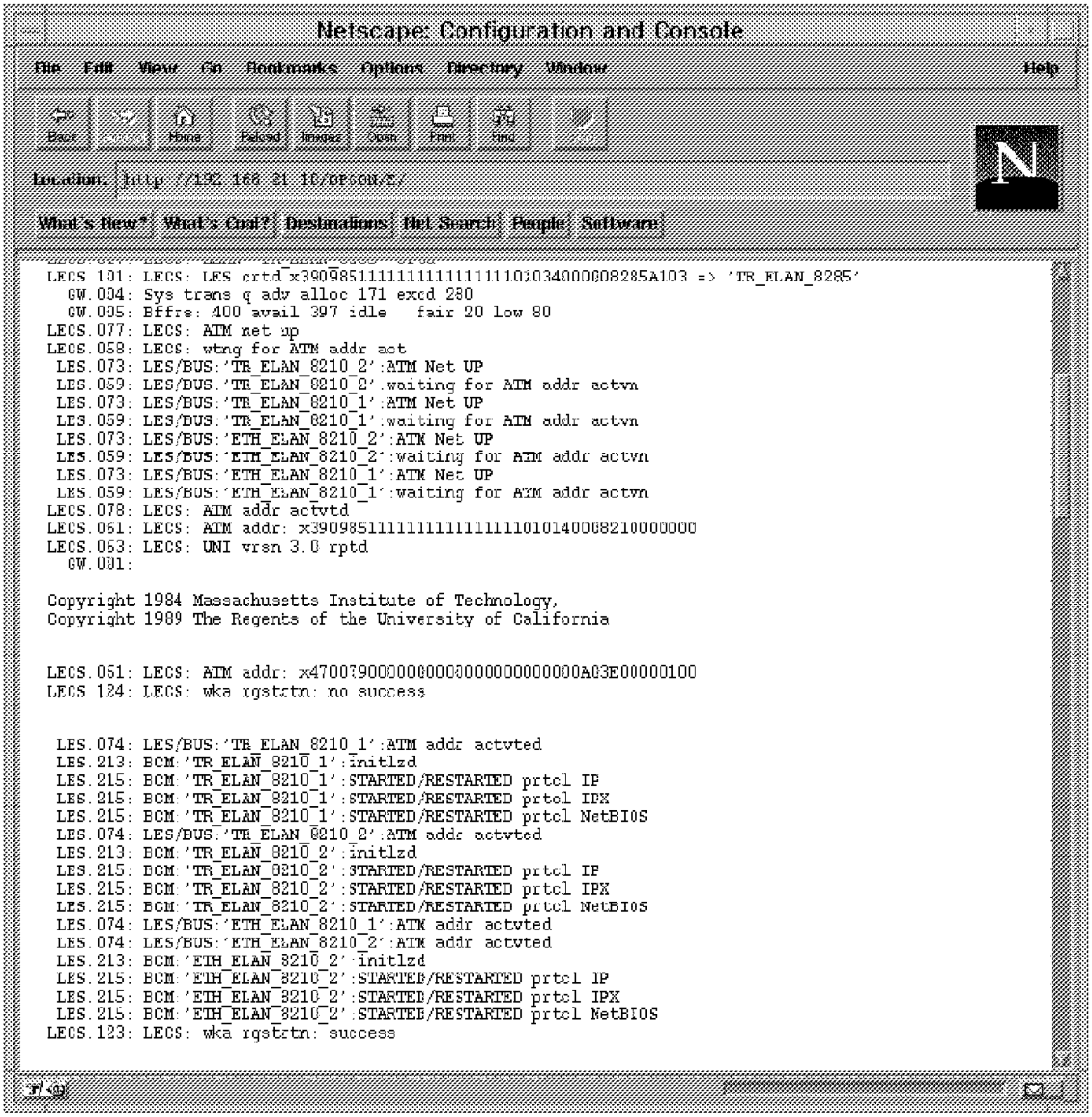

Figure 13. ELS Output for the IBM 8210

From the IBM 8210 Nways MSS Server home page you can perform both talk 5 and talk 6 functions.

Note: When making changes on the IBM 8210 using the Web interface make sure that you save and re-load the changes. There is no explicit write command at the Web browser.

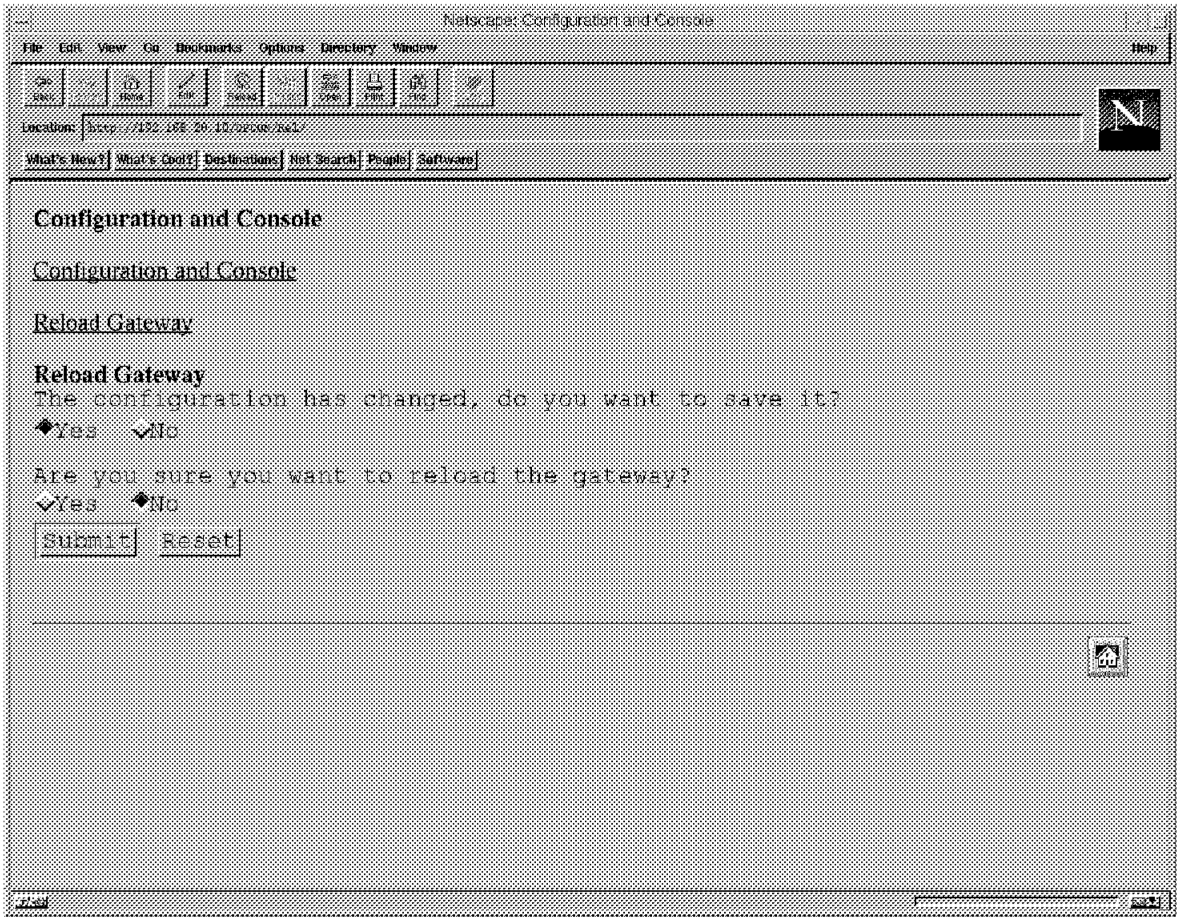

Figure 14. 8210 Reloading the Gateway

Figure 14 shows the options to reload the IBM 8210.

Chapter 3. Exploring an ELAN Network

We decided to dedicate a complete chapter to exploring our network using the tools available to us. For most, management installations take place after the network has been configured; we thought this would be a useful place to start.

For our network in particular the ELAN configuration is shown in Figure 15.

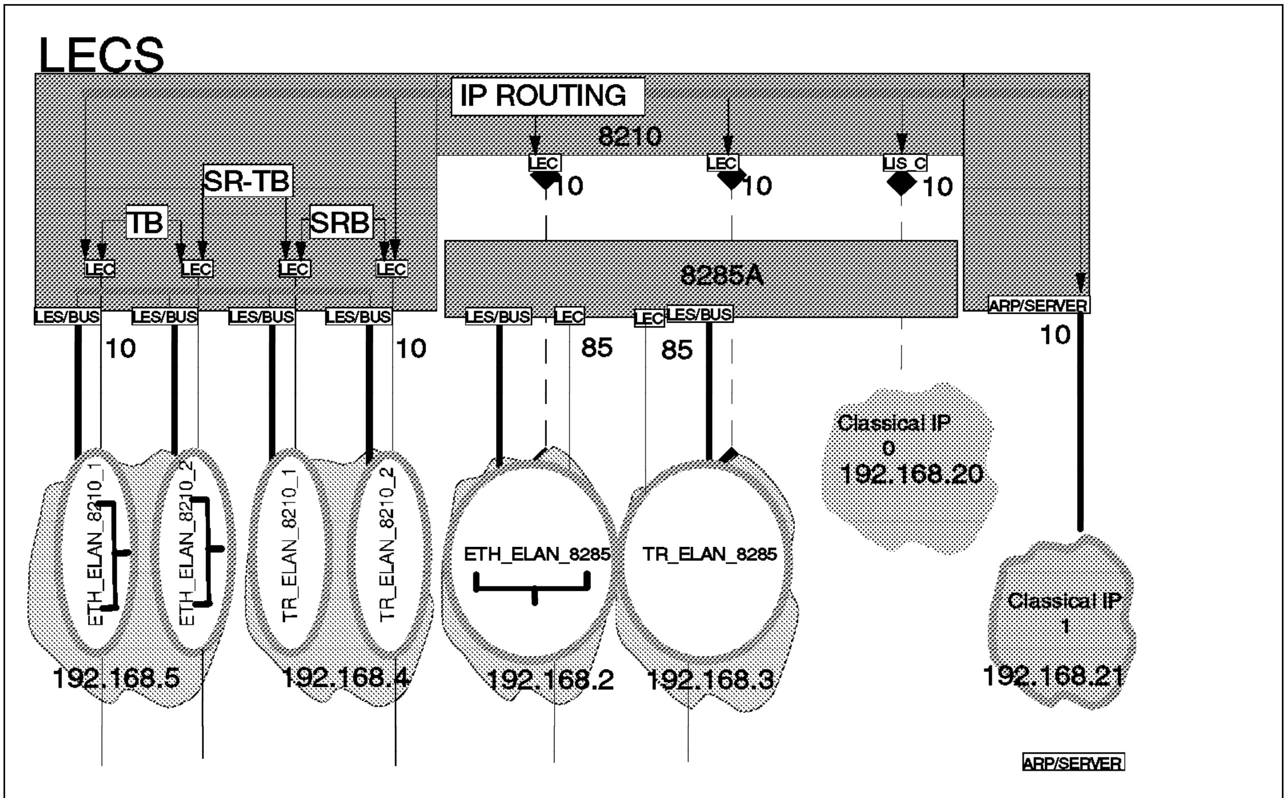

Figure 15. Our ELAN Configuration

We had six ELANs defined and two Classical IP networks. The Classical IP connections are used for management purposes only. The MSS and 8285 are depicted each having ELANs defined. In addition the MSS had a number of bridged ELANs configured.

Note: The IBM 8210 configuration guidelines can be found in the redbook *Understanding and Using the IBM MSS Server*, SG24-4915-00.

3.1.1 Our Approach

You can either begin from scratch with your network and work your way through device configuration, installation of your management software and only then describe the handling of the existing configuration and change options or you can start with an existing network. In this case you will first try to explore your network. You will probably sit in front of the different options and panels, maps and depictions and try to match the things you see with what you know about your existing network configuration. Only after this will you start making modifications and setting up thresholds and conditions that you will want to be alerted to.

Our approach was the second point mentioned. Instead of replicating the user′s guide we try to enter into a question and answer session about the network configuration. Hopefully this will highlight the features that Nways Campus Manager has to offer.

The initial starting point should be the NetView for AIX Root submap. It is the submap that opens up first, when you start the program using the nv6000 command. Since all of this installation is based on an IP network, you may first be interested in looking at your IP submaps and how far they have been affected by LAN emulation.

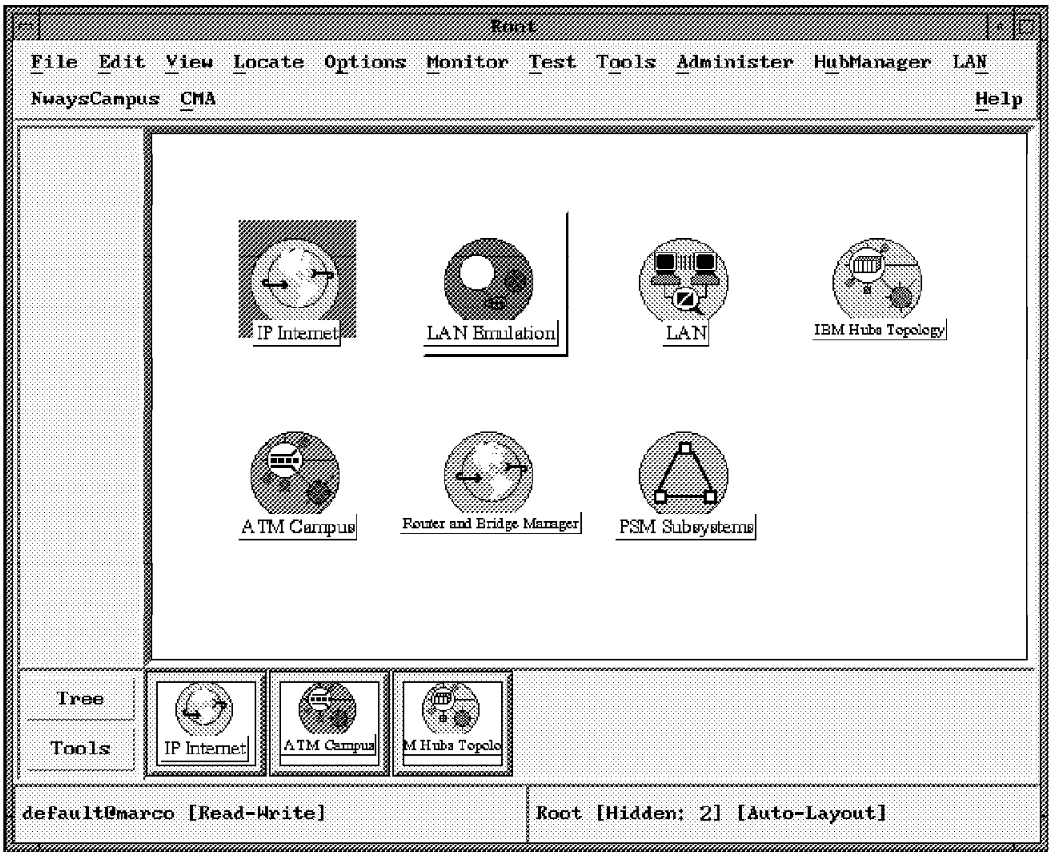

Figure 16. Root Submap

The IP network depiction is shown under the IP Internet icon of your NetView root submap. It is administered by the ipmap process, which is described in greater detail in the *NetView Administrator′s Reference Guide, Version 4*, SC31-8168-00 contained within the dynatext books that have been installed on your system.

You can read it online from the Help menu item on the main window of NetView. Since it would be beyond the scope of this book to cover every detail of NetView itself, we assume that you are familiar with these underlying principles of the program.

If you have defined your Network Management Station as a router (no -o ipforwarding=1) you will find it directly depicted on the submap which opens when you double-click on the **IP Internet** icon of the root submap. This contains all the different networks that are known to NetView, and which have been discovered by the netmon daemon. (There is a number of known complications in discovering an IP network. If what you see on your network does not meet your expectations refer to the network discovery chapter of the online documentation of NetView. Look for netmon, seedfile and demand polling). The machines netmon discovered in our network were the Network Management Station marco, some other workstations and all of our devices:

- IBM 8210 MSS Server
- IBM 8281 ATM Bridge
- IBM 8260 ATM Switch
- IBM 8285 ATM Workgroup Switch
- IBM 8282 ATM Concentrator

The IP network is shown in Figure 17.

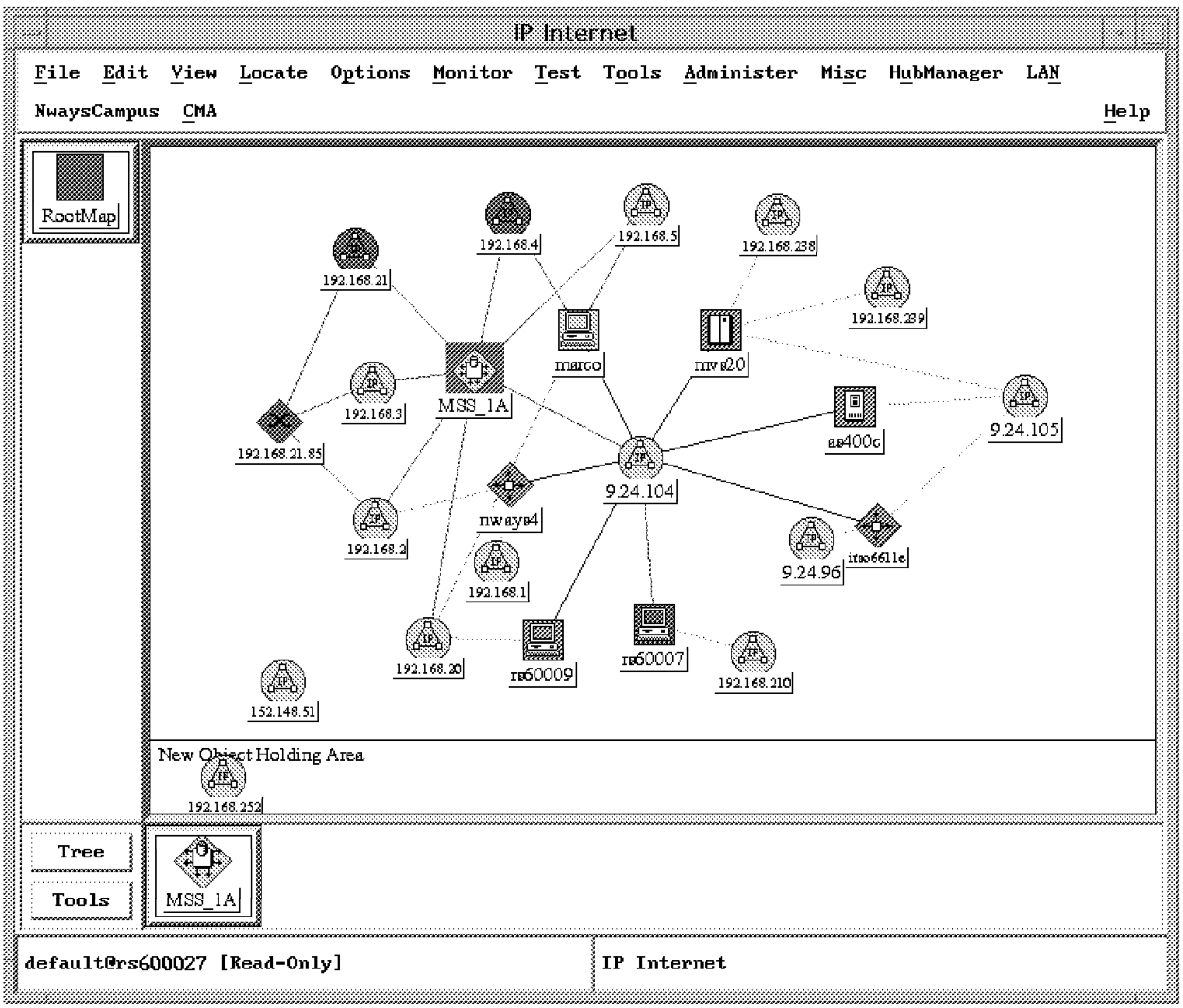

Figure 17. IP Subnet Map

This shows that our Network Management Station is connected to the legacy LAN on subnet 9.24.104 and the ATM network on subnet 192.168.

What is interesting on this IP Internet submap from an ELAN management perspective is that you do not really find any difference between IP networks that are realized using Classical IP, legacy token-ring, legacy Ethernet, ELAN token-ring or ELAN Ethernet. They all appear alike. Since the MSS is acting as a router if configured for IP management (unless you have only the host services configured for simple bridging), it should be visible with its IP addressable interfaces on this panel.

Let us focus on the MSS and the marco machine we use as our Network Management Station. As you can see from Figure 17 on page 37 marco is shown as a machine with four different interfaces. Those starting at 192.168 are emulated on the ATM card of marco; the connection to network 9.24.104.0 is from the legacy token-ring card.

Note: The connection from marco to the 192.168.20 segment is not clear from the diagram but does exist.

The actual IP address of every interface is not directly displayed. Just click on one of the connecting lines with MB3. The heading should reveal the IP address. Under the context menu shown you will also find tools->display object information which gives you some further interface information contained in the ovwdb database. Here you will also find some information about the type of the interface. Notice that the interface you select will remain selected if you change the submap you are looking at. This makes it easier to identify the corresponding interface icons and links of a station to a network.

You may find it attractive to match the interface information with the information from the command line interface. For the RS6000 you will find the following:

```
# netstat -i
Name  Mtu   Network     Address            Ipkts Ierrs    Opkts Oerrs  Coll
lo0   16896 <Link>                        159239     0   159320     0     0
lo0   16896 127         localhost         159239     0   159320     0     0
tr0   1492  <Link>10.0.5a.b1.b0.fe        147736     0   135815     0     0
tr0   1492  9.24.104    marco.itso.ral.   147736     0   135815     0     0
at0   9180  <Link>8.0.5a.99.a.b3             294     0      294     0     0
at0   9180  192.168.20  marco                294     0      294     0     0
tr1   1492  <Link>40.0.60.0.ab.4             725     0      607   133     0
tr1   1492  192.168.4   marco.itso.ral.      725     0      607   133     0
en1   1500  <Link>40.0.60.0.ee.ee           1213     0     1241    86     0
en1   1500  192.168.5   192.168.5.13        1213     0     1241    86     0
```

As you notice, there is no visible difference between the legacy token-ring interface tr0, which is based on tok0 and the ELAN token-ring interface tr1, which is based on tok1. Only if you specify an odmget command you will notice, that the emulated interface has an attribute elan_name, which of course is not the case with the legacy adapter.

```
# odmget -q"name=tok1" CuAt
 .......
CuAt:
        name = "tok1"
        attribute = "elan_name"
        value = "TR_ELAN_8210_2"
        type = "R"
        generic = "DU"
        rep = "s"
        nls_index = 13
```

You may also feel inclined to verify the information on the side of the MSS for example. Here the interfaces can be listed using the command line interface (talk 5) to enter the IP protocol environment. The interface command will show you all the IP addresses defined so far. Some interfaces may have more than one IP number.

```
# telnet 192.168.4.10
MOS Operator Control

MSS_A *
MSS_A *t 5
MSS_A +prot ip
MSS_A IP>interface
Interface  IP Address(es)   Mask(s)
   ATM/0   192.168.21.10    255.255.255.0
           192.168.20.10    255.255.255.0
   TKR/0   192.168.3.10     255.255.255.0
   Eth/0   192.168.2.10     255.255.255.0
   Eth/3   192.168.10.10    255.255.255.0
           192.168.5.10     255.255.255.0
   TKR/3   192.168.4.10     255.255.255.0
           9.24.104.115     255.255.255.0

MSS_A IP>exit
MSS_A +config
   .....

10 Networks:
Net Interface  MAC/Data-Link         Hardware                       State
0   ATM/0      ATM                   CHARM ATM                      Up
1   TKR/0      Token-Ring/802.5      CHARM ATM                      Up
2   Eth/0      Ethernet/IEEE 802.3   CHARM ATM                      Up
3   TKR/1      Token-Ring/802.5      CHARM ATM                      Up
4   TKR/2      Token-Ring/802.5      CHARM ATM                      Up
5   Eth/1      Ethernet/IEEE 802.3   CHARM ATM                      Up
6   Eth/2      Ethernet/IEEE 802.3   CHARM ATM                      Up
7   Eth/3      Ethernet/IEEE 802.3   CHARM ATM                      Up
8   TKR/3      Token-Ring/802.5      CHARM ATM                      Up
9   TKR/4      Token-Ring/802.5      CHARM ATM                      Up

MSS_A +
```

Using the config command you can also see if all the interfaces for these IP addresses are up, or if any of them have problems. For a more detailed explanation of the command output refer to the *MSS User′s Guide*, SC30 3820.

Exploding one of the icons representing an IP network you will notice, that there are segments displayed. Some devices that are normally able to connect different segments of a network will be displayed on this submap too. But although the picture may suggest this, this submap does not intend to be a topological representation of the underlying network your IP net is based on. What is really being depicted here is a collection of all such machines that share the same interface type.

TME 10 NetView reads the ifType object from the SNMP data of every device and groups the devices accordingly. Due to the fact that any interface type that is not known to TME 10 NetView defaults to the Ethernet symbol, you may see some emulated or Classical IP LAN represented by an Ethernet symbol.

Notice that the name or IP address used as a label for the device symbol does not mean that the device was detected on this interface and is being talked to via it. If a device has a number of interfaces, you may be able to ping it from your Network Management Station and still not get a response back using the test->demand poll operation, since the device was discovered (and is now being talked to) using another interface than what was given as its label.

3.2 Looking at the Underlying Structure of Your ATM Network

Now that we have discovered the IP layer of the network, our next step is to investigate the underlying connections of our ATM network. We can access it from the ATM icon in the Root submap. It will explode into a display of all the clusters that our network consists of.

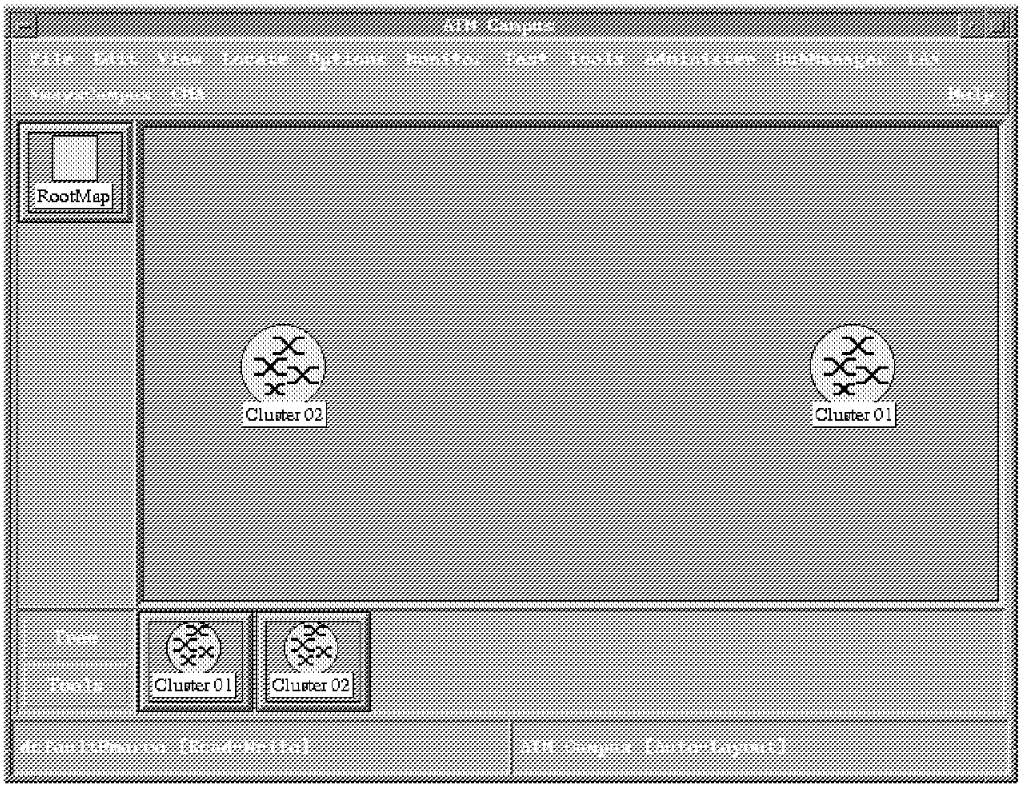

Figure 18. ATM Clusters

3.2.1 How Are the Clusters Connected?

If we want to see the connections we have between these clusters, Nways Campus Manager ATM does not really have an answer to this question. We also could not find that information reflected in any MIB, which is probably why it was not depicted. There is a chance of identifying some public interfaces on the list of interfaces given in Figure 22 on page 44 but unfortunately this does not reveal the destination of that interface. It is just a hint at a possible IISP link between two clusters. There is a panel specially dedicated to logical links, which is accessible from the list->logical links menu item on Figure 23 on page 45 but this panel only gives some information about the timer values of the logical links established on an interface. It does not mention the cluster number that a link leads to. So the only effective source of information we found here was indeed the command line interface of the 8260, from where you will find:

```
Welcome to system administrator service on 8260A.
8260ATM1>
telnet> mode character
show logical_link all
 Port Vpi Acn Side Mode Sig Traf  Bwidth Status              Index
--------------------------------------------------------------------------------
13.01   5  02 user enab 3.1  ANY   50000        UP            1

49 entries empty
```

3.2.2 What Are the Nodes in Our Clusters?

Double-click on the icon representing a cluster on the ATM submap and it will explode into a cluster submap like in Figure 19.

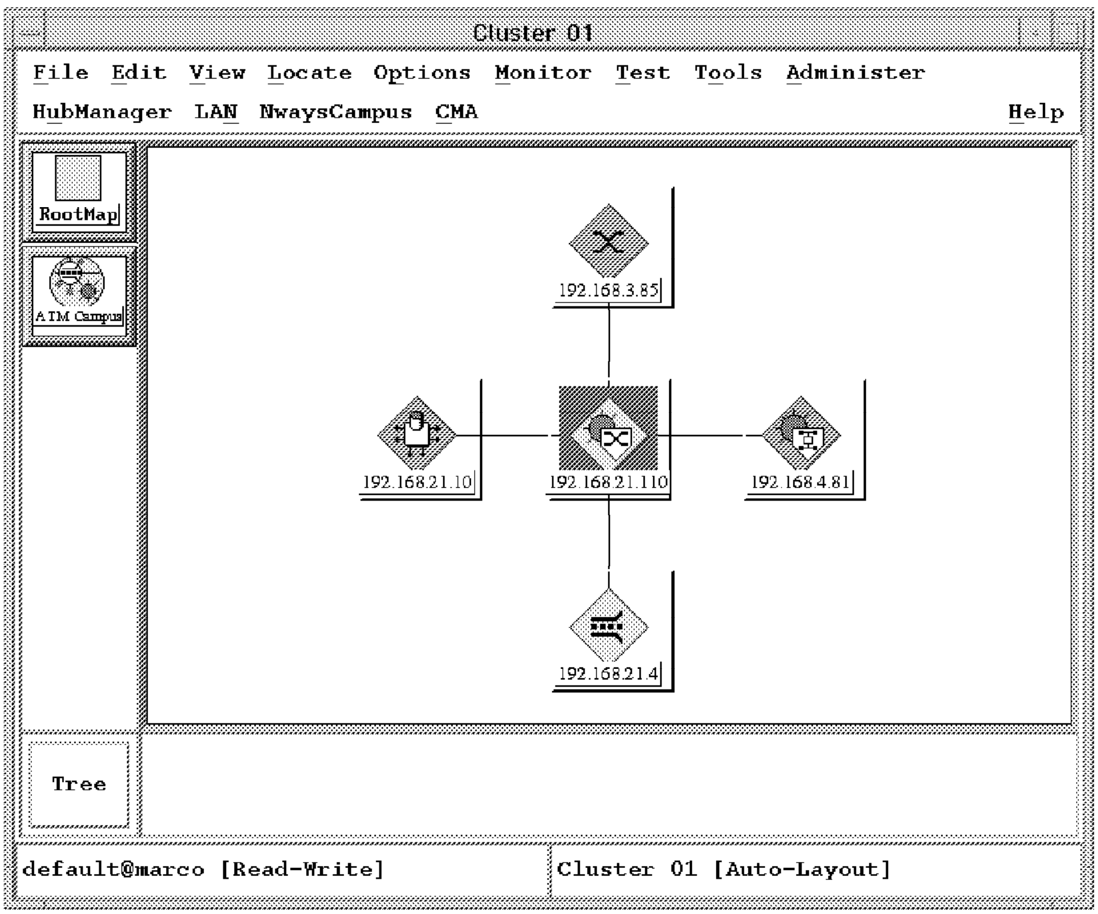

Figure 19. ATM Nodes in Cluster 01

From the symbols you can tell if the device being shown is a switching node, a concentrator, an MSS or a bridge. Aside from the pictures you find in Figure 19, there is more information shown under the help->legend menu item of the main window.

In addition you find the name or IP address as a subscription, which should give you a clue as to what you are looking at. You may notice, that all of the icons are executable now. But unlike the previous versions of Nways Campus Manager ATM a double-click on a node does not take you to a PSM if it is executable from here, but rather to the corresponding ATM View of this device seen in Figure 20 below.

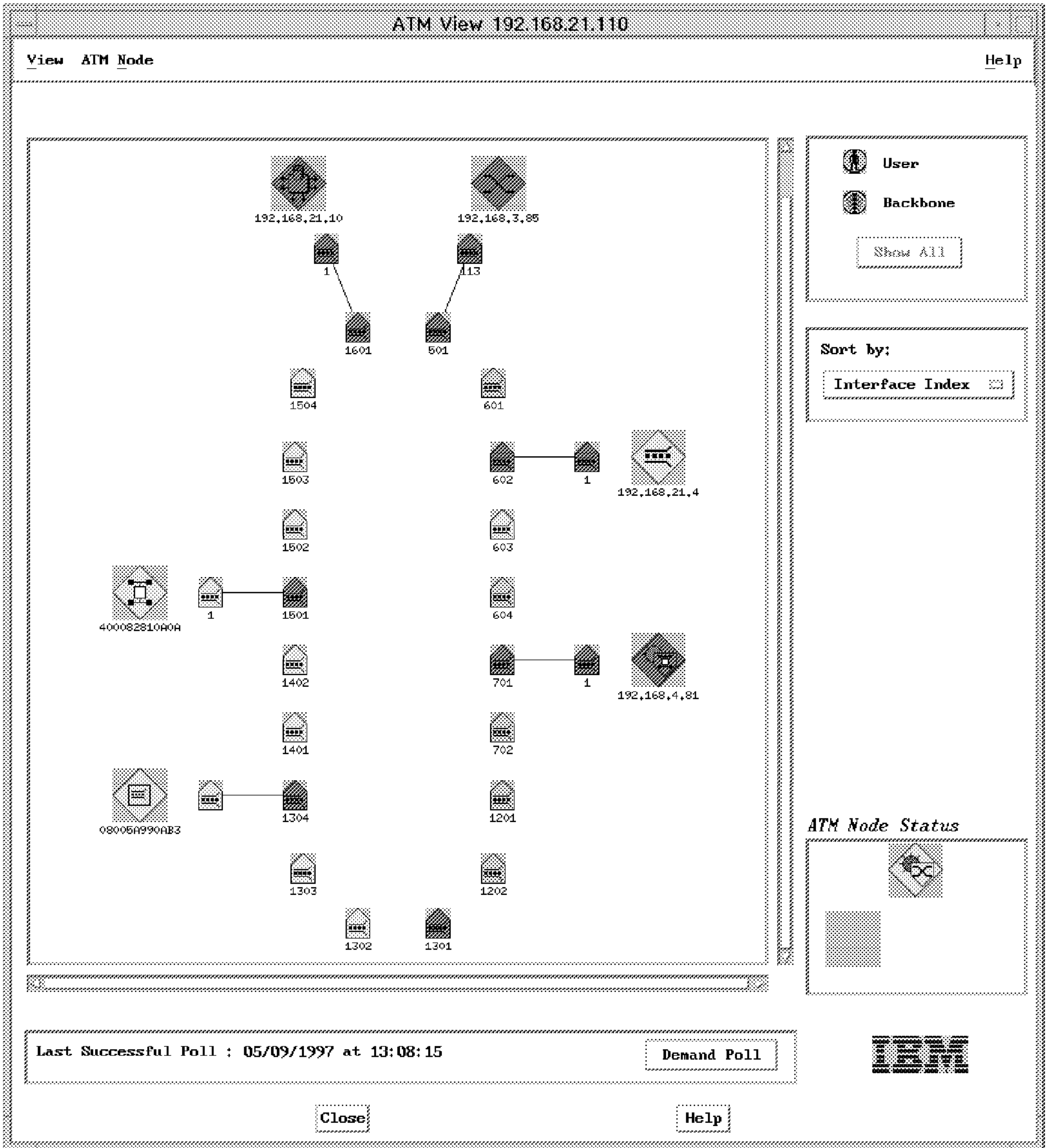

Figure 20. ATM View of ATM CPSW

The ATM View panel we are now looking at is something like a global control panel for a single ATM node. From here we can do some exploration of the node's different interfaces and attached devices. The picture on the right is giving us the known network connections. You can toggle this depiction from a star to a line-by-line or character mode display the information it gives remains the same. Figure 21 on page 43, which shows how you can display specific information for the selected node. Some elements from the menus are only selectable for switched nodes.

For such devices that have a PSM associated with them, selecting the **ATM node->device** entry will open this screen. There is other ways of starting these product-specific modules, notably from the PSM subsystems submap on the Root submap. But this way is a convenient shortcut.

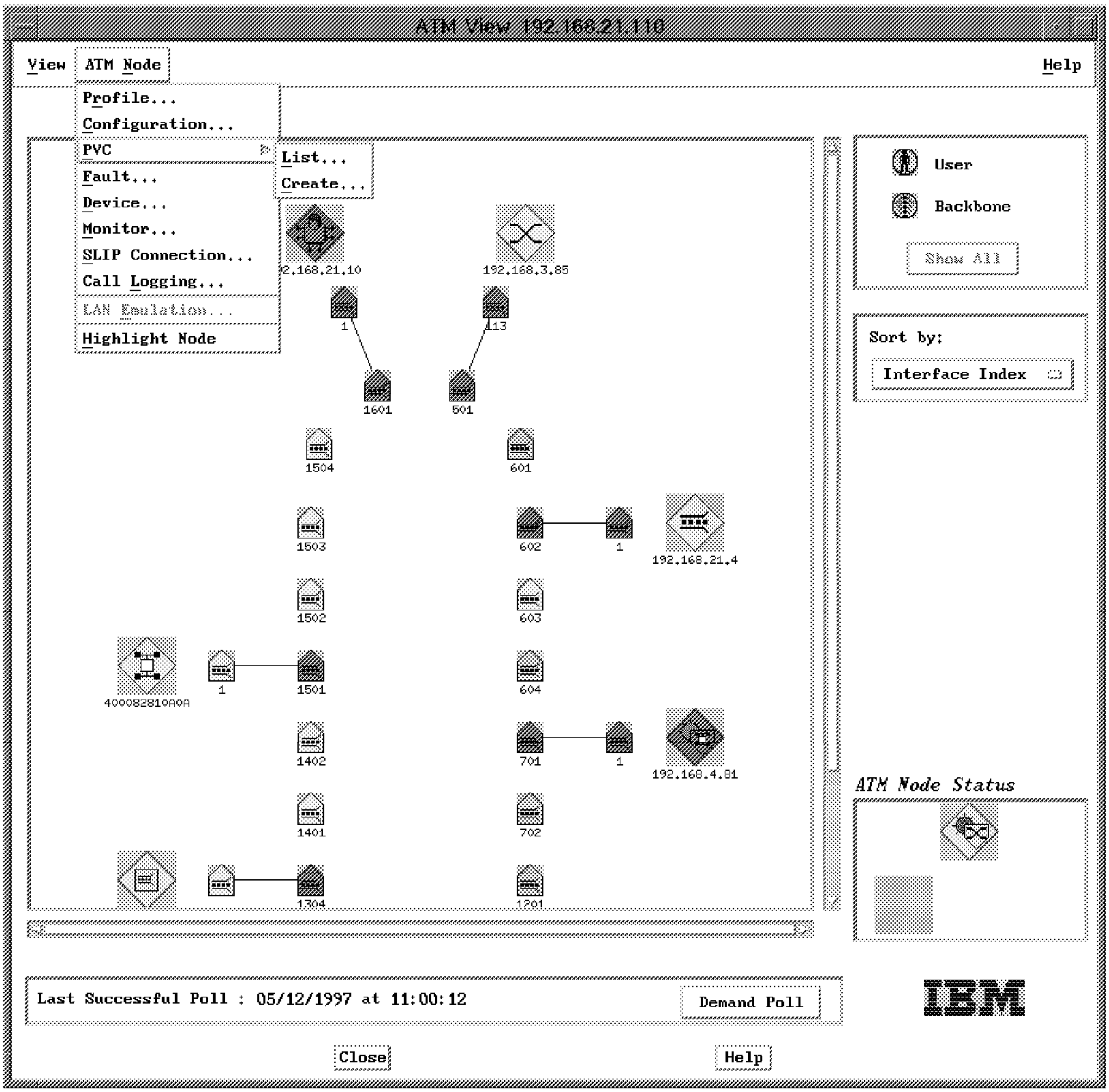

Figure 21. ATM View with ATM Node Menu

The User and Backbone buttons in the upper right of this window help in identifying the UNI and SSI connections you have specified. However, the backbone will not show those interfaces that have an IISP interface defined. You can look at what interfaces are green, yet they do not show up as user nor backbone interfaces. These interfaces are likely your network IISP links.

In the lower right corner, you find some of the ATM Node menu items replicated as an icon.

3.2.3 How Do We Best Navigate between the Nodes ESIs and IP Addresses?

Looking at the cluster submap in Figure 19 on page 41 and the configuration given either the ATM View (Figure 20 on page 42) or the ATM switch configuration (Figure 22) you will notice that the most natural identification of a node or device in the ATM world is the ATM address (or the ESI portion of it respectively). From a management point of view we are mostly working with IP addresses.

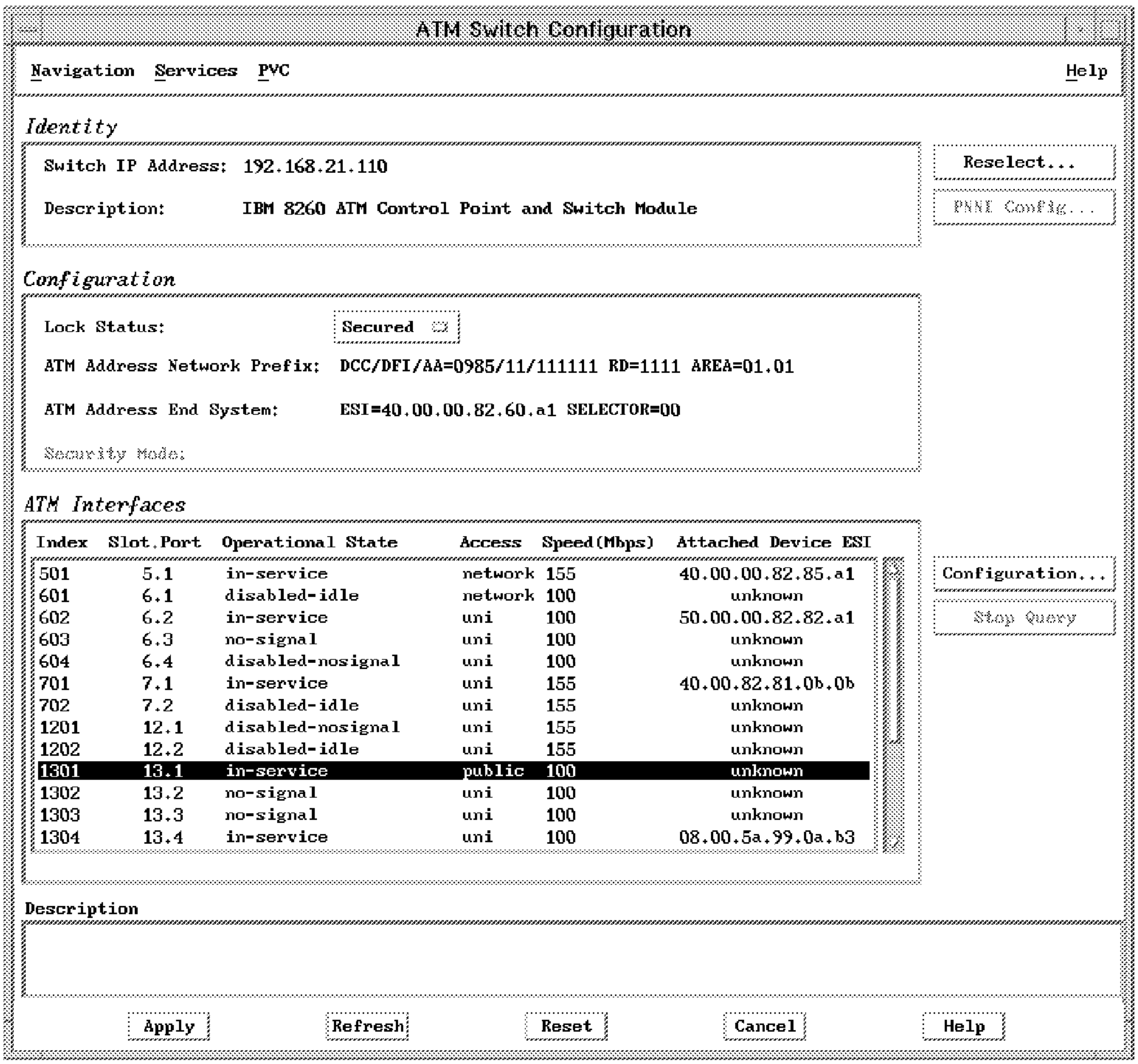

Figure 22. ATM Switch Configuration

The ATM Interfaces list on the panel above gives only the type of interface defined on a specified slot/port number and the ESI of the device that is directly attached to it. If the connection is an SSI connection (that is, the type of interface reads network in the ACCESS column of this table), the ESI belongs to the CP of the switch behind this SSI interface. In case of a UNI interface, there is the ESI of the corresponding device given in this column.

Note

We saw that in case of a UNI interface with more than two ESIs, there i s only the first ESI given in the list of the ATM Switch Configuration panel. You can use the telnet session and look at the output of the show atm_esi all command, to make sure you have all the information you wanted.

One way to match these two different representations is by selecting the interface on Figure 22 on page 44 and clicking on the **Configure** button. This will open up the panel in Figure 23.

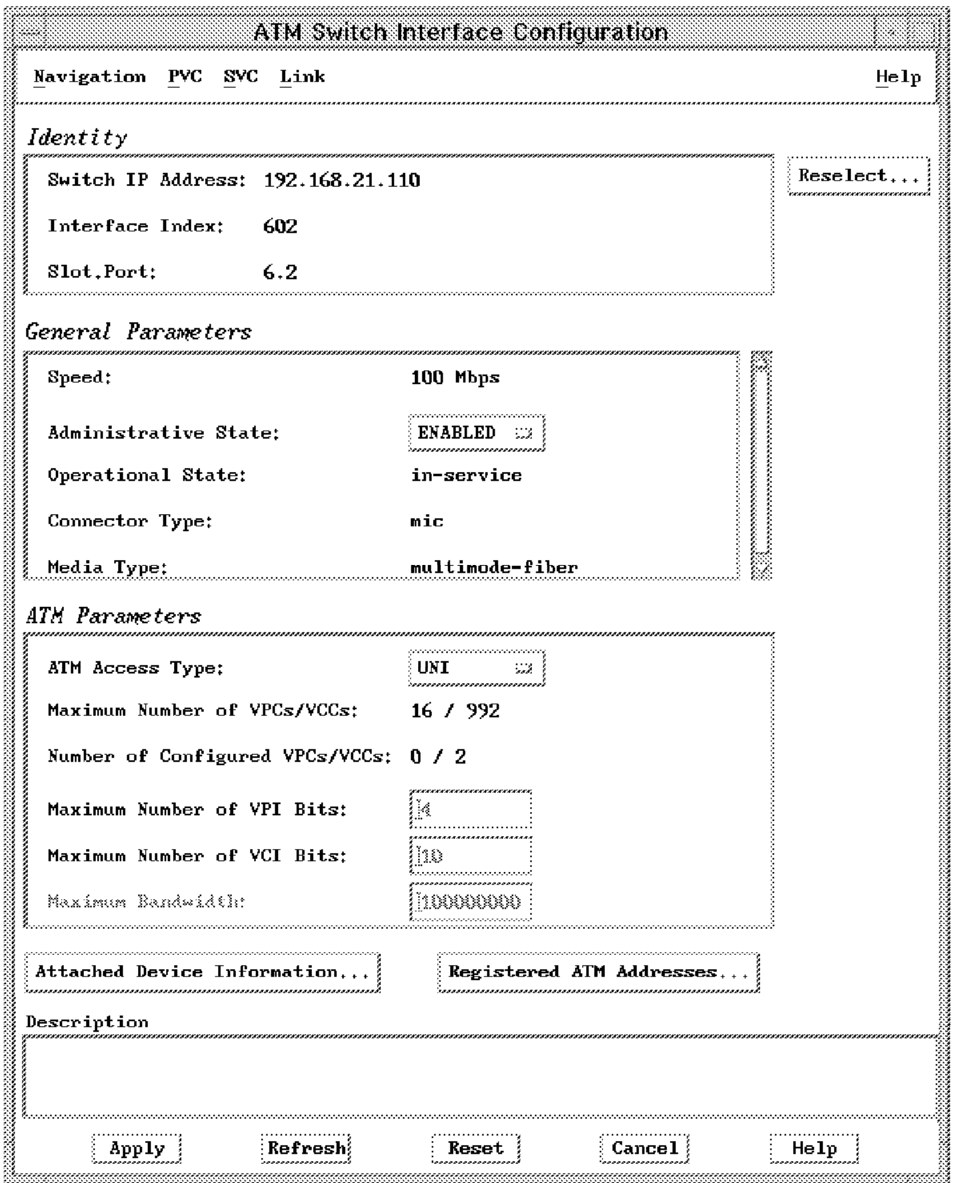

Figure 23. ATM Switch Interface Configuration

Attached Device Information on this panel will take you to Figure 24 on page 46 which has the IP address in the Configuration box at the bottom.

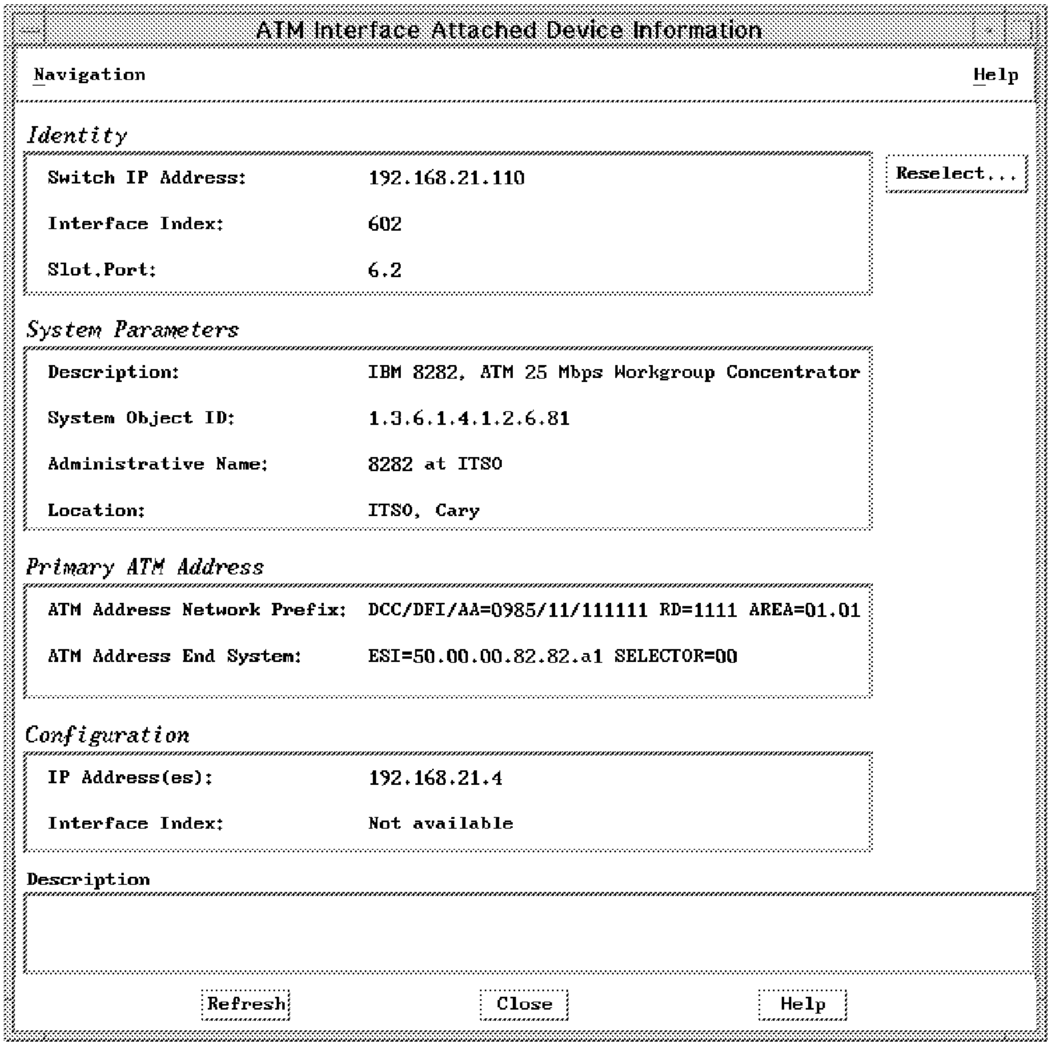

Figure 24. ATM Interface Attached Device Information

However, we have seen panels on which this information was not available. One other way is by taking the Interface index from the ATM interfaces list in Figure 22 on page 44 and looking at the symbol in the preceding panel (Figure 19 on page 41). For all the devices that are accessible you should find the name given here (which can be the devices IP address) or you can go one panel back and look at the cluster submap in Figure 19 on page 41. The Protocol option in the context menu (MB3) will show you all the different IP addresses found for this device. For simple ATM end systems such as our Network Management Station both ways may not work however, since only the ESI is given on panel Figure 19 on page 41 while they do not show up on the cluster submap. In this case turn to the NwaysCampus->search function of the main window menu. It will open the panel in Figure 25 on page 47 which holds a number of different entries to relate the different representations of a station to each other.

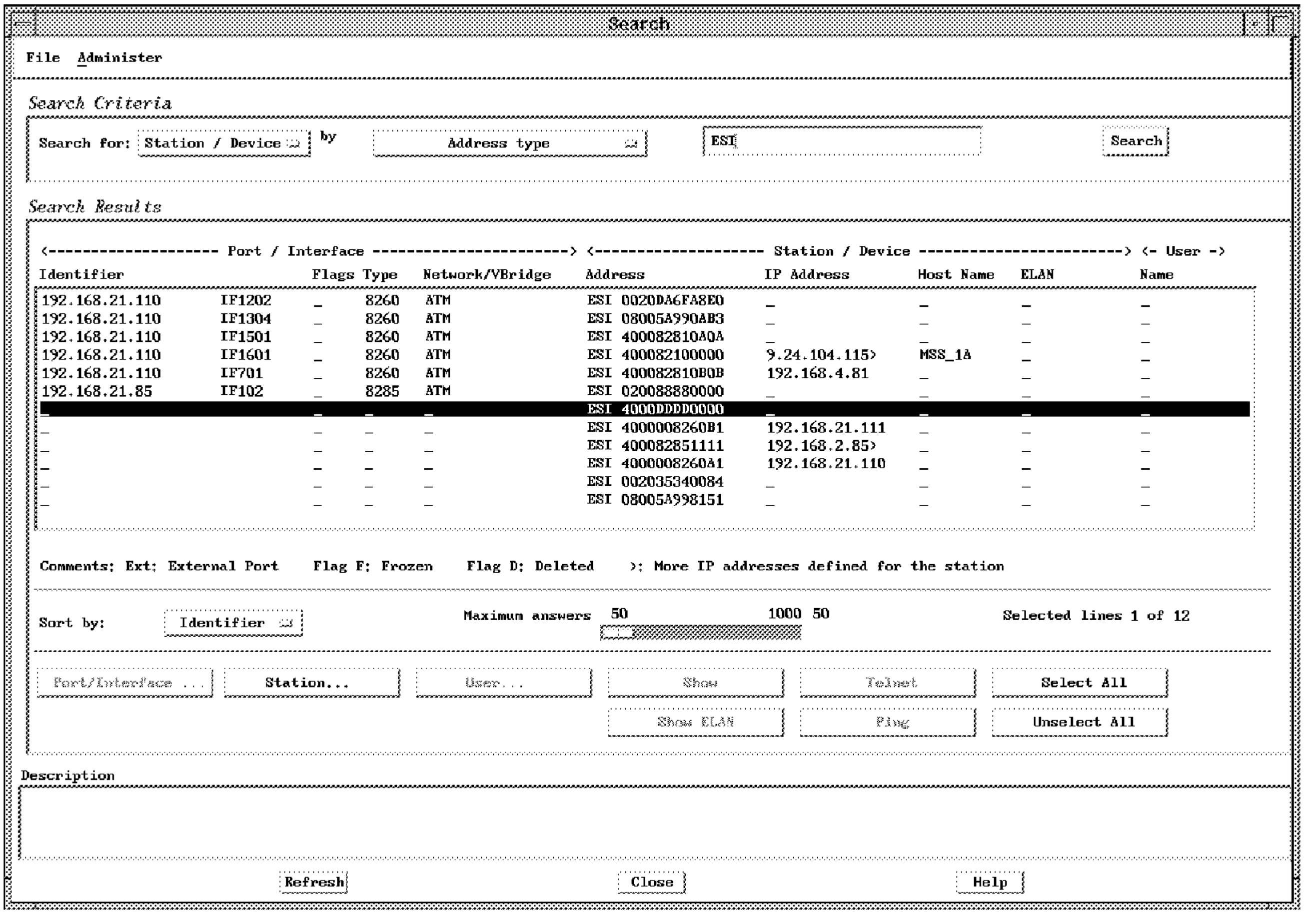

Figure 25. Search Application Panel

It uses the data stored in the Object Store database to present you with the missing parts of the information (if available here).

3.2.4 What Is Shown about the Physical Connections of ATM Devices?

The lines connecting the nodes in Figure 19 on page 41 do not reveal much information if double-clicked on, but if you select the **CMA->Configuration** option of their context menu, it will take you to an ATM Connection Configuration panel, that may serve as a convenient shortcut to the panels holding the node configuration data. In addition some information concerning the physical links is contained in this panel too like the available and maximum bandwidth on this connection.

3.2.5 What about the ATM Connections in the Network?

There are two different types of connection in an 8260-based ATM network. You can either have permanent virtual circuits (PVCs) or switched virtual circuits (SVCs). Although an in-depth explanation of all of these ATM elements would be beyond the scope of this redbook there is a brief explanation in the appendix.

You can list the PVCs from the **ATM Node->PVC->List** menu items in Figure 21 on page 43. This opens the list below for you.

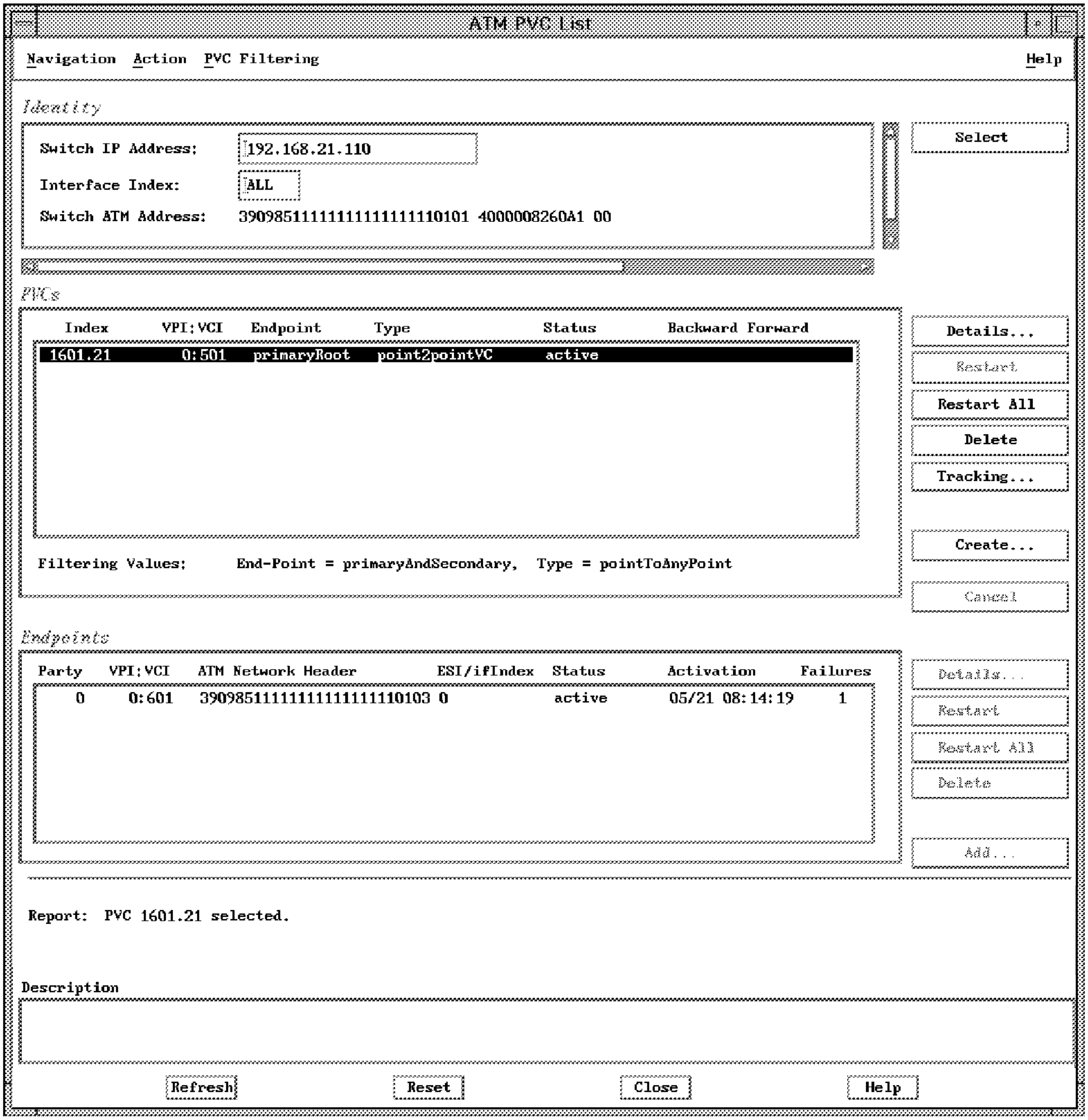

Figure 26. The ATM Node Menu

What you can see in Figure 26 is a complete list of PVCs for this node. If you want to see the PVCs listed by interface, you can also open the list for a specific interface. However, you should notice that this list only shows the PVCs that are ending or beginning at this interface. Even if a PVC is taking its path through an SSI interface, you will not find it listed on the corresponding interfaces PVC list.

PVCs will occasionally be found in networks running Classical IP, since using them permits setting aside reserved bandwidth for these connections. However, they are not a very flexible way of handling a network. You can use Nways Campus Manager ATM to set up a PVC connection. As can be seen from Figure 27 on page 49 all the controls are there to set up a PVC connection from any point of the ATM network to any other endpoint. Nevertheless we only succeeded in defining PVCs inside a single cluster (as a single definition).

Hence, if you want to set up a PVC across different clusters, make a definition in each cluster, and make sure the specifications of your VPI and VCI values match at the cluster boundaries and are consistent with the VPI value mentioned in the set logical_link definition for the links between the clusters.

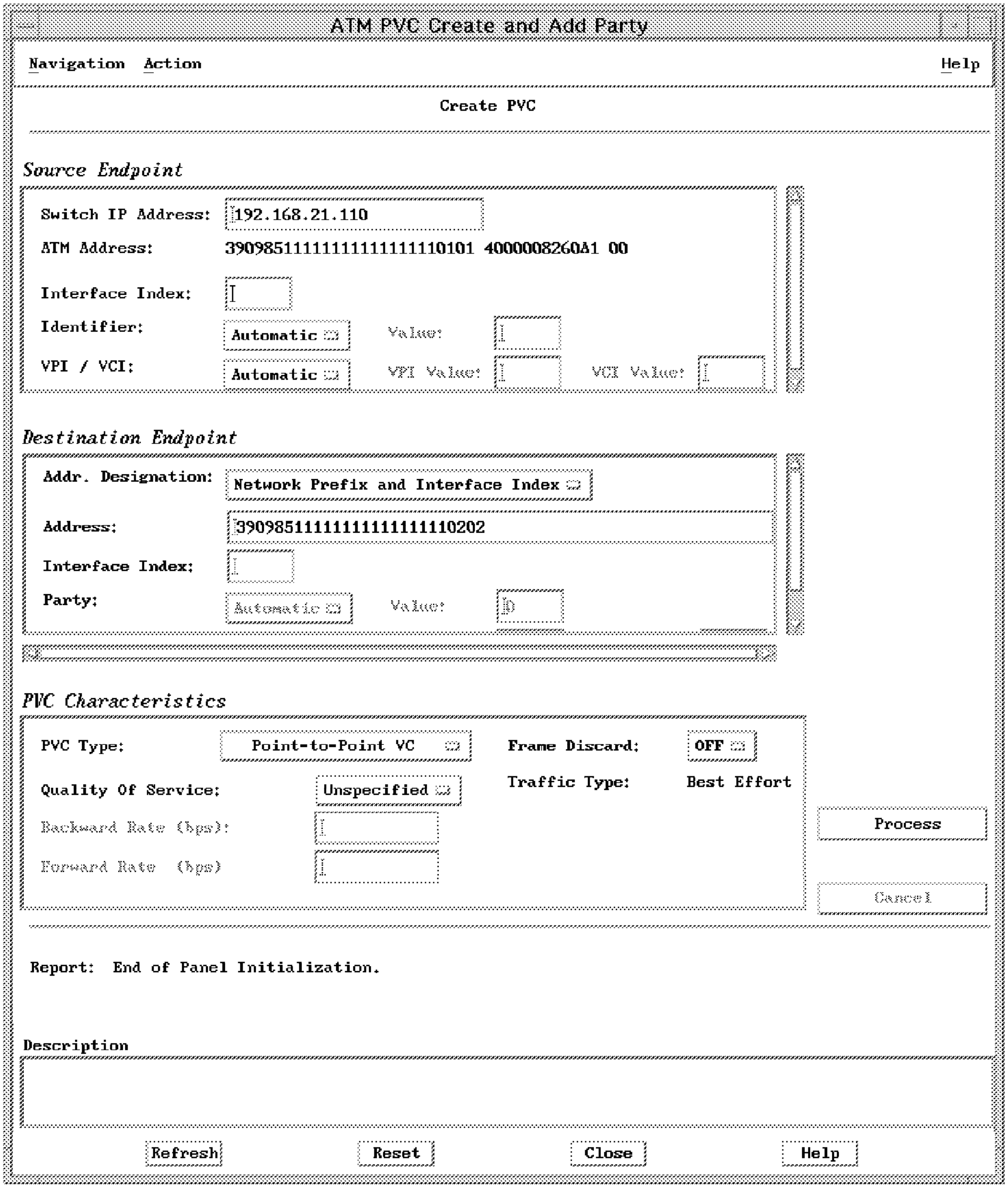

Figure 27. Create PVC

Why are PVCs of interest in an ELAN environment anyway? Most of the functions accomplished by the service entities of an ELAN are using SVC connections through the ATM network. Still with RFC 1483 a way of bridging across an ATM PVC connection based on an ATM interface has been defined, which allows you to connect the MSS 8210 to the VLAN world of an 8273/74. But aside from this, PVCs are only used in the Classical IP world. If you want to follow a PVC connection through a network, not just identifying the starting and ending point of the connection, you can use the PVC tracking function for this. Your display will look like what you see in Figure 30 on page 53, showing you the different VPI and VCI numbers used to set up the connection through your network.

While PVCs are set up manually (that is, by manual specification of the required information using command line or Nways Campus Manager ATM interfaces) SVCs are a part of the dynamic network configuration. They are set up by an ATM end system, which identifies the other side of the required connection using its ATM address. The underlying process of signalling is based on one specific type of interface which can be UNI 3.0 or UNI 3.1 with the current implementation of ATM on the 8260. LAN Emulation is based on the establishment of such SVC connections by the logical entities that constitute an emulated token-ring or Ethernet network.

In order to find the SVC connections for LAN Emulation entities turn to the panel opened by the **SVC->List** menu options of the ATM Switch Interface Configuration panel. As you can see on Figure 28 on page 51, all the SVCs belonging to this interface are shown in the SVC List table.

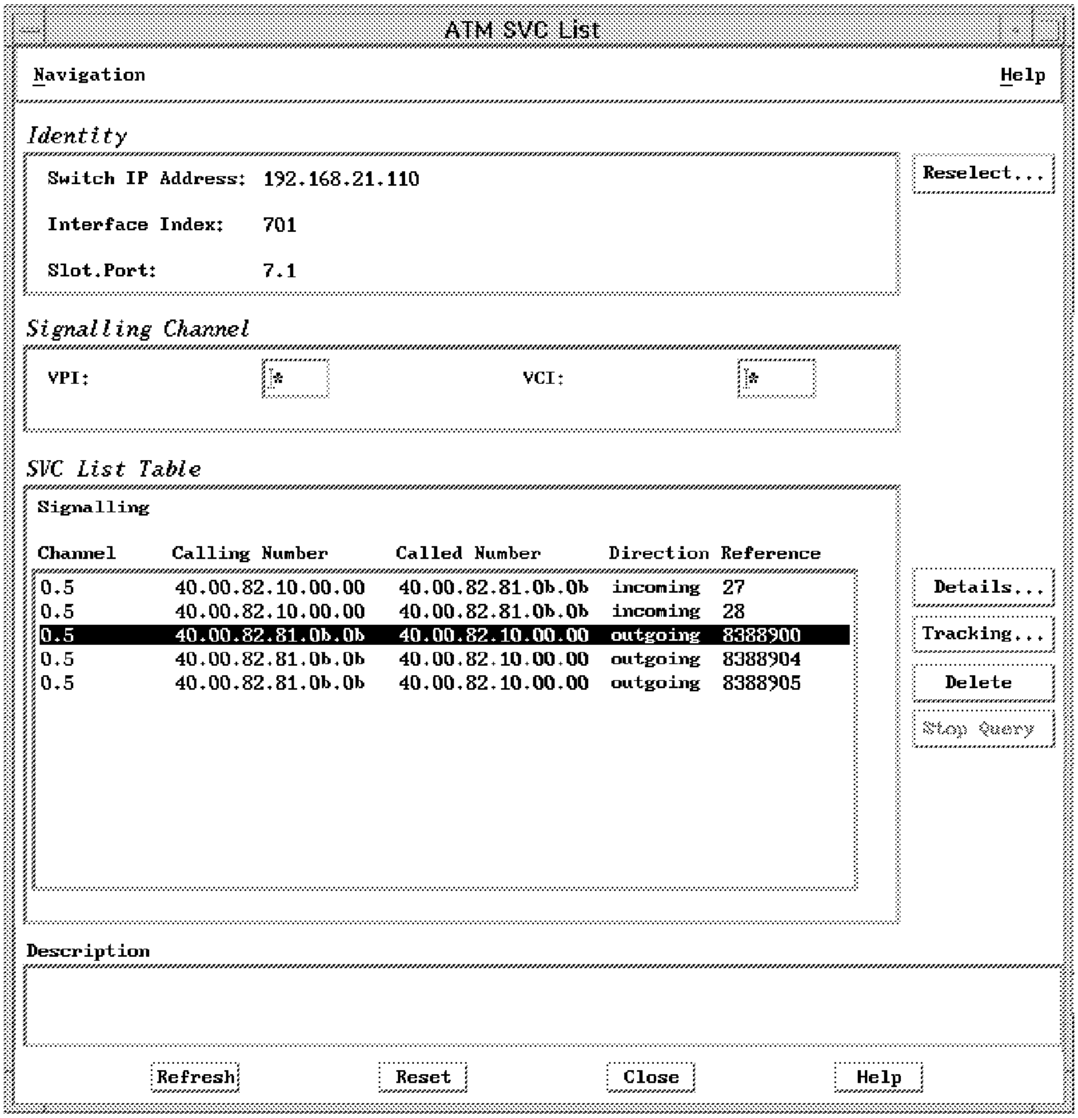

Figure 28. SVC List

For an accurate interpretation of the terms *incoming* and *outgoing* as descriptions of a call, think of the ATM end system as being something like a telephone. Any *incoming* call is a call that arrives at the ATM end system, any *outgoing* call is a call that is made from the attached end system to someone else in the network.

The example you see in Figure 28 is taken from a bridge. You can see two multicast SVCs arriving at the bridge, one from the BUS, the other one from the LES. Then there are three data direct VCCs connecting the bridge to LES, BUS and LECS. (The bridge was not very active at this time.) From this panel you can either look at some further detailed data of the SVC, as displayed in Figure 29 on page 52

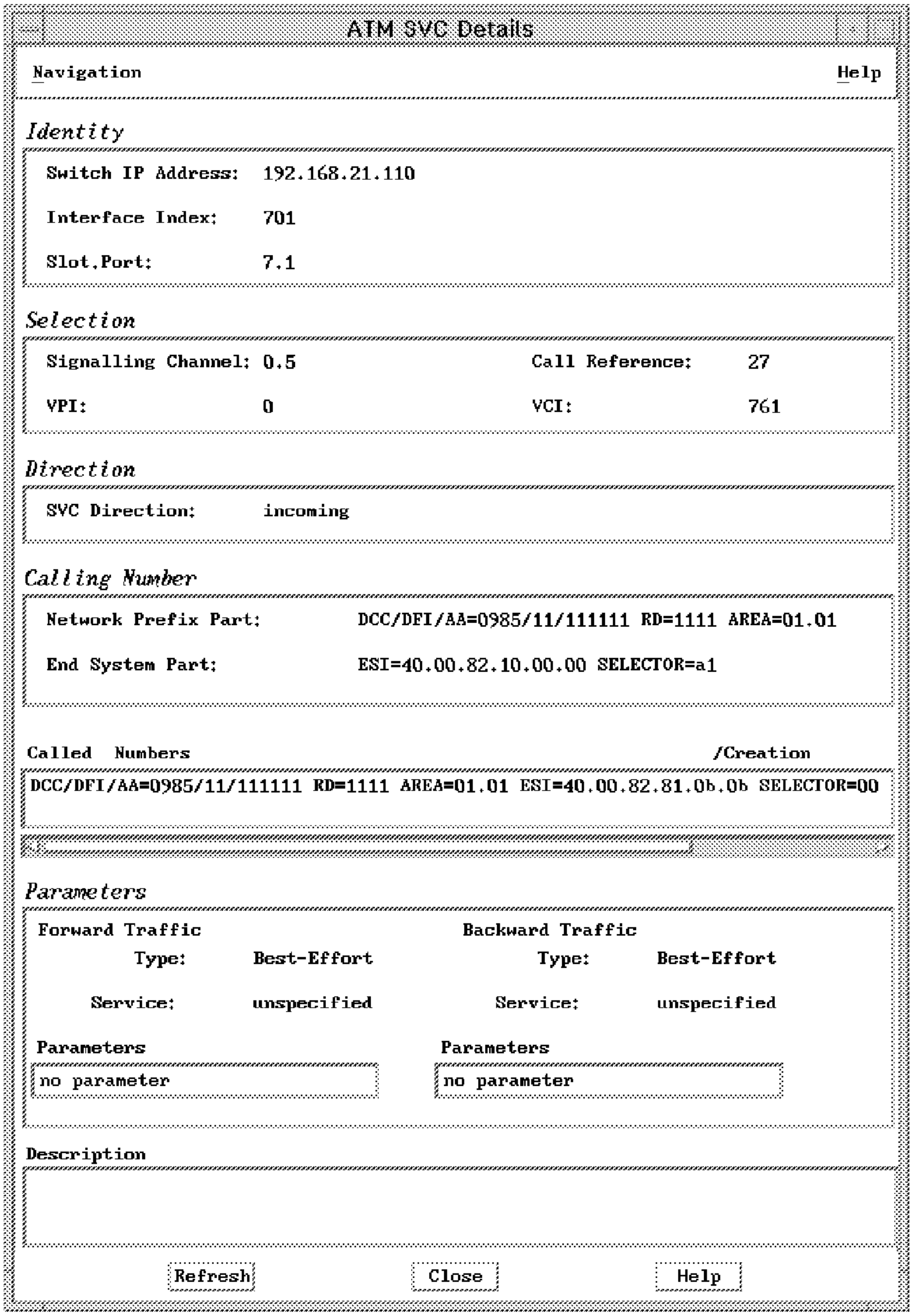

Figure 29. SVC Details

Or you can track the connection, which is shown on the panel in Figure 30 on page 53. As with the PVC connection you will find all the VPI/VCI values that are engaged in the transport of the cells through the network.

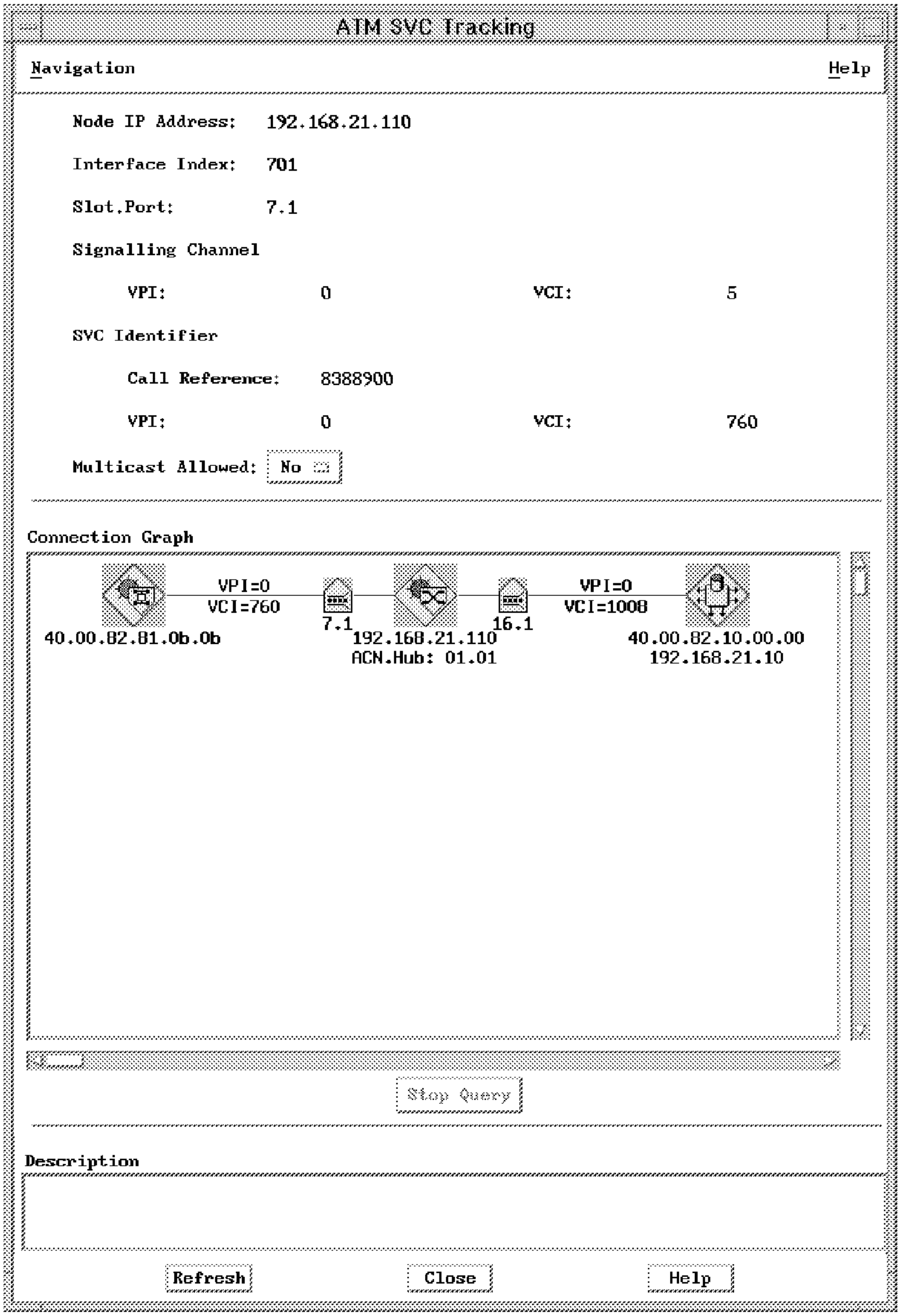

Figure 30. SVC Tracking

Unfortunately you do not see the selector byte of the ATM address at the other end of the connection on this panel; that is, you cannot really identify what LEC of an MSS this SVC is connecting you to. The selector byte is included in the ATM SVC Details panel, but even with this you may not be able to differentiate between the LES and the BUS connection. Both of them have the same ATM address, including the same selector byte. So, if you want to make sure both the LES and the BUS connection of an LE client are UP, you see this better from the command line interface of the MSS.

```
MSS_A *t 5

MSS_A +net 0
ATM Console
MSS_A ATM+le-services
LE-Services Console
MSS_A LE-SERVICES+work
ELAN Name (ELANxx) ·“? TR_ELAN_8210_1
LE-Services Console for an existing LES-BUS Pair
MSS_A EXISTING LES-BUS ′TR_ELAN_8210_1′+databases list all lec
Number of LEC′s to display: 3

    LEC-LES and LEC-BUS State  (UP=Up,  ID=Idle,  --. --.
      **=Other; Show specific LEC to see actual)    v   v
                                          LEC    State   #ATM  #Reg   #Lrnd
LEC Primary ATM Address              Proxy  ID    LES BUS  Adrs  MACs   MACs
----------------------------------------  -  ----   --  --  ----  -----  -----
3909851111111111111111010140008210000009  N  0001   UP  UP     1      1      0
3909851111111111111111010140008210000005  Y  0002   UP  UP     1      1      0
39098511111111111111110101400082810B0B00  Y  0003   UP  UP     1      5    157
MSS_A EXISTING LES-BUS ′TR_ELAN_8210_1′+
```

As you can see from the panel in Figure 31 on page 55 below, a display of one of the multicast trees would also have had more information if the selector byte were visible on it. However, you may choose to take a different ESI value for each of the networks defined on your MSS, which generally makes this panel more informative.

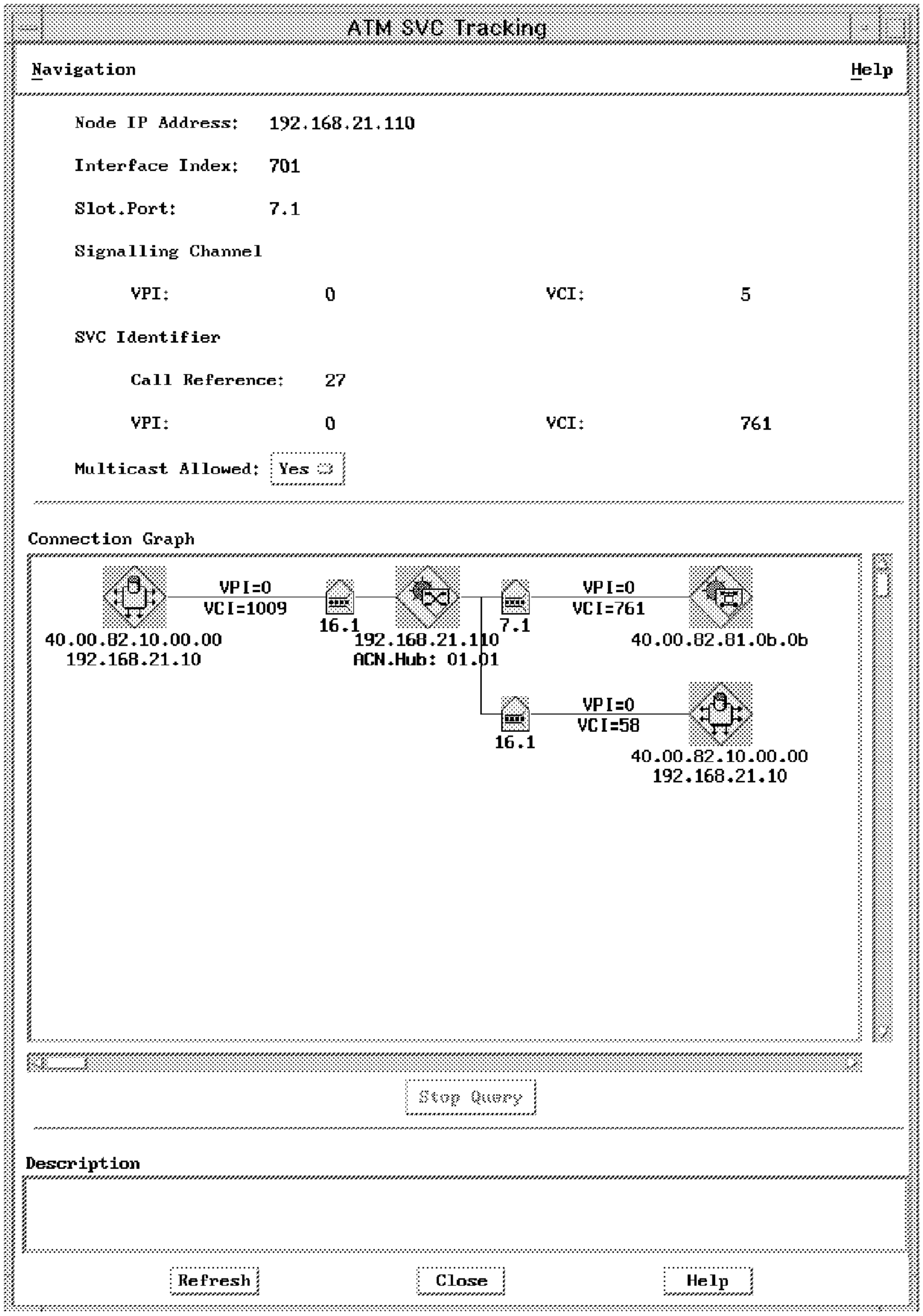

Figure 31. Tracking of a Multipoint SVC

3.2.6 What LAN Structure Do We Have in Our Network?

LAN Network Manager used to be the principle tool to answer questions concerning the MAC topology of a network in the past. With the new version of Nways Campus Manager LAN there is some information on LAN Emulation contained in its submaps.

So we turn to the LAN icon on the Root submap to find the MAC layer picture of our network. What we would like to find is an accurate picture of all the networks and all connections between these networks, based on the information that is available in the MIB information of the devices. Ideally, there should be a single network icon, representing the complete network we have and giving all the transparent and source routing bridges that connect the different parts of it.

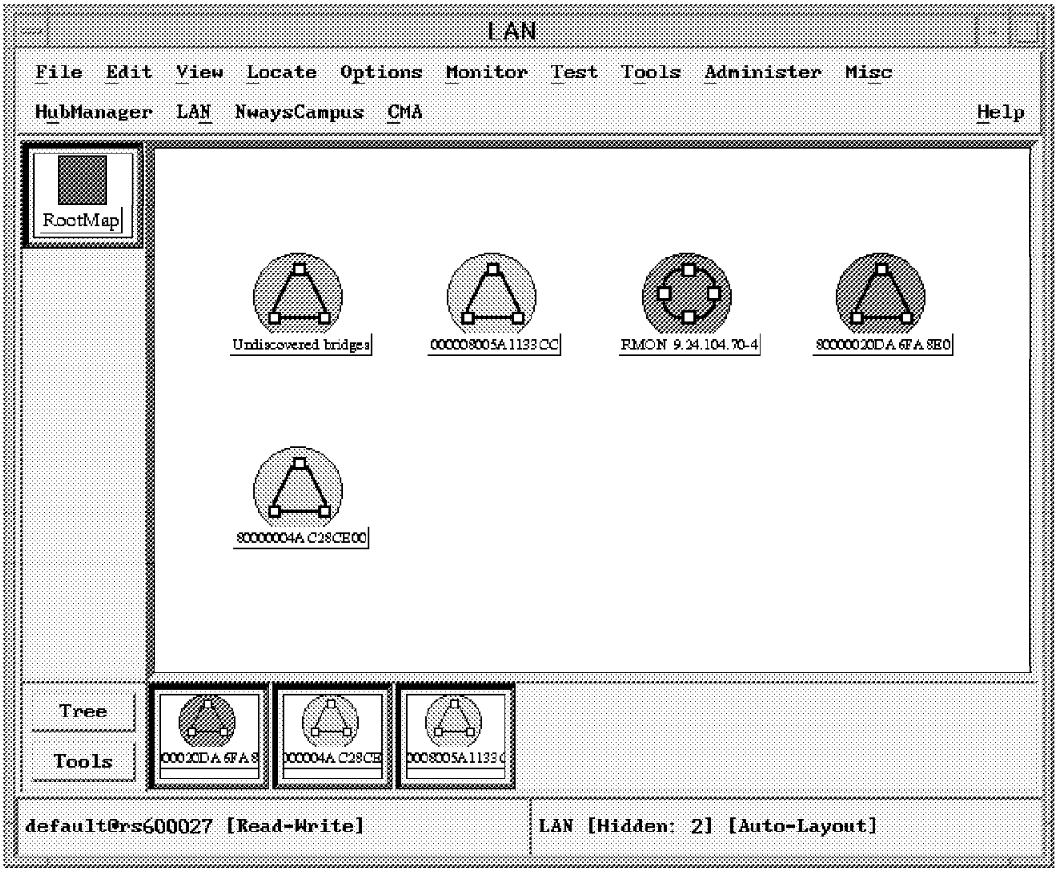

Figure 32. The LAN Submap with Different Network Icons

Looking at the LAN submap in Figure 32 you may wonder why there are so many different network icons. You should keep in mind, that the topology display of Nways Campus Manager LAN is based on what is found in the MIB concerning the spanning tree participation of the different bridge devices. In general, it can be described as a mechanism that turns any meshed topology into a tree structure by blocking *loop* connections in it. The tree structure is set up by the exchange of so-called bridge protocol data units (BPDUs) and re-initiated every time a member of the spanning tree considers the tree broken.

The root of the spanning tree is formed by a specific adapter of the root bridge. It is the *priority value* of this root bridge, followed by the MAC address of the root adapter, that is taken as a unique identifier for each spanning tree.

There can be more than one spanning tree established in a single network. Since LNM happens to derive its topology and connection information from the spanning tree data found in the dot1dBridge MIB of the SNMP-capable devices (dot1StpDesignatedRoot), it will depict every such spanning tree in the LAN submap it builds.

In addition to the network icons you can see some segment icons on the LAN submap (see the RMON icon in our example screen). LNM tries to gather information about segments from several sources, then tries to merge these segments into the correct spanning tree network.

If a LAN station located on the LAN segment interconnecting two bridges implements an SNMP *surrogate* capability, LNM will use it to retrieve the segment information from it.

These surrogate agents have knowledge of all the MAC adapters located in their token-ring segment (thanks to their promiscuous MAC adapter). They also implement the three classical token-ring servers that relay network management commands (REM, CRS, RPS) and offer to network management the capability to retrieve relevant information from these server databases. Relevant information for subnet building is the CRS ring station table that provides information about all the ring station MAC addresses of a given ring (crsStationAddress of crsRingStationTable).

If bridges have one port connected to this LAN segment, one of their port MAC addresses (ifPhysAddress of MIB-II ifTable) should match one of this segment′s MAC address (ifPhysAddress = crsStationAddress). As correlation is possible inside the bridge between the port number and the interface number of this port (dot1BasePort and dot1baseportIfIndex), then a bridge port will be associated to a LAN segment. As the token-ring surrogate agents are SNMP-readable, they allow LNM to build a complete subnet that integrates the source routing bridges and the SNMP managed token-ring segments.

With RMON agents much the same information is provided to LNM. In order to use them you have to specify the type and address representation policy (canonical or noncanonical) under the Administer->Campus Manager Smit smit panels. In case of 8230 model 13, you will also need to manually switch on the RMON data collection. Turn to the README file included in the microcode diskette for Version 5.3.1 for details on how to handle the RMON agent in it.

You may notice that occasionally the sequence of machines shown in the merged segments is not what you would have expected as NAUN sequence. We discovered, that it helps to set the corresponding RMON agent for this segment to invalidate (using the MIB browser) and re-enable it again. After this, do a resynch of the segment from the segments profile panel and the machines should be in proper sequence again.

As said above, every bridge that specifies the same type of spanning tree and the same root bridge will be merged into the existing submap of other bridges that share this information. The bridges on such a display are connected by the segments. What is new with ELAN management is that this also holds true for emulated LAN segments and the emulated bridging ports that connect them. While with the previous version of Nways Campus Manager LAN there was just an ATM cloud symbol shown as the connection between 8281 bridges for example, the new release really shows them as emulated segments now. Look at Figure 33 on page 58 to see an example of an 8281 bridge.

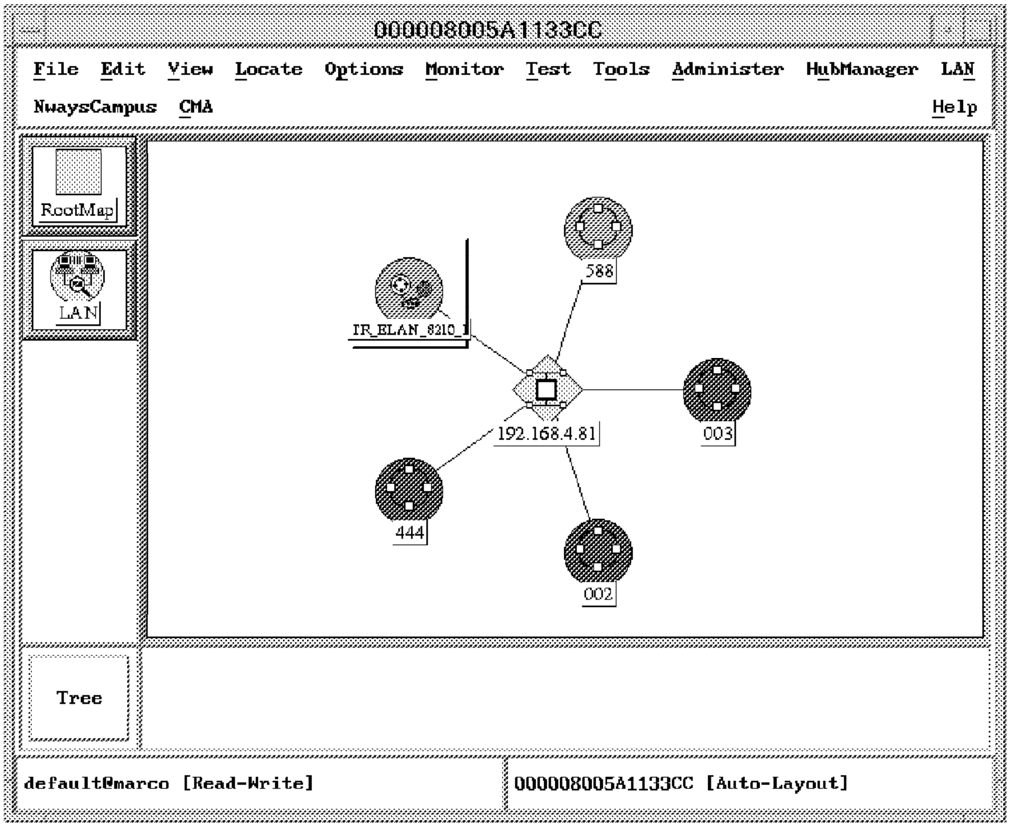

Figure 33. View of 8281 Bridge with Segments Attached

The legacy token-ring segments that are depicted on such a network submap can be exploded into a submap showing the sequence of the MAC addresses in them. This function has not changed from the previous release.

For the ELAN segment you will notice that it is executable, offering a way to start the ELAN management application from here. However, there is no such thing like a submap representation of the devices included in the ELAN segment. There is a number of different spanning tree participations that can be adopted by the MSS. A very comprehensive description of these different types can be found in the *Command Line Interface Volume 2 User's Guide and Protocol Reference* (document number SC30-3819-01). Normally, the LNM would take the local segment number specified by bridges in the same source route spanning tree to show their connection via shared segments. However, we never found the bridges merging with our level of the code. Still you could use the EXPLODED ELAN view of the connecting ELAN, to see that both the 8281 and the 8210 had interfaces to the same emulated token-ring segment.

3.2.7 Do We See All the Segments of Our Network Displayed by LNM?

Since LNM only shows the MSS as a bridge, it will only show the interfaces that are defined as bridge ports. There may be other interfaces of the MSS, even interfaces that have several IP and IPX addresses defined, which will not show up on the LAN submap. So, in fact, the network segments you find here are not the complete network. In addition to the emulated LAN interfaces that do not serve as bridge ports, there still is a number of Classical IP networks, which likewise will not be seen by Nways Campus Manager LAN. Accordingly, the LAN part can no more be regarded the all-comprising MAC layer, with all layer three elements being just a subset.

3.2.8 What about the New MSS Features?

There are a number of value add functions of the MSS that serve to set up shortcut connections through the network:

- With shortcut bridging a connection is established from one LEC to another LEC in a different ELAN, which does not involve the LEC of the bridge in the transfer of the data. Instead a direct SVC connection is established between the two participants, that allows for a communication just as if the two partners were located in the same ELAN.
- IP cut-through on an ELAN network you will likewise find direct VCCs being established between IP partners sharing the same IP network but residing in different ELANs.

No such connection is shown by either Nways Campus Manager LAN or the ipmap submaps. Likewise there are a number of features that serve to confine broadcasting to the required minimum. Notably there is:

- The broadcast manager, which is a function of the BUS, serving in conversion of broadcast request into unicast requests for the stations registered with the BUS.
- The bridge broadcast manager, which serves the same purpose for a bridged network. It will try to convert any broadcast frame destined for a known station outside the ELAN of a broadcasts originator to be converted into a unicast frame first, before eventually trying the broadcast in case of failure.

We did not find these features reflected on the LNM submaps as yet.

3.3 ELAN Management

The ELAN management application comes as a new part of Nways Campus Manager ATM to handle the different elements of ELANs that is LECS, LES/BUS pairs and LECs. While much of the information about a legacy LAN member is taken from the attached devices SNMP agent itself, most of the information about ELAN entities is taken from the information stored in the devices that hold the service entities LECS and LES/BUS. It is also these service entities that provide Nways Campus Manager ATM with the knowledge about the topology of an ELAN network. Hardly anything is taken from the LAN Emulation clients as such. Nways Campus Manager ATM interfaces with TME 10 NetView by setting an executable icon on the root submap

From this icon you will access all the ELAN-related information administered by the ahmtopod daemon. If you do not see this icon executable, it may be a good idea to see if this daemon is running. Double-clicking on the icon will open the LAN Emulation panel as shown in Figure 34 on page 60.

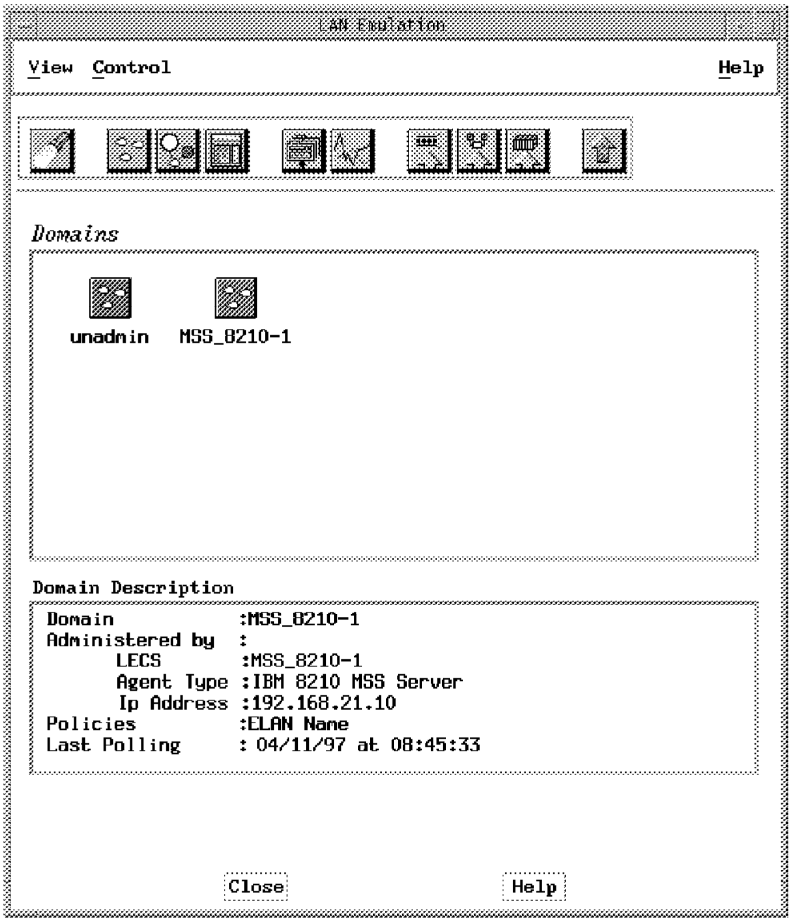

Figure 34. LAN Emulation GUI

It holds a couple of icons for so-called administered domains and one icon for the only unadmin domain it knows. This representation of the ELAN environment is oriented after the idea of an ELAN being controlled by an LECS instance. Since ELAN access can be controlled for all LE clients trying to join a specific ELAN, the ELAN is said to be under the administration of this LECS. All such ELANs that are not mentioned in the policy list of any LECS would be considered unadministered ELANs and displayed under this icon.

A domain is administered through a *policy profile*. A policy profile has the following criteria:

- Ordered set of policy rules with priority levels
- List of values defined for a given policy rule

The policy profile and the corresponding policy rules define the criteria used within a domain to assign a client to a given ELAN. The client is assigned to the ELAN when it passes the policy criteria.

A domain may have a policy profile consisting of an initial priority policy rule by ATM address followed by a second priority policy rule by ELAN name.

Each ELAN/LES pair defined in this domain has a policy that contains a list of ATM addresses and a policy that contains a list of ELAN names.

Using the ELAN application you can access and modify the following information:

1. All the administrative domains (set of ELANs administered by the same LECS).
2. All the emulated LANs belonging to a discovered administrative domain.
3. ELAN, LES/BUS, LECs and policy information:
   - All the LE clients belonging to a discovered emulated LAN
   - All the LAN emulation instances (LECS, LES/BUS, LECs) associated with a given ATM device
   - All the ATM devices supporting a given LAN emulation entity (LECS, LES/BUS, LECs, proxy LECs)
   - For a given LAN emulation instance, the ATM physical port associated with the instance
   - For a given LAN emulation proxy client, the legacy LAN port associated with this proxy
   - For a given ATM port, the LAN emulation instances associated with this port
   - For a legacy LAN port, the LAN emulation proxy client supporting this port
   - Dynamically displays the administrative and operational status of LAN emulation entities
   - Change the LAN emulation configuration by dragging and dropping selected icons

3.3.1 TME 10 NetView Icons and Labels

Let us first look at some general conventions regarding the labelling and color representation of the ELAN elements, as they are shown on the panels of the ELAN management application. The icons that represent the LECS, LES, BUS, LEC, and domains and are labeled as follows.

For LAN Emulation entities the icon is labeled by the IP address or host name concatenated with the specific instance number of the LAN Emulation entity within the ATM device.

The ELAN label is derived from a number of sources:

1. The ELAN name defined in the ELAN table
2. The ELAN name defined in the LES when no LECS was discovered
3. The ELAN name defined in the BUS when neither an LECS nor a LES were discovered

The status or color assigned to these ELAN objects depends on the current state of the device.

LEC status blue The LEC instance cannot be found in the LES LECs table. If its ATM host reports this LEC status as administratively disabled, the LEC instance may still exist but is inactive.

LEC status brown Either of the following was found to be true:

- The ATM device hosting the LEC instance is set to unmanaged by TME 10 NetView.

- The LEC is present in the LEC table of the LES and has joined the ELAN but we can no longer retrieve information from its host LEC table due to loss of SNMP connectivity.
- The ATM device implementing the LEC is currently down.
- The ATM device is SNMP readable but does not contain any information in the LEC MIB.

LEC status red Either the LEC device implementing the LEC instance is not responding to a poll request or the LEC is no longer present in the LES/BUS tables.

LEC status marginal Whenever either the device implementing the LEC is no longer responding to SNMP polling while the LEC is still known by both the LES and BUS.

LEC status green If the device implementing the LEC is responding to SNMP requests, the LEC is active and is reported in both the LES and BUS tables.

LEC status gray If the LEC instance can′t be found anymore in the LES LECs table and its ATM device no longer reports this LEC, then the LEC status is removed and the LEC icon is set to gray.

For an LES instance the following status applies:

- LES status is *unmanaged* each time the LES instance is defined in the ELAN MIB but its implementing device is not SNMP-manageable.
- The LES status is *disabled* if the device is responding to SNMP polling but the LES instance is disabled. The LES icon is then set to *blue*.
- The LES status is *critical* if either the device implementing the LES instance is no longer responding to SNMP polling (while the LES is defined in the ELAN table) or if the device answers to SNMP polling but the LES is not operational. The LES icon is then set to *red*.
- The LES status is *normal* when the LES is operational, and its device answers to SNMP polling. The LES icon is set to *green*.

For an LECS instance the following status applies:

- The LECS status is *unmanaged* if its ATM address can be found in an LECS table but its ATM device is not managed. The LECS icon is set to *brown*; this status is applicable to the ELAN view only.
- The LECS status is *disabled* if even though its ATM device is managed and answers to SNMP polling; this LECS instance is currently administratively disabled. The LECS icon is set to blue.
- The LECS status is *critical* whenever the device implementing the LECS instance is no longer responding to SNMP polling or the LECS ATM device reports the LECS status as not operational. The LECS icon is set to *red*.
- The LECS status is *normal* whenever the LECS is operational; its SNMP device responds to polling and reports the LECS status as operational. The LECS icon is set to *green*.

For an ELAN instance the following color coded status applies:

brown The ELAN status is *unmanaged* when all the devices in its group (LECS, LES, BUS, LECs) are unmanaged.

blue The ELAN status is *unknown* if there are no LES or BUS servers found for this ELAN although this ELAN is defined in the ELAN MIB of the ATM device.

red The ELAN status is *critical* whenever a primary server device is in a critical state (LECS, LES, BUS).

yellow The ELAN status is marginal whenever a LAN Emulation server (LECS, LES, BUS) LAN Emulation server disabled or a backup LAN Emulation server is in a critical state.

green The ELAN status is normal if all the LAN Emulation entities are operational. All the ATM devices are responding to SNMP polling and all the entities statuses are reported as operational.

For a domain instance the following color coded status will apply:

blue Unmanaged. If all the servers in the domain are unmanaged, the domain icon is set to this color.

red Critical. That is, an ELAN is in a critical state or the LECS is not operational.

yellow Marginal. Set if some ELANs are in a marginal state.

green Displayed if the domain status is normal and all the ELANs are operational.

3.3.2 Exploring ELAN Application Panels

As was pointed out before, there is no need to write a redbook as a repetition of the user′s guide. So, the following description of the panels will not randomly show you a sequence of different panels but rather try to answer a couple of orientation questions about your network based on the information you find displayed in the panels.

How do we find a specific ELAN? Working with the LNM submaps we have already seen some of our ELANs mentioned. This may have been by name, or by the segment number that the token-ring ELANs represent. So, how do we find these ELANs?

All the ELANs we have are arranged under one of the domain icons we find in Figure 34 on page 60. Each domain icon is identified by the IP address or the host name of the device where the LECS is defined followed by the instance number of the LECS.

Double-click on one of the domains in Figure 34 on page 60 to open the panel in Figure 35 on page 64. Primarily it holds the name of the LECS and the names of the ELANs it administers. On the right side of the panel you find the general policy rule for all of the ELANs under Policies and Priorities. Clicking on any of the items shown on this panel you will be given additional information in the ELAN Description box at the bottom of the panel.

Since every MSS can only hold a single LECS, it sounds likely that there should not be a big number of domains around and we can look for our ELAN in every domain sequentially.

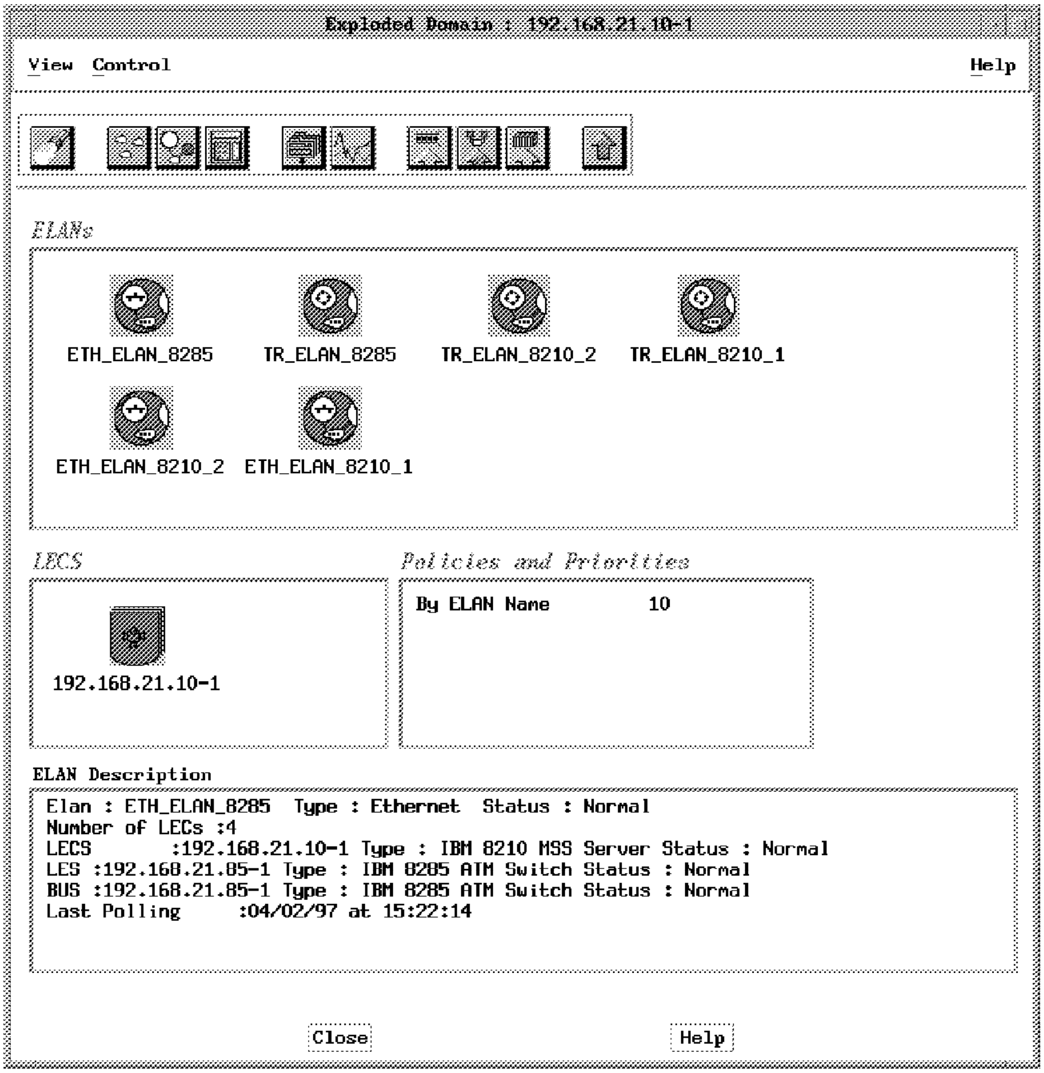

Figure 35. ELAN Configuration

As was described above, you should ensure that every device implementing the LECS or LES/BUS function is SNMP-reachable if you want to have accurate information about the state of the ELANs. In most cases the icons will simply turn critical because of an SNMP connection loss. That is, this does not indicate that the network is actually down.

If you want to find the ELAN names administered by a given LECS on the MSS, just enter:

```
MSS_A *t 5

MSS_A +net 0
ATM Console
MSS_A ATM+le-services
LE-Services Console
MSS_A LE-SERVICES+lecs
LAN Emulation Configuration Server console
MSS_A LECS console+elans
LECS ELANs console
MSS_A LECS ELANs+list

ELAN listing...

 Type         MFS   ELAN name
 ============ ===== ================================
     Ethernet  1516 'ETH_ELAN_8210_1'
     Ethernet  1516 'ETH_ELAN_8210_2'
     Ethernet  1516 'ETH_ELAN_8285'
    TokenRing  4544 'TR_ELAN_8210_1'
    TokenRing  4544 'TR_ELAN_8210_2'
    TokenRing  4544 'TR_ELAN_8285'
MSS_A LECS ELANs+
```

As you can see in this example, it is possible that the ELANs administered by a specific LECS do not reside on the same MSS.

Another way of looking at the ELANs is by the new command line interface, the ahmlecmd command.

```
# /usr/CML/bin/ahmlecmd ListDomain -server marco
Domain Name                     Status DBIndex
unadmin
9.24.104.115-1
   LECS Label                     ConfId Status ATM Address
         PolSel OSIndex
   9.24.104.115-1                      1      2 39098511111111111111110101400082
10000000      0      1
       Box IP Address  Box type             DBIndex
       9.24.104.115     Generic Box              1
   ELAN Label                     ConfId Status LANtyp DBIndex
   ETH_ELAN_8210_1                     1      2      2      5
   ETH_ELAN_8210_2                     2      2      2      6
   TR_ELAN_8210_1                      4      2      3      8
   TR_ELAN_8210_2                      5      2      3      9
   TR_ELAN_8285                        7      4      3     13
   ETH_ELAN_8285                       8      4      2     14
rs600027:/ #
```

This may be a quick way to find all the names of your ELANs at a glance, sorted by LECS and giving the box that the LECS is defined on.

What you can see on the right side of the Exploded Domain panel under the Policies and Priorities label is a group box holding the overall policy rule for the LECS and for this domain.

It is a little bit more complicated to arrive at the specific values that will then let LECS bind a certain LEC to a corresponding ELAN (that is, LES/BUS pair). What you find in the box is just a prescription as to what LEC provided values should be considered first, second, third and so on in the effort of determining a specific

LES for the LEC. Let us see how to find the corresponding values for each LES. Select **Configuration** from the context menu of the LECS and open the LECS Configuration panel in Figure 36 on page 66.

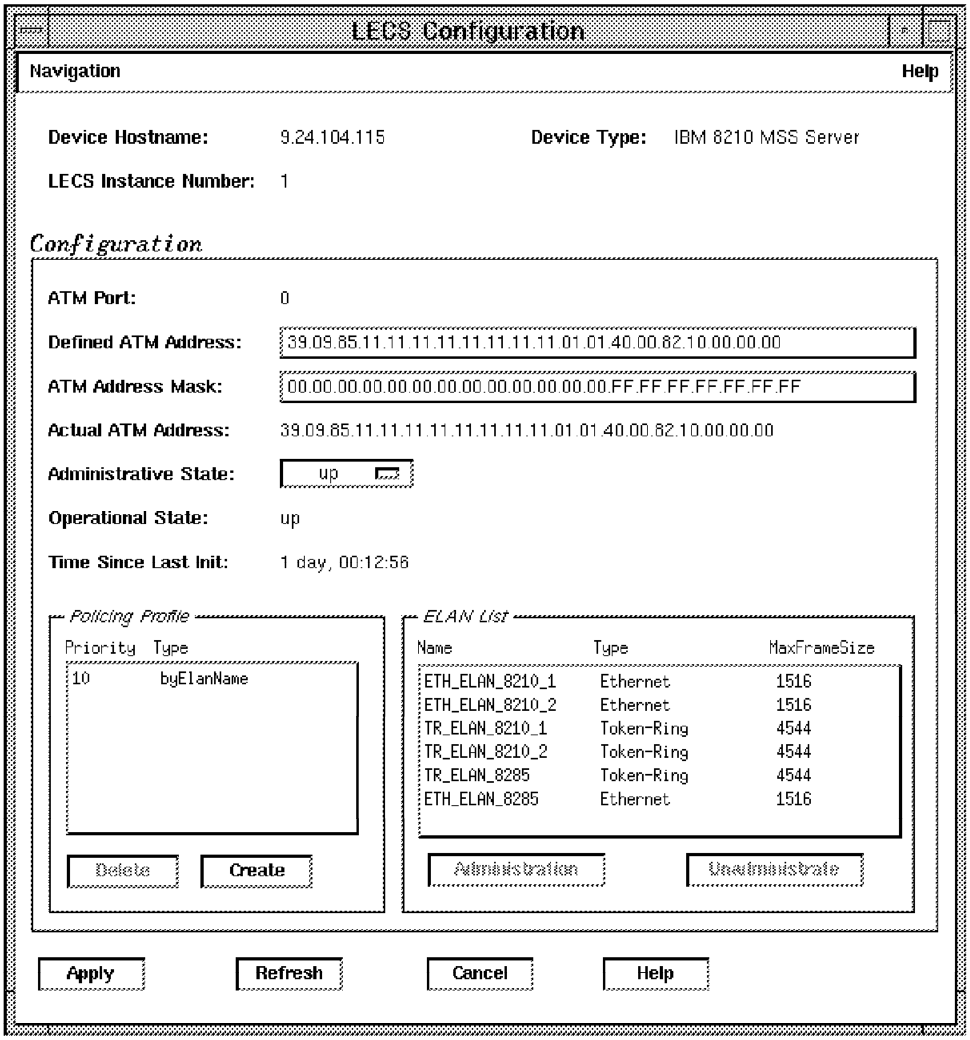

Figure 36. LECS Configuration Panel

Here you will find all ELAN names mentioned for this LECS. Select the one you are interested in and double-click on **Administration** under the ELAN name box. This will take you to the ELAN administration panel shown in Figure 37 on page 67.

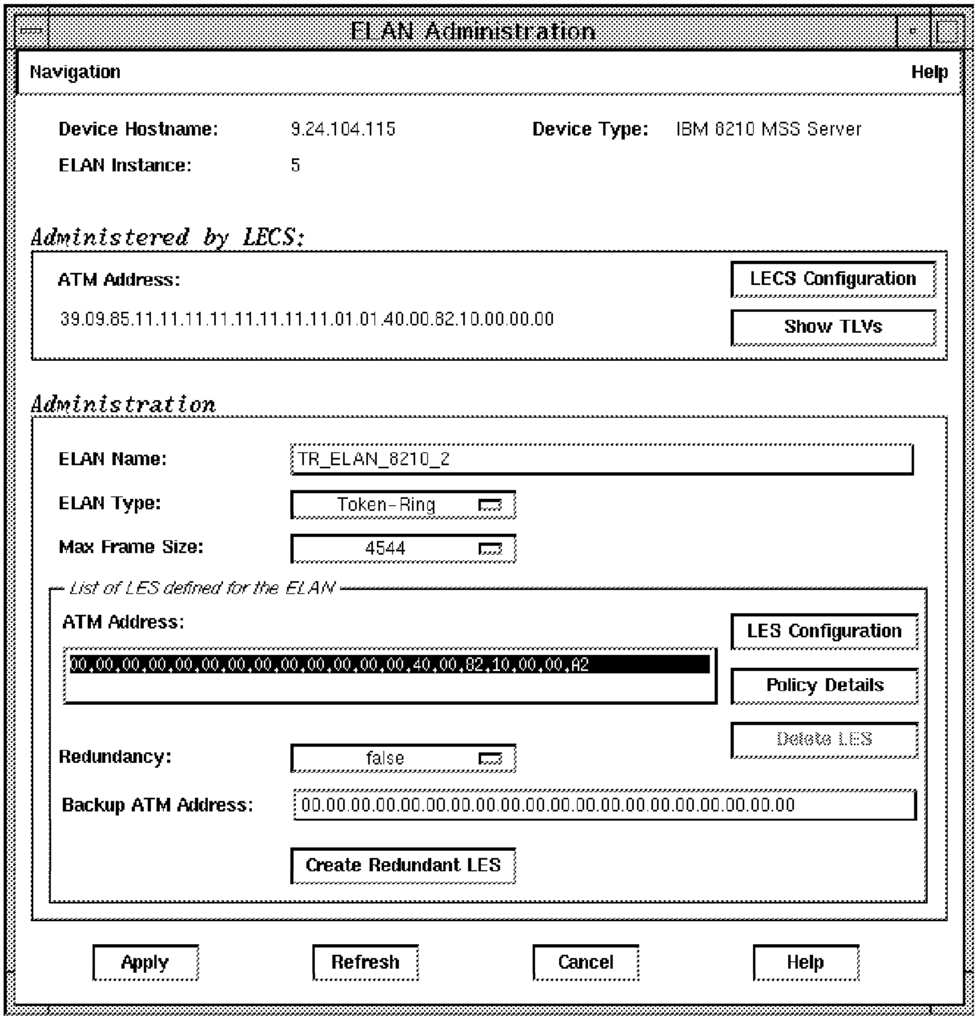

Figure 37. ELAN Administration Panel

Here again, you need to highlight the ATM address in the List of LES defined for ELAN box and select **Policy Details** right next to it. This again will move you to the Policy Rule panel shown in Figure 38 on page 68.

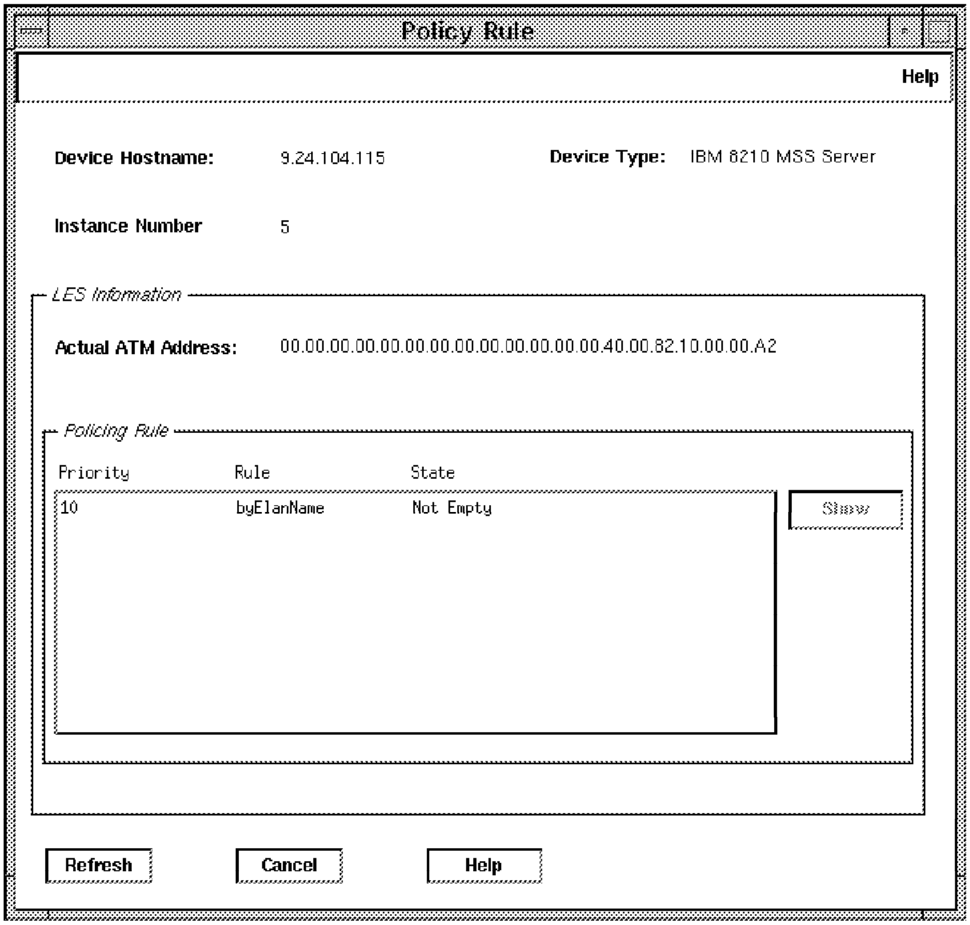

Figure 38. Policy Rules for a Specific LES

On this panel you will find back all the general policy rules mentioned that were specified for this domain. For each of them you will also find an indicator if there are one or more specific values ascribed to them for the LES you are currently looking at. The Show option by the side of the box will display them as in Figure 39 on page 69.

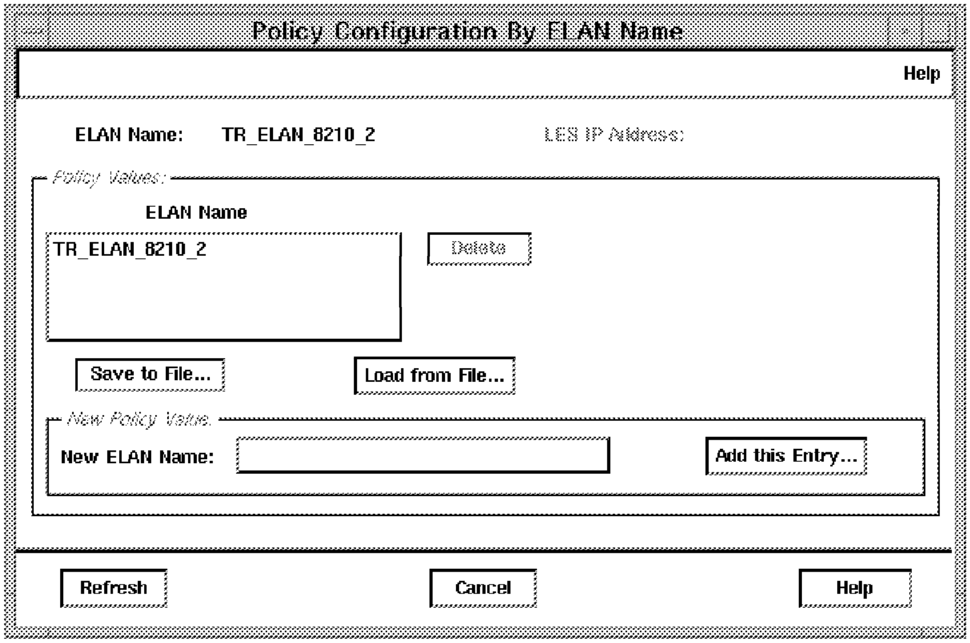

Figure 39. Specific Values for a Policy Rule

You can also use this panel to insert new values for the specified rule. However, they may be lost by reloading the MSS. You can also retrieve the configured information from the MSS via the command line interface, which looked like the following for our example.

```
MSS_A *t 6

MSS_A Config>net 0
ATM user configuration
MSS_A ATM Config>le-services
LAN Emulation Services user configuration
MSS_A LE Services config>lecs
LAN Emulation Configuration Server configuration
MSS_A LECS config>elans
Configuration of ELANs for LECS
MSS_A LECS ELANs config>select ELAN
Choice must be between 1 and 6
  (  1) ETH_ELAN_8210_1
  (  2) ETH_ELAN_8210_2
  (  3) TR_ELAN_8210_1
  (  4) TR_ELAN_8210_2
  (  5) TR_ELAN_8285
  (  6) ETH_ELAN_8285
Choice of ELAN ·1“? 2
ELAN ’ETH_ELAN_8210_2’ selected for detailed configuration
MSS_A Selected ELAN ’ETH_ELAN_8210_2’>policy list all

ATM ESI/Selectors for ELAN ’ETH_ELAN_8210_2’
Enabled  Value  =>  LES
=======  ==========================================

ATM prefixes for ELAN ’ETH_ELAN_8210_2’
Enabled  Value  =>  LES
=======  ==========================================

MAC addresses for ELAN ’ETH_ELAN_8210_2’
Enabled  Value  =>  LES
=======  ==========================================

Route descriptors for ELAN ’ETH_ELAN_8210_2’
Enabled  Value  =>  LES
=======  ==========================================

ELAN types for ELAN ’ETH_ELAN_8210_2’
Enabled  Value  =>  LES
=======  ==========================================

Max frame sizes for ELAN ’ETH_ELAN_8210_2’
Enabled  Value  =>  LES
=======  ==========================================

ELAN names for ELAN ’ETH_ELAN_8210_2’
Enabled  Value  =>  LES
=======  ==========================================
    Yes  ETH_ELAN_8210_2
            => Local LES for: ETH_ELAN_8210_2

MSS_A Selected ELAN ’ETH_ELAN_8210_2’>
```

3.3.3 What Devices Are Our ELANs Defined On?

In the context of the domains it is interesting to see what devices we actually have in the network and how many instances of what network entity we have created on them. One convenient way to answer this question is by looking at the panel in Figure 40 on page 71. It is opened through the **Control->Control View** options on the Exploded Domain panel above.

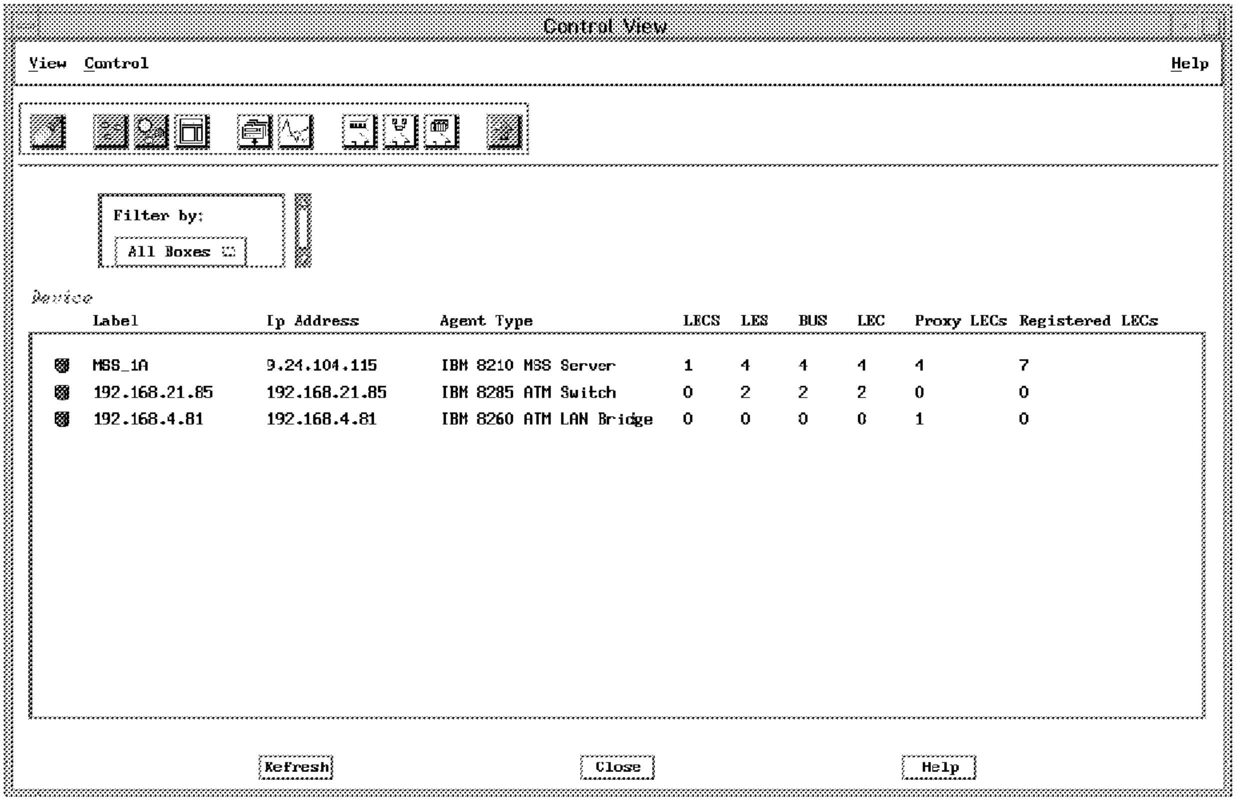

Figure 40. The Control View Panel

You can arrive at the same information from the command line again, using the ListBox command.

```
# /usr/CML/bin/ahmlecmd ListBox -server marco
Box IP Address  Box type             DBIndex
9.24.104.115     Generic Box             1
 LES Label        ConfId Status ATM Address                        OSIndex
 9.24.104.115-1    1      2 3909851111111111111111010140008 000B1      1
 9.24.104.115-2    2      2 3909851111111111111111010140008 000B2      2
 9.24.104.115-3    3      2 3909851111111111111111010140008 000A1      3
 9.24.104.115-4    4      2 3909851111111111111111010140008 000A2      4
 BUS Label          ConfId Status ATM Address             OSIndex
 9.24.104.115-1    1      2 3909851111111111111111010140008 000B1      1
 9.24.104.115-2    2      2 3909851111111111111111010140008 000B2      2
 9.24.104.115-3    3      2 3909851111111111111111010140008 000A1      3
 9.24.104.115-4    4      2 3909851111111111111111010140008 000A2      4
 LECS Label        ConfId Status ATM Address             PolSel OSIndex
 9.24.104.115-1    1      2 3909851111111111111111010140008 00000      0      1
      Box IP Address  Box type             DBIndex
      9.24.104.115     Generic Box             1
192.168.21.85    8285                        2
  LES Label              ConfId Status ATM Address      OSIndex
  192.168.21.85-1   1      2 390985111111111111111101 0340008285000002      7
  192.168.21.85-2   2      2 390985111111111111111101 0340008285000003      8
  BUS Label          ConfId Status ATM Address         OSIndex
  192.168.21.85-2   2      2 390985111111111111111101 0340008285000003      5
  192.168.21.85-1   1      2 390985111111111111111101 0032008285000002      6
192.168.4.81     integrated 8281           3
```

3.3.4 Identifying LAN Emulation Clients in the Network

Double-click on one of the named ELAN icons in Figure 35 on page 64 to open the panel for the single ELAN. It is this same panel that you can also arrive at by double-clicking on an ELAN on the LNM submap in Figure 33 on page 58. The heading of the panel (see Figure 41) mentions the name of the ELAN (which can be helpful in case your LNM submap only gave you the segment number, as sometimes encountered on our installation).

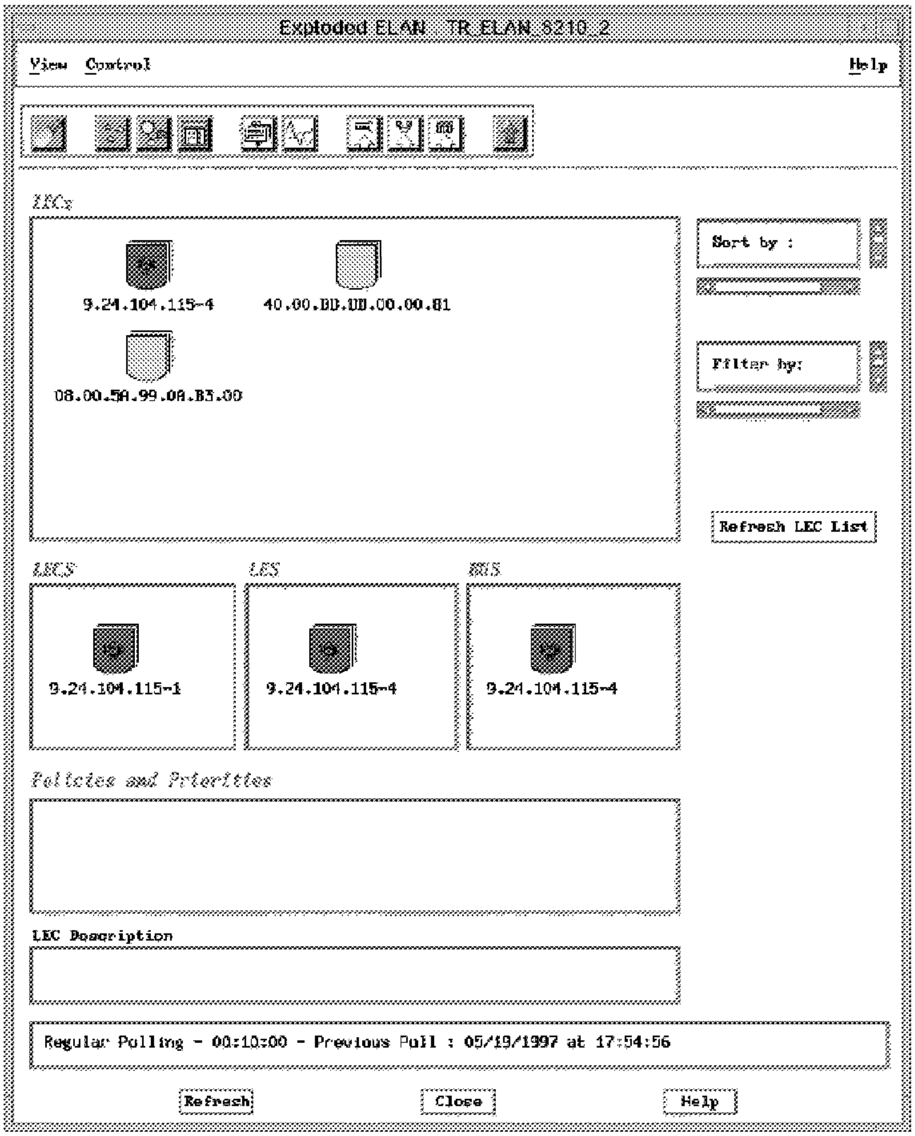

Figure 41. Exploded ELAN TR_ELAN_8210_2

A number of different elements can be found on this panel.

- All the LECs that have joined this Emulated LAN with an icon referring to their ATM host.
- The LES in charge of servicing all these LECs for address resolution with a relevant icon too.
- The BUS paired with this LES.
- An LECS whenever the domain is administered.

No LECS icon doesn′t mean that the ELAN is unadministered, but maybe that there are no matching LECSs found on existing ATM devices.

- Redundant LES and BUS (for backup) when relevant with a white triangle.
- Old clients, even when no longer found in the ELAN (grey icon).
- Current clients whose ATM device LEC information is not available (brown icon).

To get more information about the LECs that are displayed in graphical mode click on **View** and select **Change Mode**.

The graphical display of LECs will be shown in tabular format providing LAN Emulation-related information such as:

- The ATM address of the LAN Emulation client (selector included)
- The MAC address of the LAN Emulation client

3.3.5 How Do We Find a Specific Client in an Emulated Network?

The first attempt could be to look for it here on the display of the LE clients for a specific network. However, this may be a clumsy way to find a specific ELAN participant, as soon as the number of LE clients exceeds a more than trivial level. Look for the sorting function on the right side of the panel to sort the listed items by ATM or MAC address or filter the display by proxy, non-proxy, power off or alive LE clients.

Another way of finding an ELAN client would be by browsing the output of the /usr/CML/bin/ahmlecmd ListLec -server marco command. In this you will find the MAC address, ATM address and the implementing boxes IP address that the LEC is defined on.

The most useful tool however in these cases is the new search function again, that opens either from the NwaysCampus->search entry in the NetView main panel or from the torch symbol on any ELAN management application panel (see Figure 42 on page 74). There is quite a number of different criteria, that you can combine to pinpoint a specific machine in its ELAN. You can look for a station or device based on its:

- Address (that is, its MAC address, ESI or ESI and selector byte)
- Address type (that is, either MAC or ESI). This produces a complete list of known stations which is probably a good starting point for a search.
- IP address or host name
- Location and wiring information
- Miscellaneous information ascribed to it manually (department number)
- ELAN name
- Last polling date

In our example we looked for the Interface of a specific station, assuming that we have the MAC address it is emulating on the ELAN. However, as you can see on the same picture below, some of the detail data is not filled in. Most notably the IP address of the machine itself. The IP address given on the left-hand side of the panel is that of the box holding the interface where the station is attached. It is not the IP address of this station.

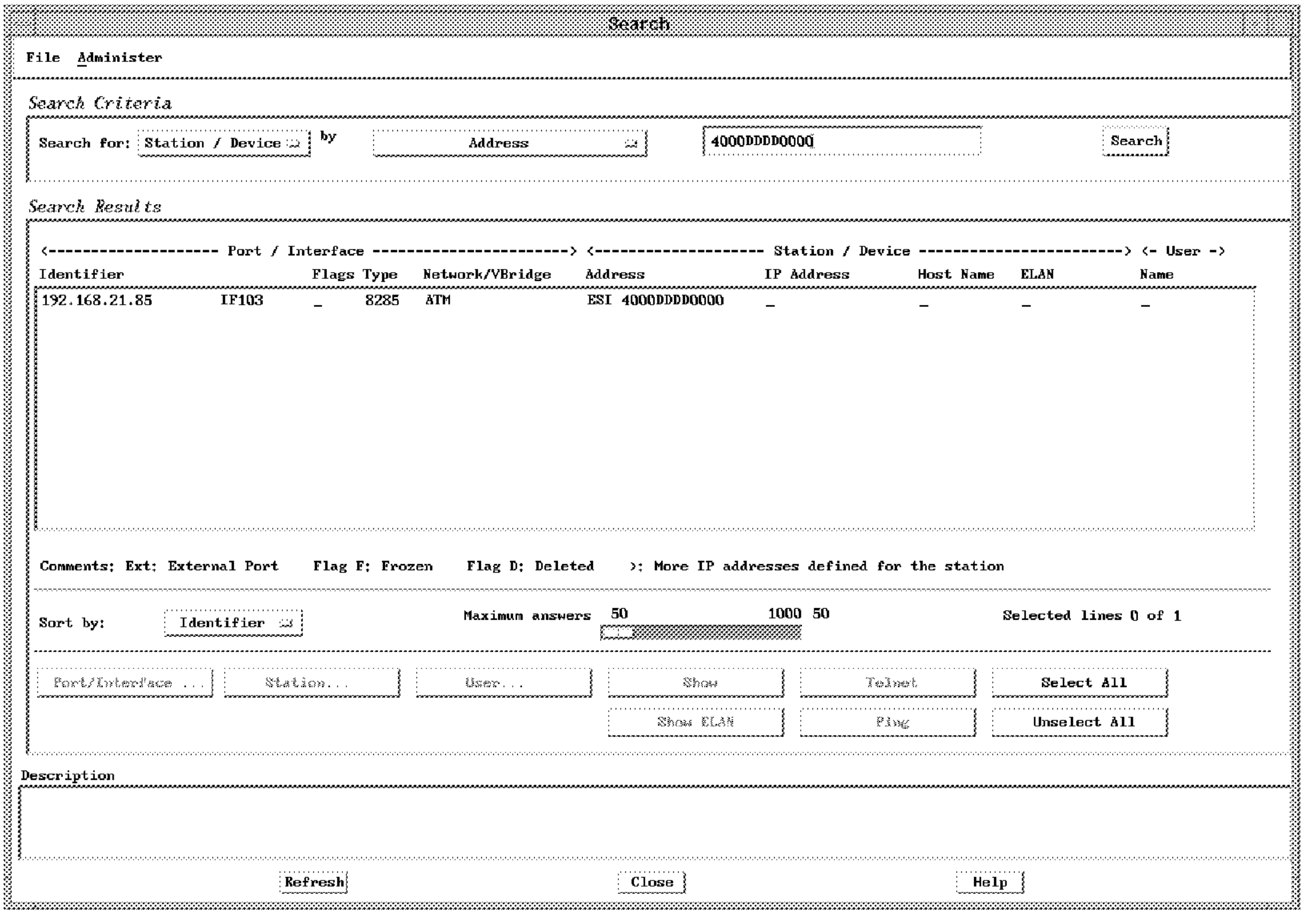

Figure 42. Search Result for Station with MAC 4000DDDD0000

However, the search function is rather usable on supplying miscellaneous information. Select a station from the list, select **Station** and you will open a station details panel as shown in Figure 43 on page 75.

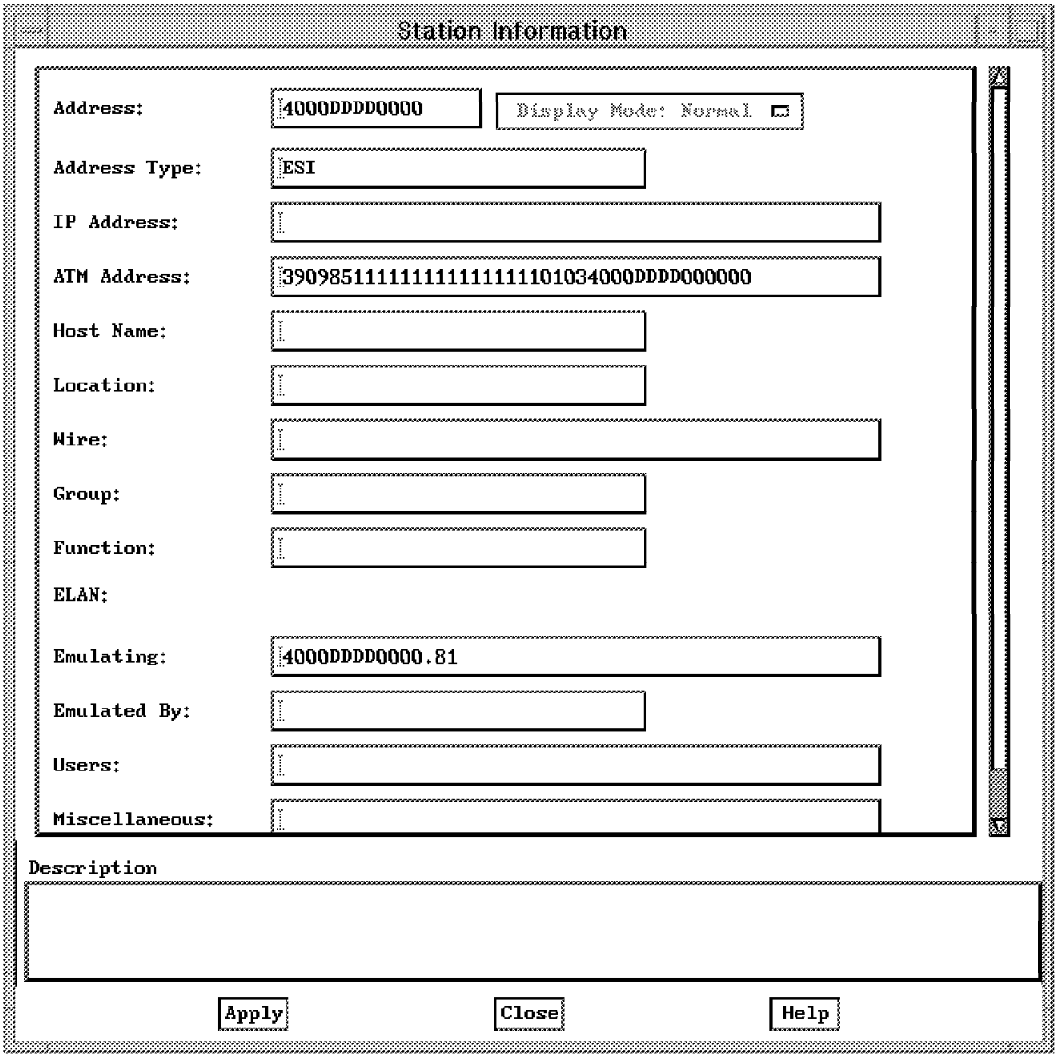

Figure 43. Detail Information on Station 4000DDDD0000

Feel free to enter some wiring information here, adding functional and organizational data as needed. After applying this data you can also use it as a search argument.

In addition you can define users to your search database. Select the **Administer->Create New User** option to open the panel given in Figure 44 on page 76.

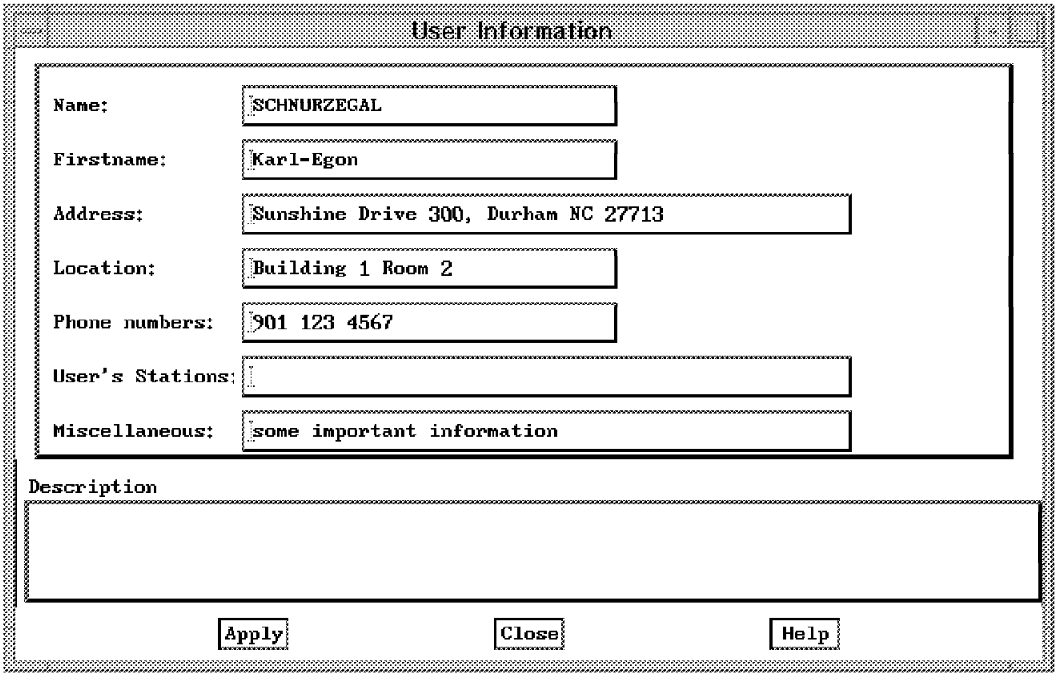

Figure 44. Create a New User Panel

Enter the required information and select **Apply**. Having done this, you can select any station from a search result, open the station detail panel as in Figure 43 on page 75 and specify the name of the user as the normal user for this station. The search function will show the station related to this user any time after this definition is made. You can also define several stations for the same user or several users for the same station.

Especially with the creation of users, it may be convenient to dump the complete database to ASCII flat files, manipulate it using some tool and upload it again. You can do so using the Administer->Save database to formatted file and Administer->Update database from formatted file options of the search panel. It lets you specify a name and path, which it uses to generate three files with the following extensions:

stations Holding all the station definitions

users Holding all the user definitions

interfaces For all interface information

A part of the information held in the search database for a station is merged into the *profile* panel of the LAN Emulation client (see Figure 45 on page 77 below). Don′t be confused by the IP address in the upper left corner. It is the IP address of the box that has the LEC defined to it. This may, but need not be, the IP address of the LEC we opened the profile for.

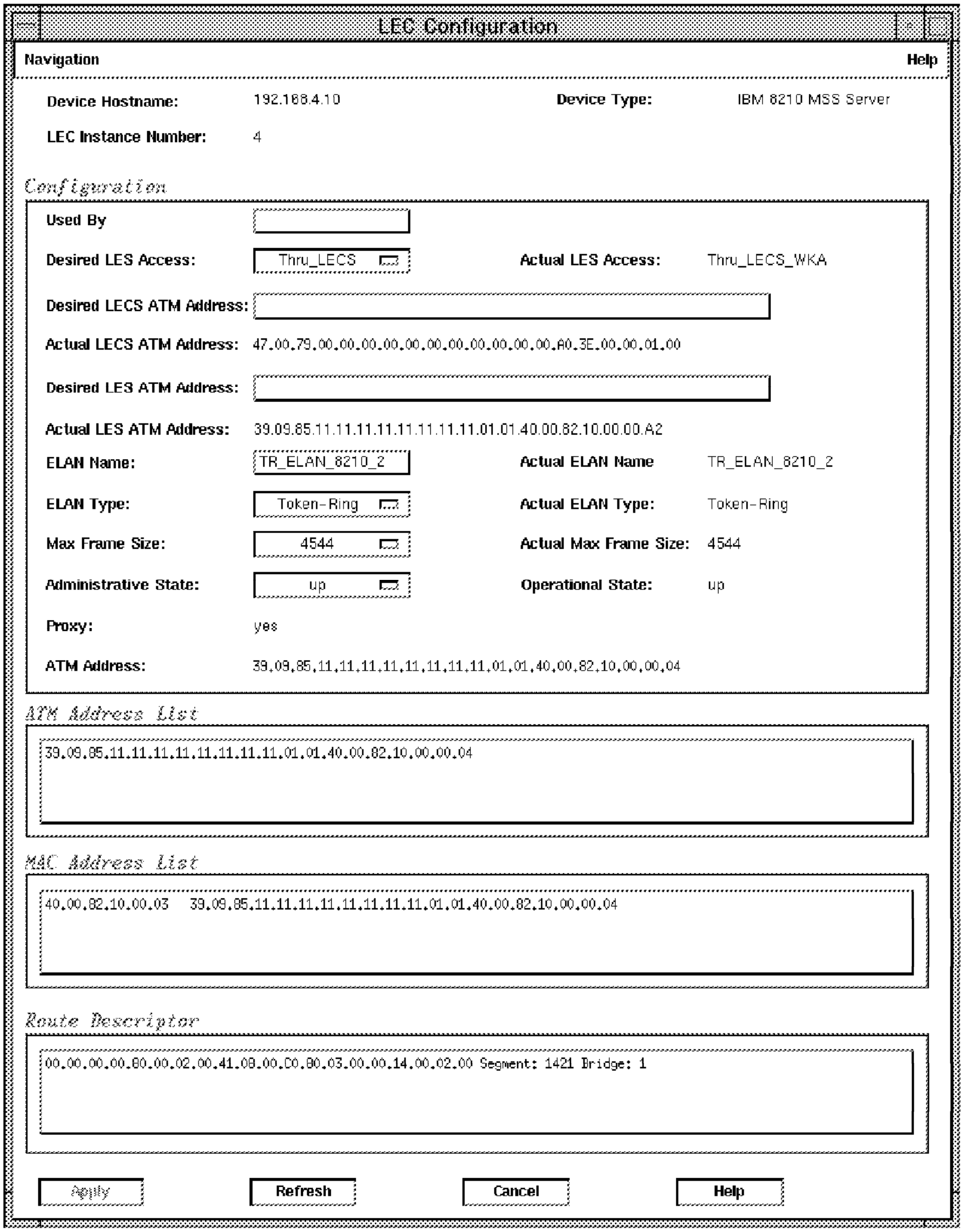

Figure 45. Profile Panel of a LAN Emulation Client

If you need the IP address to MAC address relation the easiest way we found for LE clients is by the locate function of NetView. Given an IP address you can locate the IP address from the **Locate->Objects->by Attribute** panel. It will allow you to open the Interface submap of the device in question. On the interface submap select the corresponding interface and choose **Tools->Display Object Information** from its context menu. The item SNMP ifPhysAddr contains the MAC address for the corresponding interface, regardless of this interface being an ELAN or legacy LAN interface.

On the other hand, if an IP address needs to be found from a MAC address, you can likewise locate it through the SNMP ifPhysAddr, which is a locatable object item.

What other information do we find on the LEC Configuration panel? The Configuration group box partly holds information provided in the LECs definition and partly reflects the current actual data of the ELAN it currently joined. For example, the Desired LECS field is the LECS entered in the LECs definition. It may have been left empty in order to use the ILMI provided information from the switch.

The Actual LECS field holds the ATM address of the currently accessed LECS. You may see a sequence of zeroes in here, indicating that the LES address was entered in the LEC configuration instead.

Most of the fields are self-explanatory from the terminology of the FC LAN Emulation Concepts, so here we focus on just some of them.

The MAC Address List holds the MAC addresses that were adopted by this LEC and the ATM addresses they relate to.

In case of a proxy LEC you can find more than one line in this box, giving all the different addresses that were registered with this interface.

The box at the lower end also holds some information for proxy LECs. With a normal 8281 configured for 802.5 for example, it will show you the sequence of ATM Interface address, legacy LAN segment number and the bridge number that was registered with the LES. It is taken from the MIB object.

```
private -> enterprises -> atmfForum -> atmfForumnetwork..
Management -> atmfForumlanEmulation -> leClientMIB -> leClientMIBObjects
lecRouteDescrtable -> lecRouteDescrEntry -> lecRouteDescratmBinding
```

For the MSS server things look a little bit different. The fact that the first part of the route descriptor is not a valid ATM address is a simple bug in the SNMP code of the MSS and will be fixed soon.

The bridge number you find here is the bridge number of the internal segment of the MSS. This is not a bug but simply the same behavior displayed by the normal edge devices. Since there is no legacy LAN that this bridge port would connect the ELAN to, the internal segment was taken instead. Any other segment number could have confused the LES for this ELAN.

You can display the segment number of the ELAN segment that this MSS LEC is connected to via the command line interface. It is shown in the display of the port under the asrt configuration of the MSS. Notice that the number is given in decimal on the panel. You need to convert it to hex first before using it. (This will probably be changed by development soon.)

```
MSS_A *t 6
MSS_A Config>prot asrt
Adaptive Source Routing Transparent Bridge user configuration
MSS_A ASRT config>list port
Port ID (dec)    : 128:01, (hex): 80-01
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Source Route Bridging Only
SRB: Segment Number: 0x58E       MTU:  4399     STE: Enabled
Assoc Interface  : 3
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
 ...
```

The internal segment of the MSS is used by the MSS if more than two of its LE clients connect to their segments as bridges. If some additional translational bridging is performed between Ethernet and token-ring ELANs, you will also find a virtual source route bridge segment assigned to all the Ethernet parts of your network. Both of these segments are not visible on the LNM submaps. However, you can find them on the command line interface of the MSS.

```
MSS_A ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                ===============================================

Bridge:                  Enabled                Bridge Behavior: SR<->TB
                   +----------------------------+
-------------------| SOURCE ROUTING INFORMATION |-------------------------------
                   +----------------------------+
Bridge Number:           01                     Segments:          2
Max ARE Hop Cnt:         14                     Max STE Hop cnt:   14
1;N SRB:                 Active                 Internal Segment:  0x58D
LF-bit interpret:        Extended
                   +--------------------+
-------------------| SR-TB INFORMATION |----------------------------------------
                   +--------------------+
SR-TB Conversion:        Enabled
TB-Virtual Segment:      0x58C                  MTU of TB-Domain:  1470
                   +-------------------------------------+
-------------------| SPANNING TREE PROTOCOL INFORMATION |-----------------------
                   +-------------------------------------+
Bridge Address:          Default                Bridge Priority:   32768/0x8000
STP Participation:       IEEE802.1d on TB ports, IBM-8209 and IBM-SRB proprietary
                   +--------------------------+
-------------------| TRANSLATION INFORMATION |----------------------------------
                   +--------------------------+
FA<=>GA Conversion:      Enabled                UB-Encapsulation:  Disabled
                   +-------------------+
-------------------| PORT INFORMATION |-----------------------------------------
                   +-------------------+
Number of ports added: 4
Port:   1      Interface:      3     Behavior:    SRB Only   STP:  Enabled
Port:   2      Interface:      4     Behavior:    SRB Only   STP:  Enabled
Port:   3      Interface:      5     Behavior:    STB Only   STP:  Enabled
Port:   4      Interface:      6     Behavior:    STB Only   STP:  Enabled
```

If you want to know about the segment numbers of the segments the LEC is actually connected to, look at the dot1dBridge MIB entry dot1dSrPortTable.dot1dSrPortEntry.dot1dSrPortLocalSegment. It holds the corresponding (decimal) segment number for each port number.

When dealing with bridging interfaces of an MSS, keep in mind that bridging and routing exclude each other on this device. Hence, whenever there is a bridge port defined on an interface, you will not be able to ping the IP address that is defined on the same interface.

3.3.6 How Can We Navigate to Other Representations of ELAN Entities?

Opening the context menu of the icons of the Exploded Domain and the Exploded ELAN panel you will find the Open View-> submenu. Wherever such a view applies, it offers you access to the following views wherever such a view applies:

- ATM view
- LNM view
- Device view

3.3.6.1 Navigation to LNM Topology

Since an LECS may be located in an ATM device that implements an SNMP bridge capability it may be relevant to LNM topology.

The IBM 8210 MSS server implements SNMP bridge functionality. An ELAN emulates a logical LAN and appears in LNM topology submaps, provided it is connected to an SNMP bridge (IBM 8281 ATM Bridge for interconnection with legacy LANs or an IBM 8210 MSS Server). If an ELAN is not connected to an SNMP bridge (RFC 1493), it will not be displayed in the LNM topology. The LNM application can display legacy LANs even if they are not bridged or if their connected bridge has not yet been discovered by LNM. LNM relies on token-ring surrogates or RMON agents to discover token-ring legacy LANs. These two kinds of SNMP agents belong to its discovery plan. To make LNM discover even isolated ELANs, LNM should ask NCMA for all its isolated ELANs.

Another useful way to locate the LNM network topology is to display the IBM 8210 PSM module. By clicking on the second icon on the right-hand side of the screen the information is shown. The Bridge Designated Root value can then be used to locate the LNM segment.

Note: We′ve seen some problems with LNM submaps: bridges are never interconnected by ELANs; sometimes the ELAN names are replaced by a segment number, and some ELAN icons are not exploded (not surrounded by a square).

3.3.6.2 Navigation to ATM Topology

Opening the ATM View connection from the context menu will show you the corresponding ATM submap with the device highlighted that implements the entity you opened the submap for. This can either be the LECS or a LAN Emulation client; the option is not available on ELAN icons.

3.3.6.3 Navigation to PSM View

For the LECS and the LE client icons, the option is offered to open the PSM of the device that implements the corresponding ELAN element. It is a convenient shortcut, but you can also access the PSMs from the The PSM submap icon under the root submap. By double-clicking on this icon the PSM Subsystems icon will be displayed (see Figure 46 on page 81).

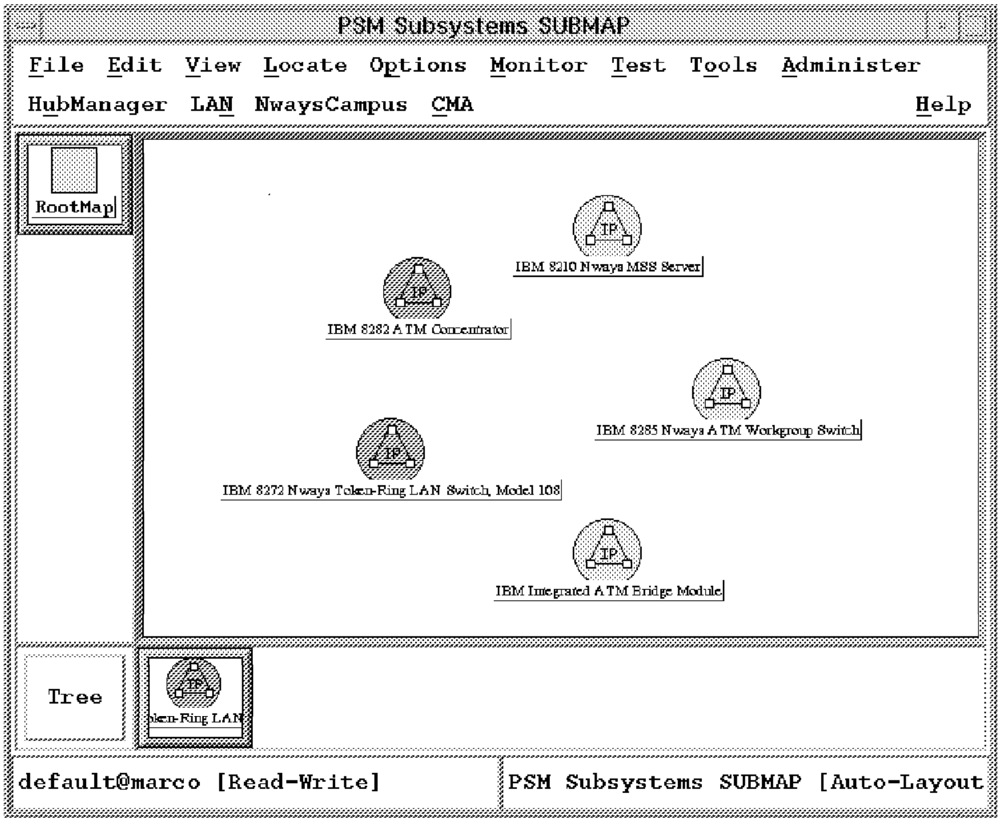

Figure 46. PSM Subsystems Submap

This submap contains four PSM icons, one for each type of device:

- IBM 8210 Nways MSS Server represents the IBM 8210 MSS Server device topology.
- IBM 8285 Nways Workgroup Switch represents the IBM 8285 ATM Workgroup Switch device topology.
- IBM Integrated ATM Bridge Module represents the 8281 ATM bridge.Rel1.0 blade in the 8260.
- IBM 8282 ATM Concentrator represents the IBM 8282 ATM Concentrator device topology.
- IBM 8272 Nways Token-Ring LAN Switch, Model 108 represents the Token-Ring switch.

Double-click on one of these PSM topology icons and open the IBM 8210 Nways MSS Server submap. All the IBM 8210 MSS Server device icons will appear (see Figure 47 on page 82).

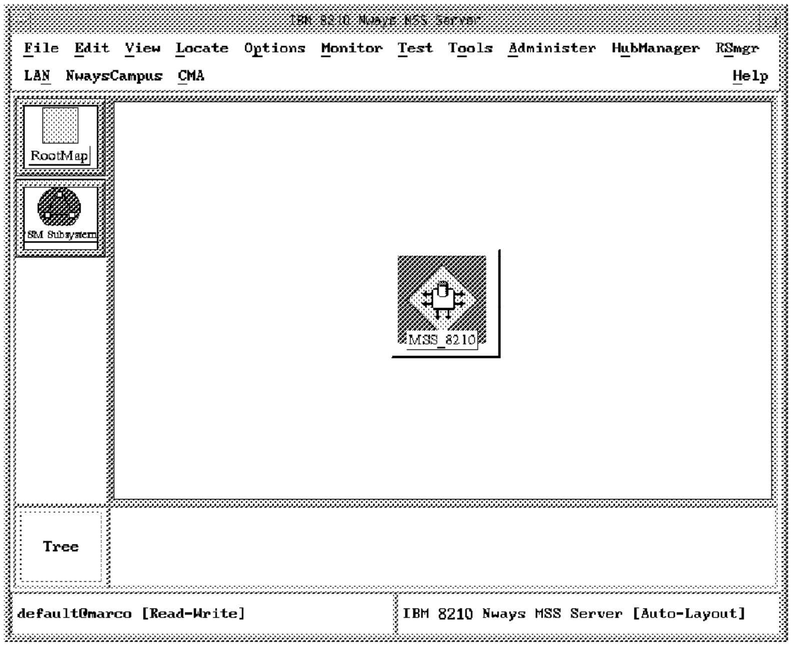

Figure 47. PSM IBM 8210 MSS Server Submap

If you double-click on an icon in this submap, the IBM 8210 MSS Server Box view will appear (see Figure 48).

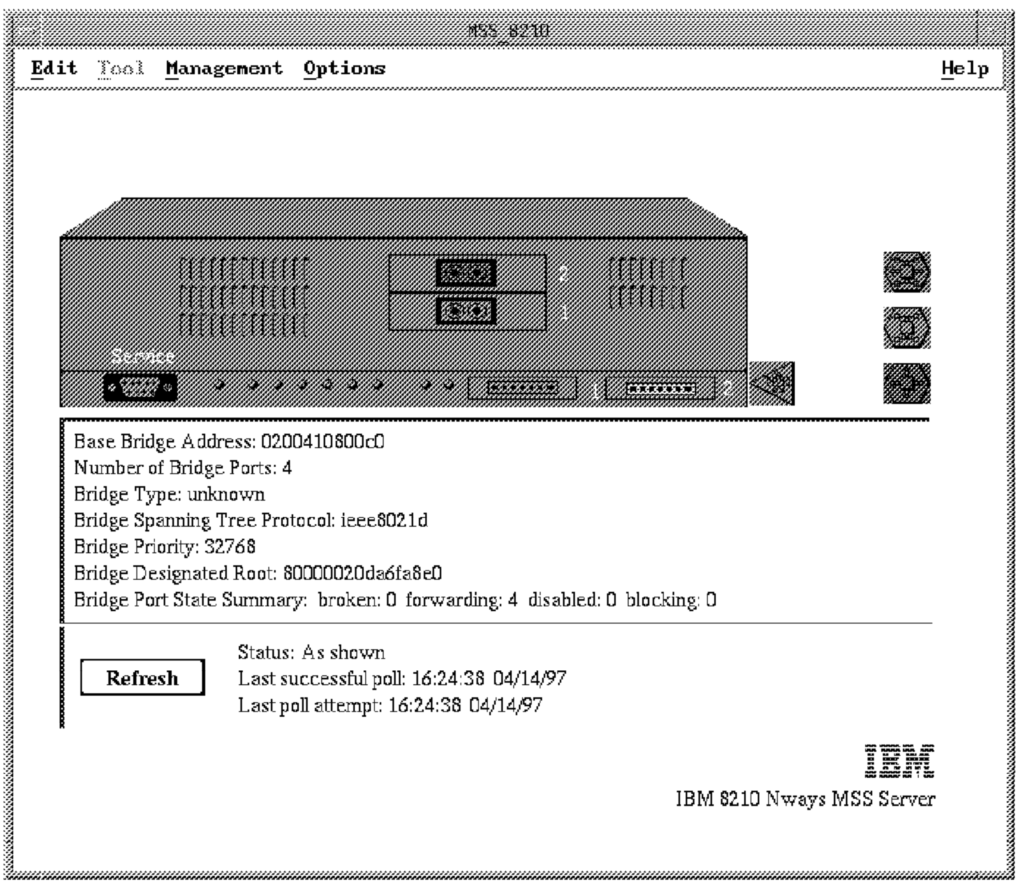

Figure 48. IBM 8210 MSS Server Box View

3.4 Other Navigational Aids

A last interesting navigation aid, which should be mentioned here is the Nways Protocol panel available from the context menu of the different representations of each device under the different protocol sections represented in the root map. Since each network object can find one or more of its representations with any of the network applications that are based upon TME 10 NetView this panel serves as an aid to access any one of them. It is available from most context menus under the Nways Protocols entry and opens as shown in Figure 49.

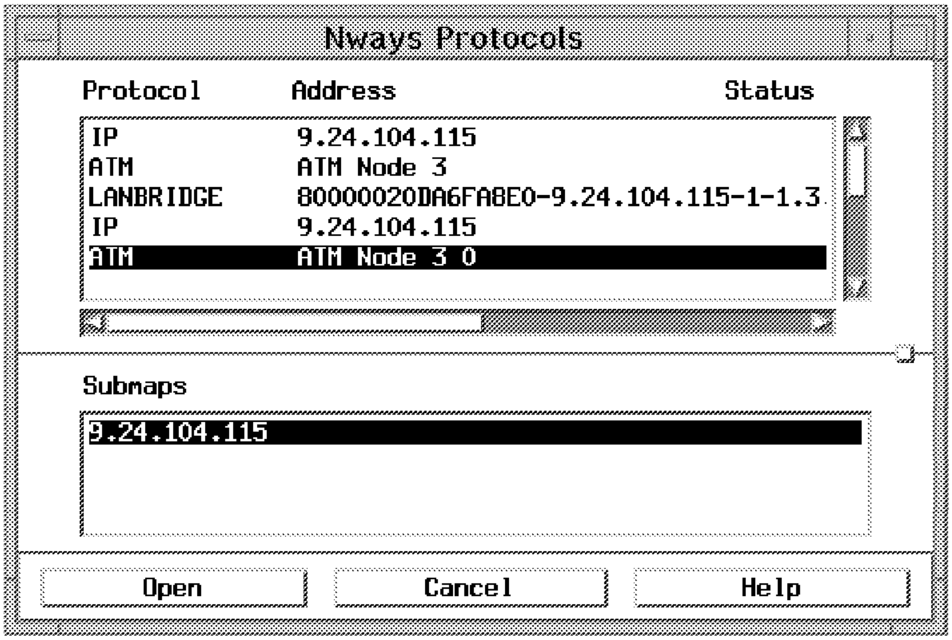

Figure 49. The Nways Protocols Panel

3.5 Nways Campus Manager ATM Command Line Functions

This section details the Nways Campus Manager ATM Command Line Interface commands installed as part of the Nways Campus Manager ATM. These commands could be used for both problem diagnostics, automated configuration or for performing remote configuration if the GUI is not accessible.

The following is a list of available commands. The command line interpreter is contained in the ahmlecmd file in the /usr/CML/bin directory. Almost all functions available from the graphical user interface are also available from this command line.

This list can be obtained by typing in the command:

```
/usr/CML/bin/ahmlecmd -Help
```

All the commands use a similar syntax.

By using these commands in shell scripts you can create a hard copy of the ELAN definitions.

Most of the LAN Emulation function can be performed from the command line including defining and deleting ELAN components.

3.5.1 Examples Using Our Database

To list the LECS issue the command:

/usr/CML/bin/ahmlecmd ListLecs -server marco

```
LECS Label                ConfId Status ATM Address
192.168.21.10-1                1      2 39098511111111111111010140008210
    Box IP Address  Box type       DBIndex
    192.168.21.10    Generic Box         4
```

The current ELANS can be listed by issuing the command:

To list the LEC information issue the command:

/usr/CML/bin/ahmlecmd ListElan -server marco

```
ELAN Label             ConfId Status LANtyp DBIndex
ETH_ELAN_8285            0      2      2     11
   LES Label              ConfId Status ATM Address
   192.168.21.85-1             1      2 39098511111111111111010340008285
TR_ELAN_8285              0      2      3     12
   LES Label              ConfId Status ATM Address
   192.168.21.85-2             2      2 39098511111111111111010340008285
ETH_ELAN_8210_1           1      2      2     17
   LES Label              ConfId Status ATM Address
   192.168.20.21-1             1      2 39098511111111111111010140008210
ETH_ELAN_8210_2           2      2      2     18
   LES Label              ConfId Status ATM Address
   192.168.20.21-2             2      2 39098511111111111111010140008210
ETH_ELAN_8285             3      4      2     19
   LES Label              ConfId Status ATM Address
   40.00.00.82.85.A1.02        0      1 39098511111111111111010340000082
TR_ELAN_8210_1            4      2      3     20
   LES Label              ConfId Status ATM Address
   192.168.20.21-3             3      2 39098511111111111111010140008210
TR_ELAN_8210_2            5      2      3     21
   LES Label              ConfId Status ATM Address
   192.168.20.21-4             4      2 39098511111111111111010140008210
TR_ELAN_8285              6      4      3     22
   LES Label              ConfId Status ATM Address
   40.00.00.82.85.A1.03        0      1 39098511111111111111010340000082
```

To list the LES information issue the command:

/usr/CML/bin/ahmlecmd ListLes -server marco

The output is shown below:

```
LES Label              ConfId Status ATM Address
192.168.21.85-1             1      2 390985111111111111111101034000828500
    Box IP Address  Box type     DBIndex
    192.168.21.85    8285             2
    BUS Label               nfId Status ATM Address
    192.168.21.85-1            1      2 39098511111111111111110103400082
192.168.21.85-2                  2 39098511111111111111101034000828500
    Box IP Address  Box type     DBIndex
    192.168.21.85    8285             2
    BUS Label               nfId Status ATM Address
    192.168.21.85-2            2      2 39098511111111111111110103400082
192.168.20.10-1                  2 39098511111111111111101014000821000
    Box IP Address  Box type     DBIndex
    192.168.21.10    Generic Box              4
    BUS Label             ConfId Status ATM Address
    192.168.21.10-1            1      2 39098511111111111111110101400082
    02.00.88.88.00.00.81       0      7 39098511111111111111110103020088
 9
```

To list the LEC information issue the command: /usr/CML/bin/ahmlecmd ListLec -server marco

A snapshot of the output is shown below:

```
192.168.21.10-1              1      2 390985111111111111111010140008210
    Box IP Address  Box type       DBIndex
    192.168.21.10    Generic Box         4
    BUS Label                ConfId Status ATM Address
    192.168.21.10-1              1      2 3909851111111111111110101400
    LEC Label                ConfId Status ATM Address
    192.168.21.10-6              6      2 3909851111111111111110101400
    02.00.88.88.00.00.81         0      7 3909851111111111111110103020
192.168.21.10-2               2      2 39098511111111111111101014000821
    Box IP Address  Box type        DBIndex
    192.168.21.10    Generic Box         4
    BUS Label                ConfId Status ATM Address
    192.168.21.10-2              2      2 3909851111111111111110101400
    LEC Label                ConfId Status ATM Address
    192.168.21.10-8              8      2 3909851111111111111110101400
    192.168.21.10-7              7      2 3909851111111111111110101400
    40.00.82.81.0A.0A.00         0      7 3909851111111111111110101400
192.168.21.10-3               3      2 39098511111111111111101014000821
    Box IP Address  Box type        DBIndex
    192.168.21.10    Generic Box         4
    BUS Label                ConfId Status ATM Address
    192.168.20.21-3              3      2 3909851111111111111110101400
    LEC Label                ConfId Status ATM Address
    192.168.20.21-9              9      2 3909851111111111111110101400
    192.168.20.21-5              5      2 3909851111111111111110101400
    192.168.4.81-1               1      2 3909851111111111111110101400
192.168.21.10-4                  4      2 3909851111111111111110101400
    Box IP Address  Box type             DBIndex
    192.168.21.10    Generic Box              4
    BUS Label                     ConfId Status ATM Address
    192.168.21.10-4                   4      2 39098511111111111111101
    LEC Label                     ConfId Status ATM Address
    192.168.21.10-4                   4      2 39098511111111111111101
40.00.00.82.85.A1.02               0      1 390985111111111111111010340
40.00.00.82.85.A1.03               0      1 390985111111111111111010340
```

Chapter 4. Configuring LAN Emulation Elements

This chapter shows what configuration tasks we can perform on our managed elements. The ATM devices can be configured by the PSM modules via the GUI interface with the exception of the IBM 8210.

The Nways Campus Manager ATM does not provide an interface to allow customization of the Classical IP. This must be performed using either a telnet session to the specific device or by using a configuration tool (for example, the MSS configuration tool for the IBM 8210).

4.1 LAN Emulation Elements

For the LAN Emulation entities (LECS, LES, BUS, LECs) the majority of configuration can be performed from the Nways Campus Manager ATM GUI. This section is about what needs to be provided for this.

The logical ELAN configuration is shown in Figure 15 on page 35.

In Chapter 4, "Configuring LAN Emulation Elements" we have gained an overview about the existing configuration of our ELAN. Changing this configuration implies:

- Creating new LAN Emulation entities
- Deleting LAN Emulation entities
- Modifying the LAN Emulation entities

Let us begin with the definition of a domain. Select **CMA->LAN Emulation** from the pull-down menu (see Figure 50 on page 88).

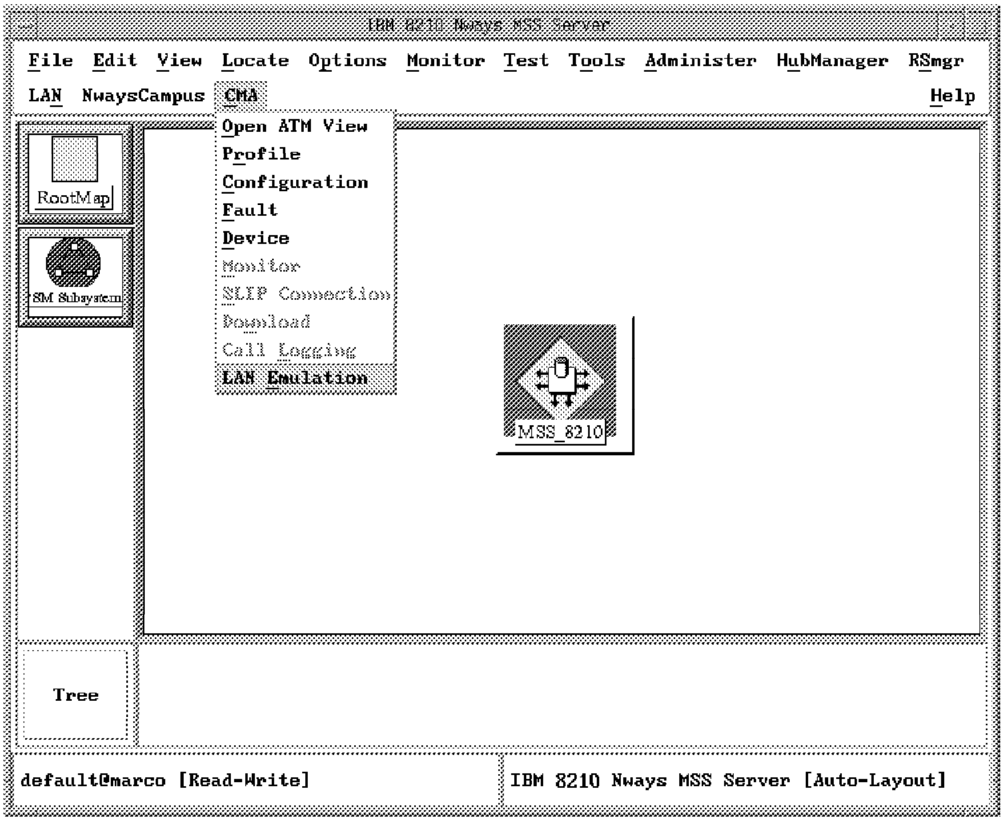

Figure 50. The LAN Emulation Context Menu

You can open the ELAN configuration panel by selecting **Control->Create Domain** (see Figure 51 on page 89).

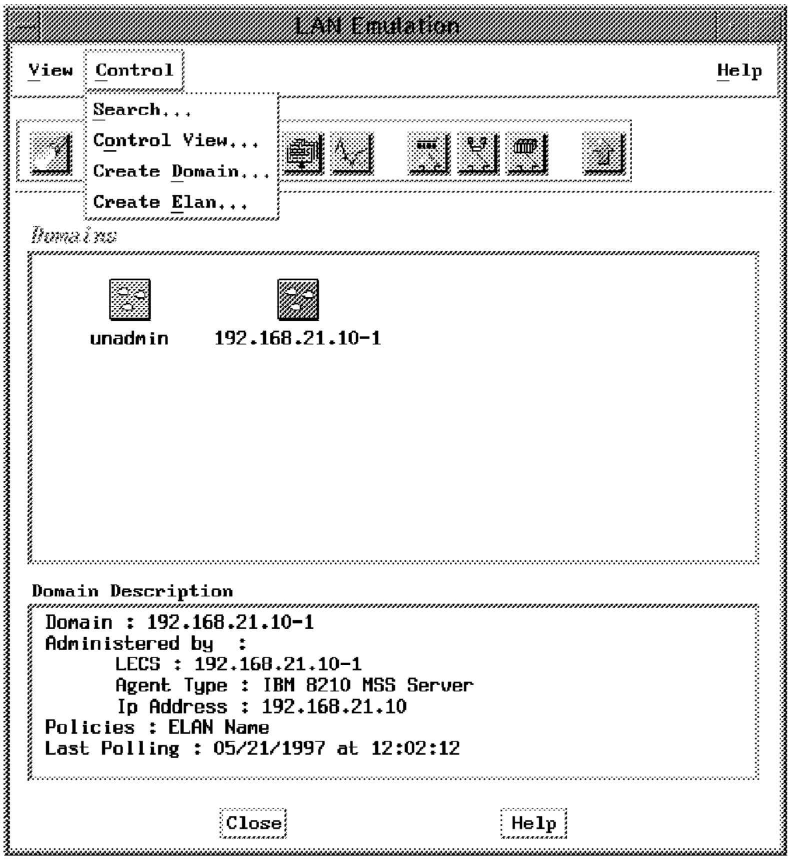

Figure 51. Calling the Create Domain Panel

The Create Domain panel is shown in Figure 52.

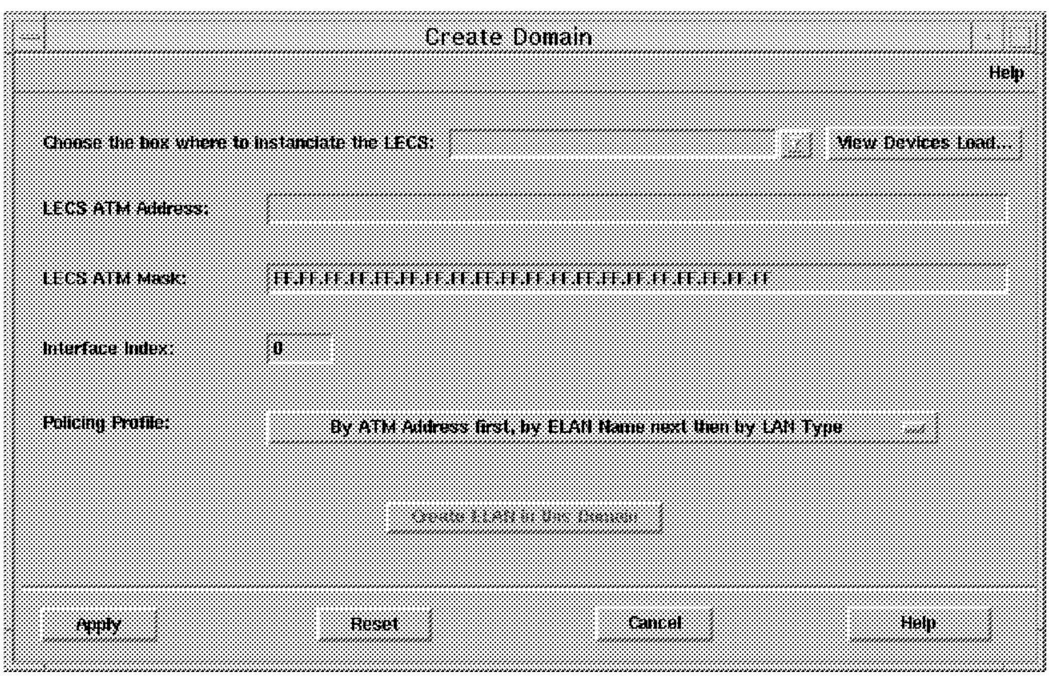

Figure 52. The Create Domain Panel

The Create Domain panel will only appear if the ATM device addressed supports LECS capability. Creating a domain involves defining an LECS with associated policy rules.

Creating policy rules is giving this LECS a general scheme to assign LECs to ELANs. It is possible that either this ATM device doesn't implement any LECS capability or it has already instantiated all its potential LECS instances. When this is the case, the Create Domain selection will fail.

You can change the six bytes of the ATM address ESI part. NCMA displays the default ESI, but you can replace it with a locally administered one.

The LECS ATM address mask is applied to the already defined ATM address in order to determine a portion of the ATM address that the LECS will use to derive its actual ATM address.

It seems that as an LECS can be listening to LE_CONFIGURE requests on more than one ATM interface, the mask is a useful method to specify one of these given ATM interfaces.

The actual address of the LECS resulting from the AND operation between the specified ATM address and the ATM address mask is computed by the LAN Emulation software running in the ATM device.

A given LECS will only use one policy profile with a hierarchical list of policies. If another LECS was activated in the same ATM device, it could be assigned another policy profile.

The policy profile applies to all the future ELANs administratively defined in this ATM device.

Click on **Apply** to send the request to the ATM device. The next step is to create administratively controlled ELANs. In order to create an ELAN in this domain select **Create ELAN in this Domain** on the Create Domain panel (Figure 52 on page 89).

Note: You do not need to create an administrative domain before creating an ELAN. You can create this ELAN by only activating an LES instance and a BUS instance.

4.1.1 Creating an ELAN

We entered the following information: the domain name is the IP address or the host name of an ATM device implementing an LECS. If a domain is selected, the panel information will be used to update the administrative data of the ELAN MIB.

The LECS and the LES do not need to be located on the same ATM device.

Specifying an ATM address and a selector byte for the new LES you should keep in mind, that this selector byte must not be in use at the moment. If you just key in the selector byte at the end of the input field for it and after doing this accidentally select the IP address from the Agent Selection scroll box again, you will find the selector byte reset to the (wrong) previous version. It may be a good idea to set the selector byte last.

The lower bound LEC ID and the upper bound LEC ID are private variables linked to a given LES implementation. They are not really required at this stage, with only a single ELAN. However, with the future support of SuperElans coming around soon, this feature will serve to avoid duplicate LEC IDs.

Notice that when first selecting the ATM device from the BUS area, the selection is not mirrored in the LES area. The ATM Forum doesn′t explicitly specify that both the LES and the BUS instances should be collocated. The Create ELAN panel allows the capability to uncouple the BUS instance from the LES instance.

The procedure below shows how we defined the BUS and LES. Starting with the BUS first, enter the IP address of the ATM device where the BUS is to be instantiated using the list box menu. When you get to the LES configuration area, don′t use the default list of ATM device IP addresses; rather, enter the ATM device IP address manually.

Note: If your ELAN creation was successful, an LES and BUS instance have been created and the ATM device LAN Emulation tables updated.

4.1.2 Configuring the Policies of a New ELAN

If the ELAN is administered, you must specify policy values for this ELAN. These policy values will refer to this particular ELAN. If at the time of creating your domain you have chosen a general policy rule by ELAN name, this policy rule will apply to all the ELANs controlled by the same LECS. Consequently, there is a specific policy value for each different ELAN. For every LEC the LECS will then try to determine from the values specified by the LEC what ELAN this LEC is going to join. The overall policy rule prescribes the order the LEC provided values are tested.

The ELAN specific values you are about to enter here will serve as comparison values of whether or not this LEC should join this ELAN.

The LECS will analyze the policy values tables to find a match between the field value found in the LE_CONFIGURE request sent by the LEC and an entry in these tables.

If the ELAN is not administered, then you just have to enter in each LEC the ATM address of the ELAN LES.

If your ELAN creation is successful and your ELAN is administered, the Configure policy button at the bottom of the Create ELAN panel is now highlighted. Click on it to display the Policy Configuration panel below.

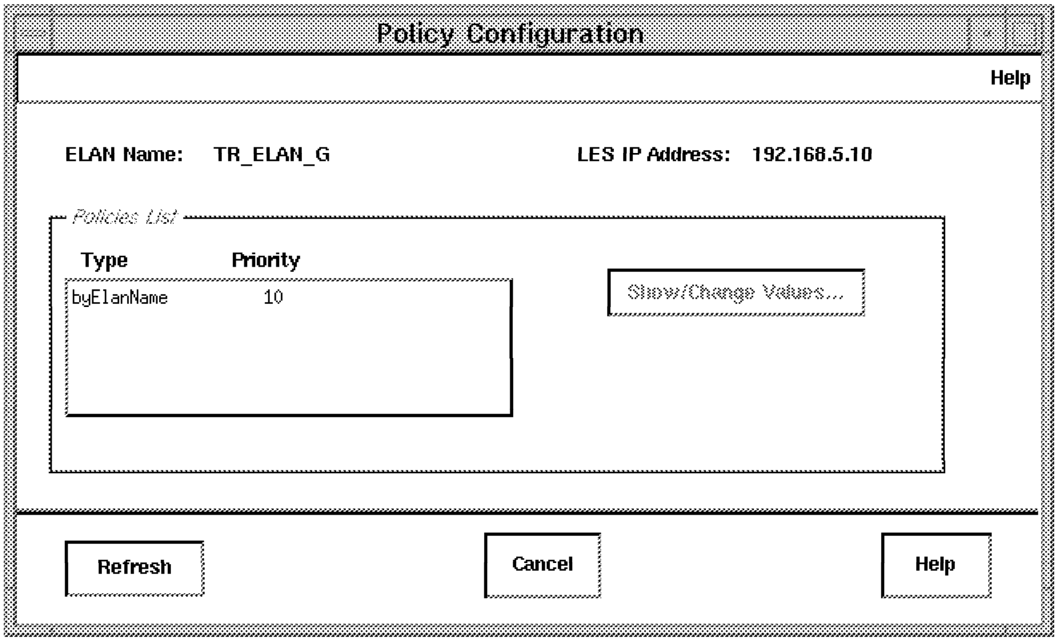

Figure 53. Policy Configuration for a Newly Created ELAN

This panel allows the configure policy values to be entered for a newly created ELAN and refers to this ELAN by the ELAN name and the IP address of the ATM device implementing the LECS. The most relevant information is the priority type and priority, shown in the diagram as byElanName and 10 respectively.

Alternatively the policies can be added later by selecting the domain, by using the right-hand mouse button and choosing configuration.

To enter the policy values of this ELAN, enter an ELAN name in the New Policies Values field and click on the **Add this Entry push button**. The ELAN Name Area is updated by the new ELAN name.

Note: You can enter more than one ELAN name in the ELAN Name Area by repeating this procedure. The By ELAN Name table is appended with the new values entered. Even if there is only a single name in the table, this name does not necessarily have to be the name of the ELAN which you specified when creating it. What you specify here is just a value which is to be compared to the ELAN name specified in the LE_CONFIGURE request sent by an LEC.

The administrative ELAN name is used by the LECS in LE_CONFIGURE response frames. The link between the administrative ELAN name and the ELAN name (defined in the the policies values table elanLecElanName) is done by double indexing the policies values table.

To allow an LEC to join this ELAN we need to configure this LEC′s ELAN name with one of the ELAN name′s entered in the policy value By ELAN Name table.

When the LEC sends its LE_CONFIGURE request to the LECS, the LEC ELAN name will match the ELAN name of the By ELAN Name table, and the LEC will receive the ATM address of the LES in the LE_CONFIGURE response.

4.1.3 Deleting ELAN Entities

At any time, you can delete an ELAN by clicking on an ELAN icon in the LAN Emulation Administrative Domain view with the right mouse button. Next, select **Delete**.

Deleting a domain will de-activate the LECS instance in charge of it, and will remove all the ELAN-related information from the ELAN table associated with the LECS. It won′t de-activate the LES and the BUS instances associated to each ELAN. Nevertheless if an already connected LEC reboots for any reason, it wouldn′t be able to find its LES ATM address and should be set up again in manual mode.

4.1.4 Creating a Redundant LES/BUS

One thing you may want to modify after ELAN configuration is the definition of a backup LES/BUS pair for your ELAN. In order to do this, select the **Administration** option in the context menu of the ELAN shown in the Exploded ELAN panel below.

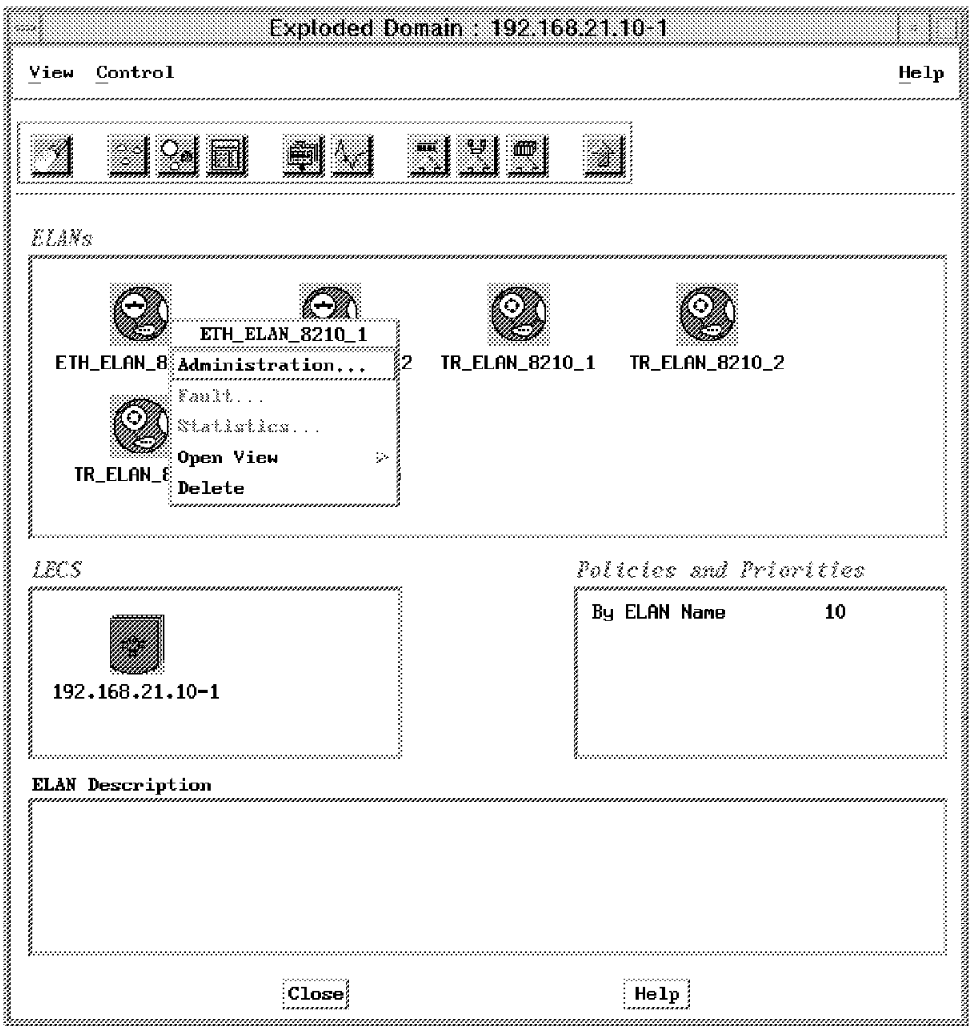

Figure 54. Administering an ELAN

The ELAN Administration panel is displayed (see Figure 55 on page 94).

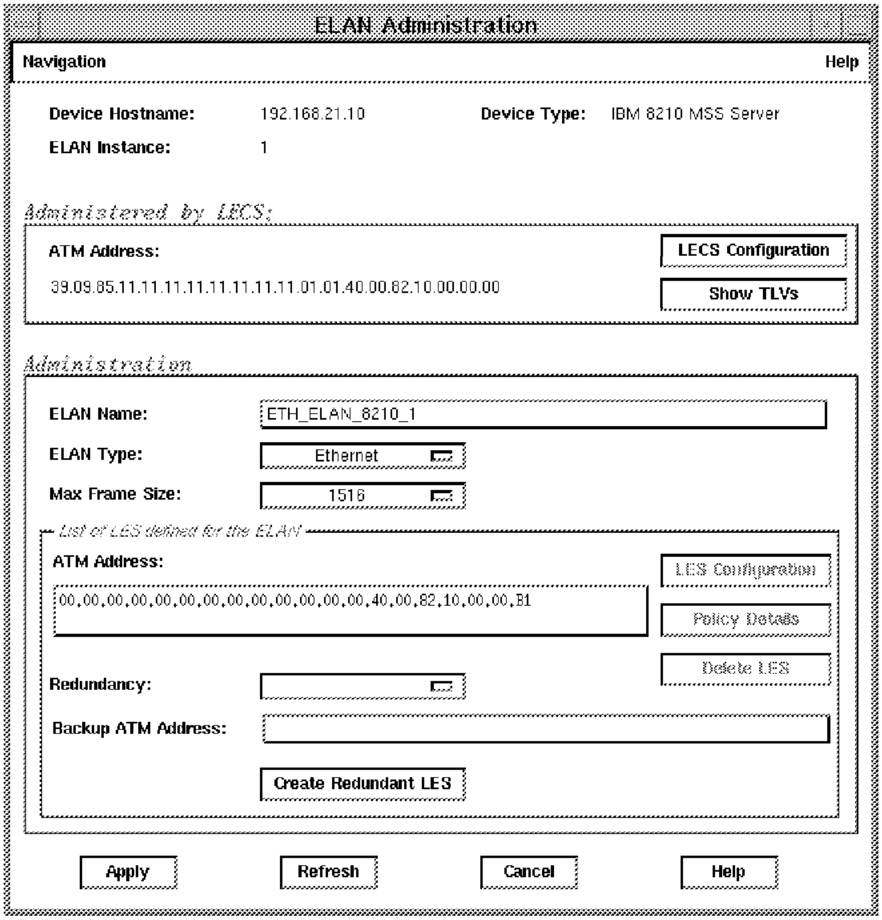

Figure 55. The ELAN Administration Panel

This panel shows administrative data for the ELAN domain.

Creating a redundant LES/BUS for this ELAN will provide added contingency to an ELAN.

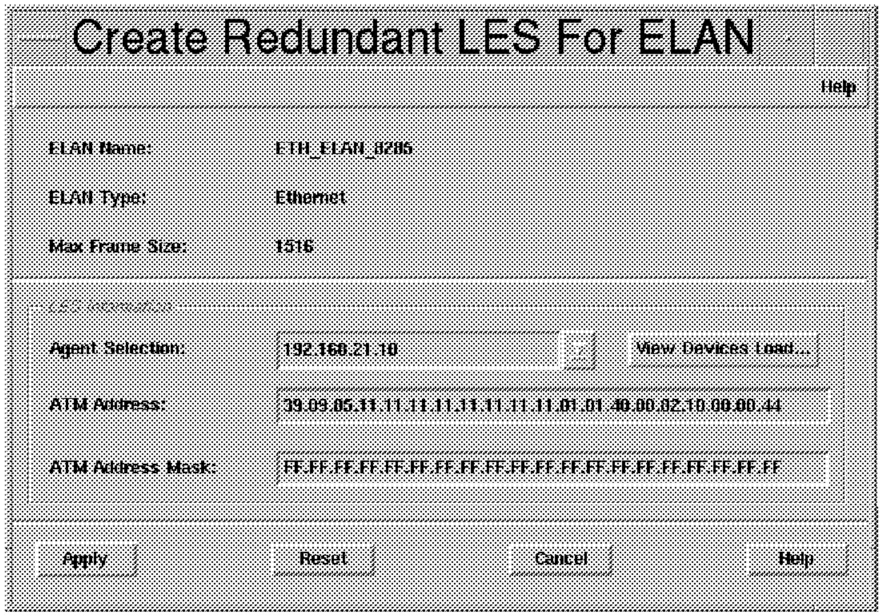

Figure 56. The Create Redundant LES for ELAN Panel

In the case of the primary LES/BUS failing, the backup LES/BUS will be activated by detecting that the VCC to the primary LES/BUS is no longer present. Hence the backup will start servicing LEC LE_JOIN requests.

When the primary LES/BUS is operational (the redundancy VCC is up), the backup LES/BUS will not accept control direct VCC calls and will force requesting LECs to repeat the configuration phase (LE_CONFIGURE requests to the LECS).

When detecting a failure via released VCCs, the LECs will re-send LE_CONFIGURE requests to the LECS. Upon receiving the LE_CONFIGURE request, the LECS assigns the LEC to the appropriate ELAN, and then issues a local query to determine if there is a local LES active, as either primary or backup, for the ELAN.

If there is an active local LES, the query returns the real ATM address of either the local LES or the primary LES at the other end of the redundancy VCC, based on the configured role of the local LES and the current status of the redundancy VCC.

If there is no active local LES for the ELAN, the LECS uses an algorithm to select the ATM address to be returned to the LEC. In this case, the LECS has no knowledge of the redundancy VCC between the two LESs since both the primary and the backup are external to its ATM device.

To implement the heuristic, the LECS maintains a short-memory of the LES ATM address that was last provided to each LEC (five minutes). If the LECS has no short-memory for a given LEC, the ATM address of the primary LES is returned to the LEC; otherwise, if the LEC returns to the LECS within 5 minutes of its last configuration request, the LECS alternates between the primary and backup LES.

This panel allows you to create a redundant LES and BUS instance for the currently operating LES and BUS. In both the active LES/BUS and backup LES/BUS, redundancy information is appended. You can choose the IP address of the ATM device implementing the backup LES and BUS instances, the ATM address and the ATM address mask of the redundant LES/BUS instance.

The creation of a redundant LES (in fact, a redundant LES/BUS pair) is not ATM Forum LAN Emulation-compliant. It′s a private implementation of IBM for the IBM 8210. Therefore, this redundancy option requires two IBM 8210 servers in its network.

4.1.5 LECS Policy Configuration

The LECS Configuration panel is located by clicking on **LECS Configuration** (see Figure 57).

Figure 57. The LECS Configuration Panel

To customize the LECS parameters select a policy rule (By LAN type, By MAC Address, By ELAN Name, By Route Descriptor, By ATM Address, By Packet Size) and a policy priority, and then click on the **Apply** push button to validate. The new policy rule is immediately appended in the LECS Configuration panel Policy Profile area. That means the LECS will use this new policy rule to assign LECs to the appropriate LES. In case you specify a new rule at the same priority level as the previous ones, make sure you have a value ascribed for this rule with every ELAN administered by the LECS. Otherwise the LECs will have trouble joining these ELANs again.

You can delete an existing policy rule by selecting a policy rule entry in the LECS Configuration Policing Profile area and then by selecting **Delete**. The policy rule is immediately removed from the policy rule and the LECS will no longer use it to assign LECs to ELANs.

Note: The LECs already assigned to a given ELAN following the deleted policy rule won′t be disconnected from their ELAN, until they reboot. They will then send an LE_CONFIGURE request to the LECS which may in turn assign them to another ELAN (another LES ATM address).

If you have deleted a given policy rule, all the related entries in the policy values table are automatically removed.

4.1.6 Configuring the Security Feature

From the ELAN Administration panel in Figure 55 on page 94 you can navigate to the LES Configuration panel.

The ATM device-related area displays the ATM address of the ATM device implementing this LES, the type of this ATM device, and the LES instance number.

The Configuration area presents current configuration parameters of this LES instance.

Options area depending on the ATM device type: Security refers to the capability of the LES to force LECs to use LE_CONFIGURE requests before joining an ELAN.

To our best knowledge, only the IBM 8210 MSS Server implements this security function. If you use this feature, the LES will establish a VCC with the LECS and act as a proxy forwarding LE_CONFIGURE requests on behalf of LECs. If the LECS answer is OK, then the LES will accept the LE_JOIN request; otherwise, it will be rejected.

Even if an LEC has already connected to an LECS, the (security) LES will issue an LE_CONFIGURE request on behalf of this regular LEC.

When an LEC sends an LE_ARP request to its LES for a given MAC address, if the given LES doesn′t have the information in its ARP table it will forward this LE_ARP request to *all* its known LECs over its *single* control distribute VCC. It makes sense for proxy LECs to be sent such LE_ARP requests as their MAC addresses potential is important, but no sense at all for standard LECs whose MAC addresses have been already registered by the LES. IBM 8210 MSS Server implements two control distribute VCCs: one for the proxy LECs and one for the standard LECs.

4.1.6.1 Forcing an LEC to Disconnect from the ELAN

The Registered LAN Emulation Clients (LECs) area shows the list of all the LECs that have already joined this LES ELAN. You can select one LEC and by clicking on the **Unregister** push button force it out of the ELAN. You can also select an LEC entry and click on the **Details** push button to get more details about this LEC. The LES-LEC Details panel is displayed (see Figure 58 on page 98).

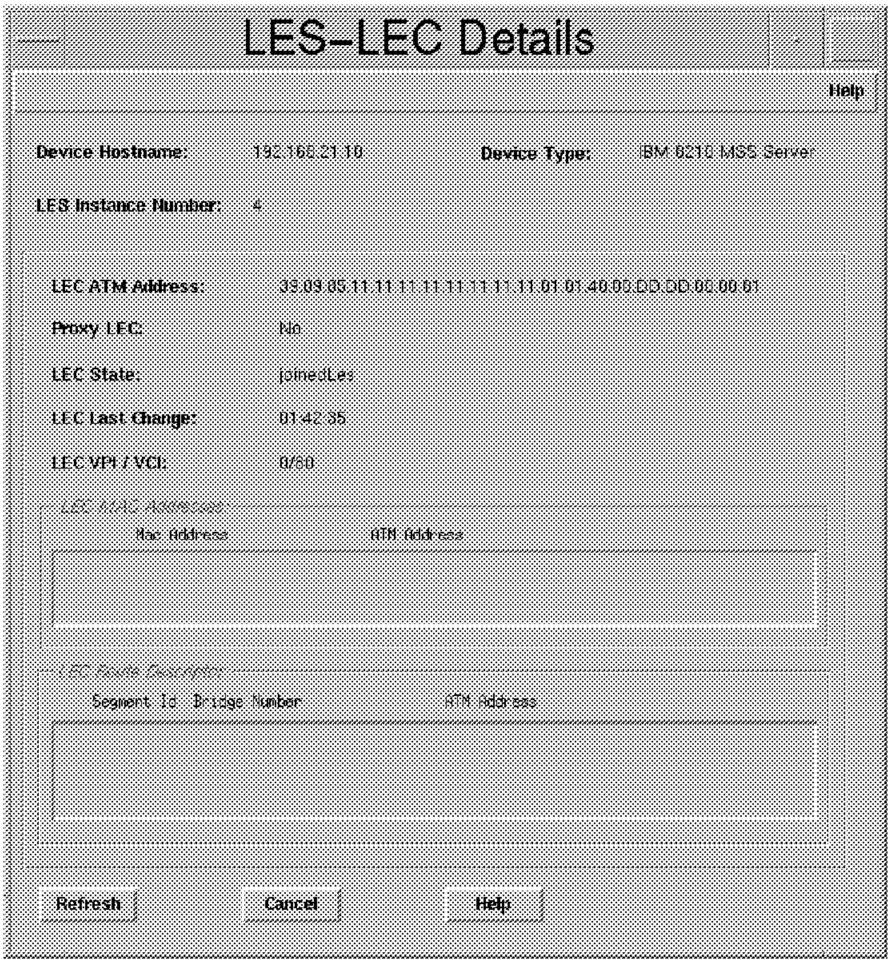

Figure 58. The LES-LEC Details Panel

Most of the information shown is contained in the LES LECs table showing all the LECs that have joined or attempted to join the ELAN.

The values should come from either the LES MAC Address ARP table for standard LEC and transparent bridging proxy LECs or the LES Route Descriptor ARP table for source routing LECs

4.1.6.2 BUS Information

If two multicast forward VCCs are used, the BUS will not broadcast unicast frames to all LECs. Instead, unicast frames destined to non-proxy LECs will be transmitted directly to the destination LEC over a control direct VCC, and all other unicast frames will be only transmitted directly to proxy LECs using proxy multicast forward VCC.

This is an IBM private implementation, and the BUS has knowledge of the LEC type proxy or non-proxy, through the LES. One advantage of this intelligent BUS or IBUS mode is a reduction in client unicast frames not destined to the client.

The Broadcast Manager field allows to activate the Broadcast Manager (BCM). The principal task of the BCM is to improve overall performance and efficiency by reducing both network traffic and endstation processing overhead associated with filtering nuisance broadcast frames.

Without BCM, every multicast frame sent to the BUS is forwarded to all LECs on the ELAN. Furthermore, LECs that include the proxy function to provide bridging support then forwards the broadcast frame onto other LAN segments. All endstations receive and process every broadcast frame. BCM can be configured for IP, IPX and NetBIOS on individual ELANs.

When enabled, a minimum amount of layer 2 and layer 3 information is decoded for specific types of broadcast frames sent to the BUS. Whenever possible, BCM transforms broadcast frames into unicast frames, and sends them only to interested LECs and endstations.

The BUS Monitor field allows you to activate the BUS monitoring function. The BUS Monitor provides a way to identify end users that are over-utilizing the BUS. When enabled, the BUS Monitor periodically samples the traffic sent to the BUS on a particular ELAN.

At the end of each sample interval, the BUS Monitor identifies the top users of the BUS by their source MAC addresses, LEC ATM addresses, and the number of sampled frames each of them sent to the BUS. The sample rate is configured via the Campus Manager interface.

If you set Bus Monitor to On, the setting of the BUS monitoring function and the sample rate are available. The BUS Monitor Statistics push button highlights. If you click on it, the Nways Manager Statistics Interface panel appears.

The Connected LECs area presents the list of all the LECs having established a multicast send VCC with the BUS, with their ATM addresses and the VPI/VCI of the multicast send VCCs at the BUS endpoint.

4.1.7 LEC Configuration

LEC creation is not currently implemented by Nways Campus Manager ATM. IBM 8210 MSS Server is an exception and a network manager could remotely create LECs through SNMP requests. The Nways Campus Manager ATM assumes that the LEC instance has already been created by any local means and addresses only the LEC configuration management area.

To get to the LEC Configuration panel, double-click on the LEC icon in the LAN Emulation ELAN view, or from the Device Configuration panel, click on the **Configuration** push button. The LEC Configuration panel is displayed, containing the following information:

- ATM device host name, type and LEC instance number.
- The Used By read-write field points to the entity that configured this entry and is therefore using the resources assigned to the LEC.
- The Desired LES Access selectable field allows you to set the way the LEC will join the ELAN at next restart (thru an LECS or directly).
- The Actual LES Access read-only field displays the way the LEC has joined its ELAN during this current session.
- The Desired LECS ATM Address read-write field allows you to specify the address of an LECS. This LEC will ask for configuration parameters at next restart.

4.2 Examples of Creating New ELAN Entities

Although our exploration chapter assumed that the network would already be there, it is interesting to look at the process required to set up an at first simple, then increasingly complex, network structure.

The first stage was to configure the IBM 8210. The scenario here was developed before the installation of AIX 4.2.1 on our Network Management Station. You will hence find ATM Classical IP connections only for this machine.

What you should keep in mind generally is that it may lead to a lot of confusion occasionally, if there is more than one way out of your Network Management Station to the different devices of your network. The four-way access to the MSS via ELAN token-ring, ELAN Ethernet, legacy token-ring and Classical IP was by no means required for any particular purpose. It was just a convenient way of showing the different options you have. In fact *any* IP connection you can establish to the devices you want to manage will serve this purpose.

For the following examples we used a different connection to the ATM network, running NetView from marco with an IP address of 192.168.20.10 on the ATM interface.

4.3 Creating LAN Emulation Elements Scenario

The purpose of LAN Emulation is to continue using already existing applications and to provide connectivity with legacy LANs at the same time. We require a connection to be established between a LAN Emulation workstation and a legacy LAN workstation through an IBM 8281 ATM bridge. The procedure is as follows:

1. Define the Network Management Station as an ARP client.
2. Resolve our ARP server configuration in the IBM 8210.
3. Configure an LEC in the MSS.
4. Assignment an IP address to the LEC.
5. Create a domain in the IBM 8210.
6. Create an administered ELAN in the IBM 8210.
7. Configure the the 8281 ATM bridge.
8. Configuration of an ATM LAN Emulation endstation.

The scenario shows how we can interconnect an ATM workstation into a specific ATM ELAN.

4.3.1 RISC System/6000 ARP Configuration

The Classical IP server address is as follows:

```
39.09.85.11.11.11.11.11.11.11.11.01.01.50.00.82.10.00.00.10
```

We added a route from marco to the other subnetworks on the 192.168 network as follows:

```
route add -net 192.168.0.0 -netmask 255.255.0.0 192.168.20.10
```

4.3.2 Configuring an ARP Server in the MSS

From the IBM 8210 command line we can see the ARP server address we needed for our configuration. This was:

```
MSS_A Config>prot arp
ARP user configuration
MSS_A ARP config>list atm-arp

ATM Arp Clients:
--------------------------------------------------
If: 0  Prot: 0  Addr: 192.168.20.10    ESI: 50.00.82.10.00.00  Sel: auto
Server: Yes  Refresh T/O: 5    AutoRefr: no    By InArp: yes  Validate PC
Use Best Effort: yes/yes  (Control/Data)   Max B/W(kbps):      0
Cell Rate(kbps):  Peak:      0/     0      Sustained:      0/     0
Max SDU(bytes):   9188
```

By using the smit interface we defined marco with the following definitions (see Figure 59).

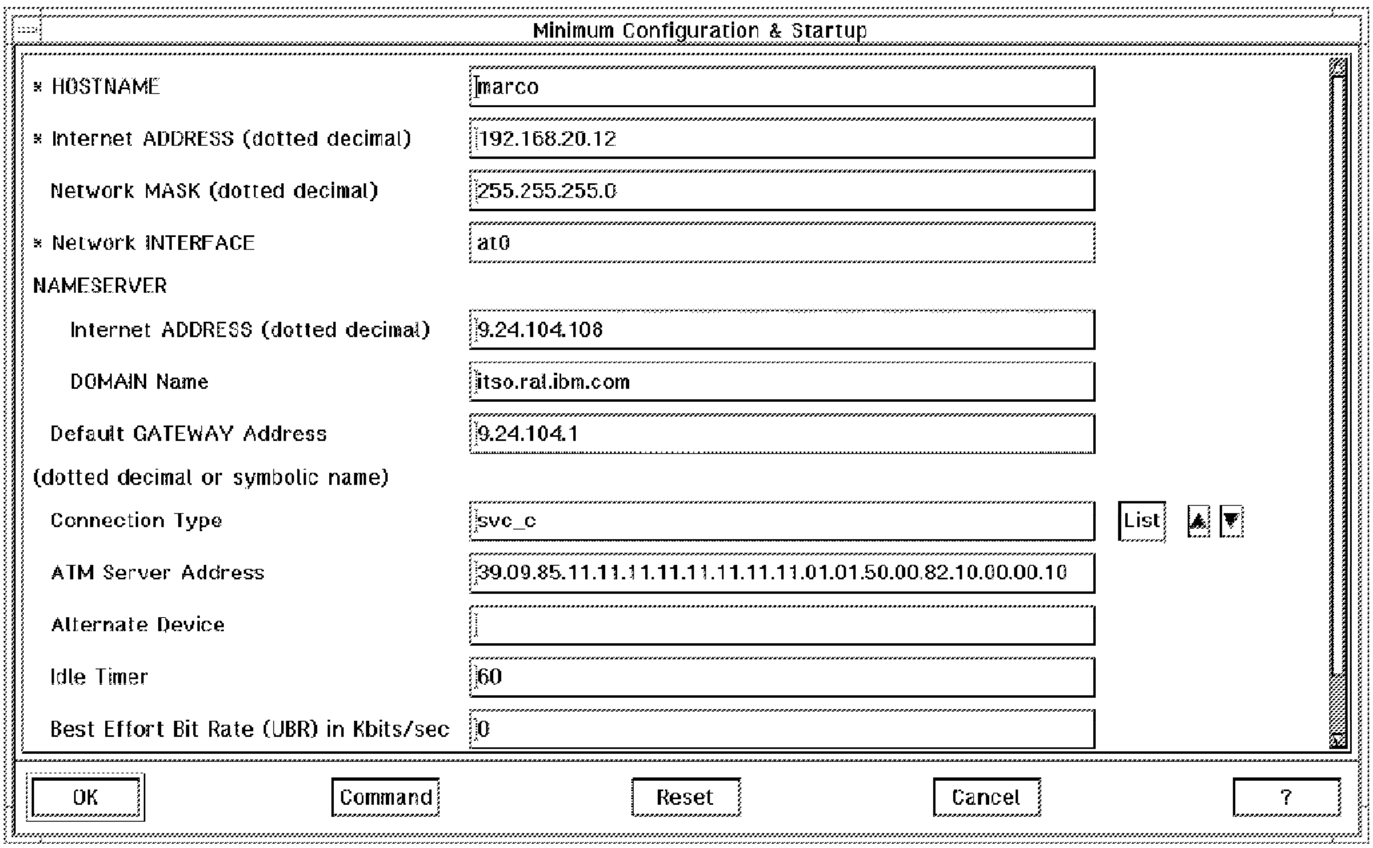

Figure 59. Configuring the ATM ARP Server Address

To verify the Classical IP address use the following command:

```
*t 6
Config>
Config>protocol
Protocol name or number [IP]?
IP config>list
```

We can now access the MSS device from marco.

4.3.3 Configuring the ELAN

The next step is to configure our ELAN by first defining the LAN Emulation entities (LECS, LES and BUS).

We want to verify what the IP addresses are of the associated virtual interfaces for the IBM 8210.

Associated to these virtual interfaces (in our case the IP address of 192.168.20.10) is connected to the internal LAN Emulation clients.

The IBM 8210 automatically enables the routing capability between these two IP interfaces LECs ATM devices over our new ELAN if they implement an IP stack.

Note: The creation of the Lan Emulation Clients has to be performed manually as the capability for this does not exist in Nways Campus Manager ATM.

4.3.4 The Virtual Interface (LEC) in the MSS

To view a virtual interface in the IBM 8210 we use the procedure shown below:

```
Config>network
Network number [0]?
ATM user configuration
ATM Config>le-client
ATM LAN Emulation Clients configuration
LE Client config>add token-ring
Added Emulated LAN as interface 1
LE Client config>con
Emulated LAN interface number [1]?
ATM LAN Emulation Client configuration
Token Ring Forum Compliant LEC Config>set elan-name
Assign emulated LAN name []? TR_ELAN_8210_2
Token Ring Forum Compliant LEC Config>SET ESI
Select ESI
   (1) Use burned in ESI
   (2) 40.00.82.10.00.00
   (3) 50.00.82.10.00.00

Enter selection [1]? 2
Token Ring Forum Compliant LEC Config>SET MAC
Use adapter address for MAC? [Yes]: NO
MAC address [00.00.00.00.00.00]? 40.00.82.10.00.00
Token Ring Forum Compliant LEC Config>SET SELECTOR
Selector byte for primary ATM address in hex [2]? 10
Token Ring Forum Compliant LEC Config>
```

We have now created an emulated LAN interface whose interface number is: [1]. We now have two interfaces in our MSS. Let′s assign an IP address to the new interface.

The LECSs can be viewed as follows:

4.3.5 Assigning an IP Address to a Virtual Interface (LEC)

```
Token Ring Forum Compliant LEC Config>
Token Ring Forum Compliant LEC Config>EX
LE Client config>EX
ATM Config>EX
Config>PRO IP
Internet protocol user configuration
IP config>ADD ADD
Which net is this address for [0]? 1
New address [0.0.0.0]? 192.168.4.10
Address mask [255.255.255.0]?
IP config>
```

The two interfaces now have IP addresses associated with them. The ATM physical interface is assigned 192.168.20.10 on subnet 192.168.20 and the LAN emulated virtual interface is assigned 192.168.4.10 on subnet 192.168.4. Our MSS activates its IP routing capability between these two IP subnets. The subnet 192.168.4 will be used for for our ELAN.

Verify the ARP connection by issuing the command:

`arp -t atm -a`

4.3.6 Creating a Domain

Now we can define the administered ELAN. From the NetView root map:

1. Double-click on the **LAN Emulation** icon.
2. Select **Control** followed by **Create domain** (see Figure 60 on page 104).

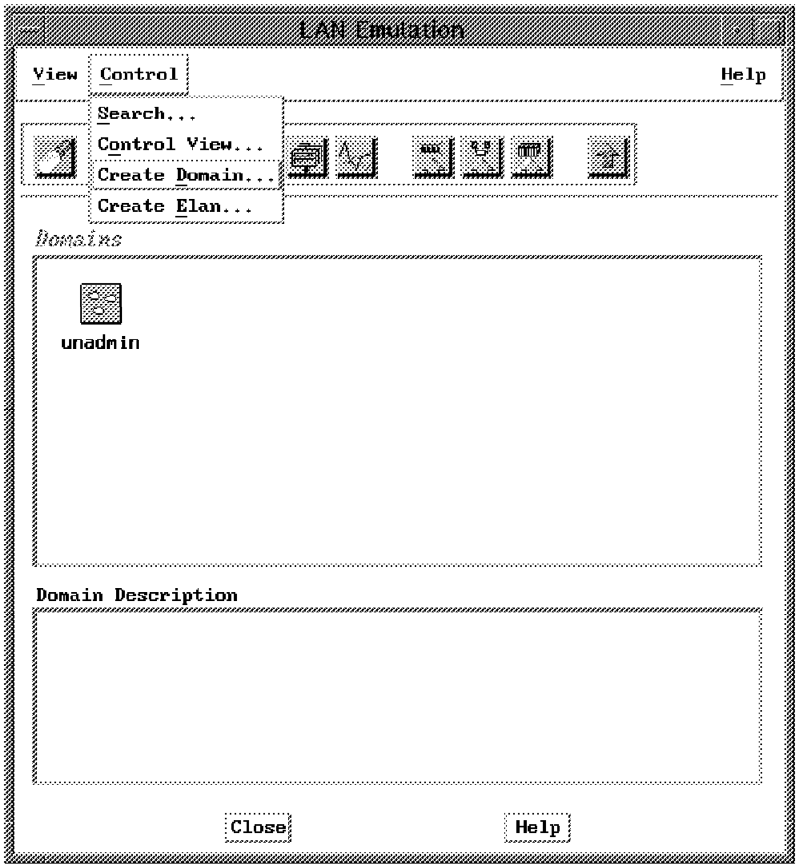

Figure 60. Selecting the Create Domain Option

3. Select the IBM 8210 IP address **192.168.20.10** for the device where you want the LECS to be defined.

4. Enter the ATM address for this LECS instance.

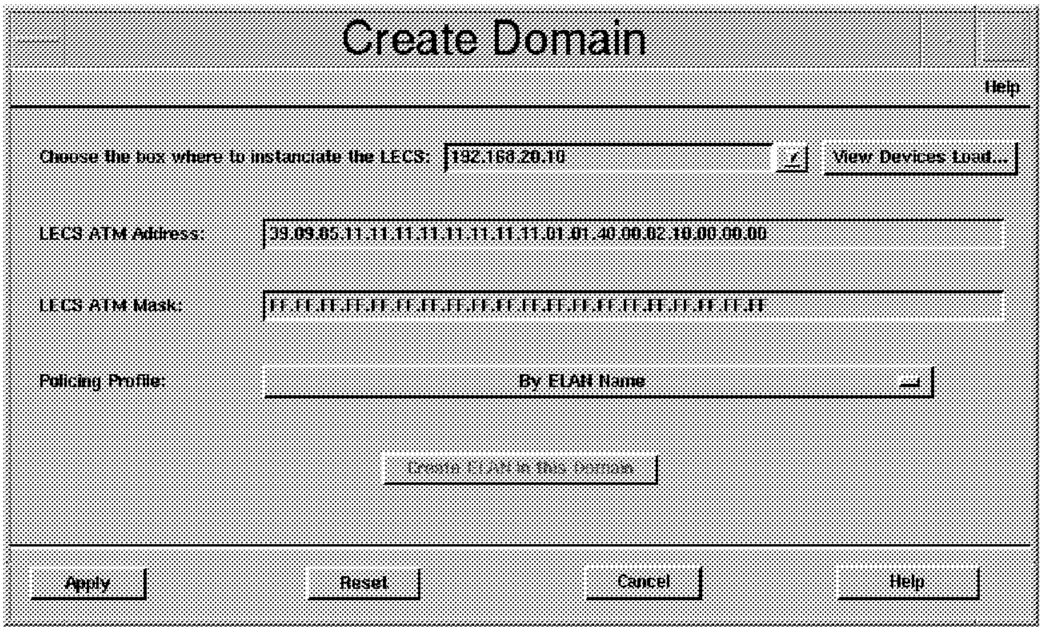

Figure 61. Configuring the Domain

For the policy profile we chose **By ELAN Name**. Let′s validate by selecting **Apply**. The LAN Emulation submap shows a new domain icon: 192.168.20.10-2.

The next stage is to define our ELAN.

4.3.7 Creating an ELAN

From Figure 62 on page 106 we select **Create ELAN**.

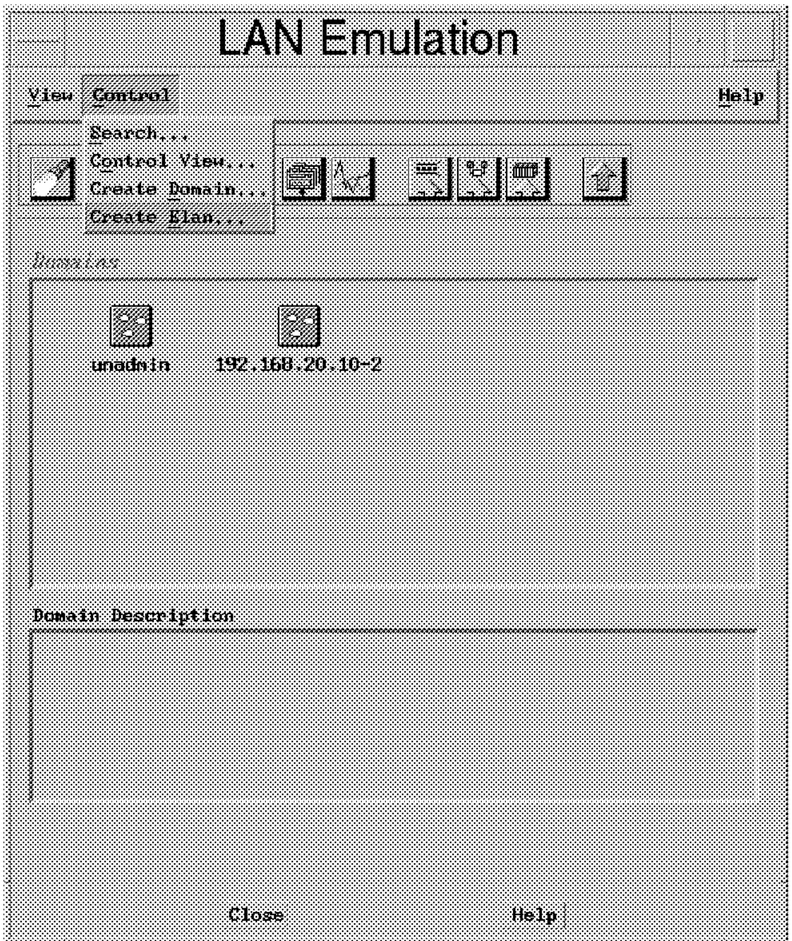

Figure 62. Create an ELAN

The ELAN name selected was **TR_ELAN_8210_2**.

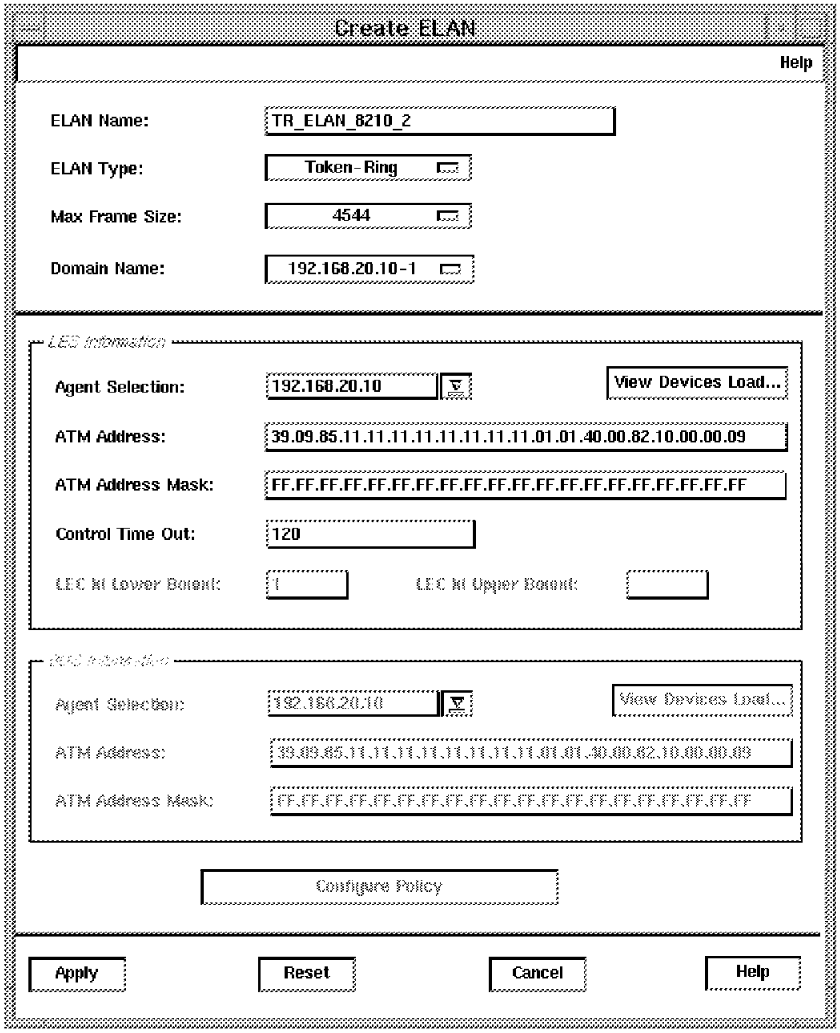

Figure 63. ELAN Definition

Here we selected the ESI part the ATM address of the LES/BUS instance, as the LES/BUS instance ATM device will register their ATM address to the local ATM switch.

The 8210 device implementing our LES instance supports only collocated LES/BUS instances.

Note: Verify that the selector byte is not already in use by another LAN Emulation instance.

Select **Apply** to perform the validation.

If we double-click on our domain icon in the LAN Emulation Network submap and open the LAN Emulation Domain submap we find our ELAN icon **TR_ELAN_8210_2**. If we double-click on this icon we can view the ELAN submap. In the Create ELAN panel the Configure Policy panel is now highlighted.

We selected **By ELAN Name**. Now we can set policy values for our ELAN. Click on **Configure Policy** and the Policy Configuration by ELAN Name panel is shown.

4.3.8 Configuring Policy Values

In the New ELAN Name field we entered the ELAN name value that the LECS instance will associate to our LES instance ATM address TR_ELAN_8210_2. This new ELAN name immediately appears in the ELAN Name field.

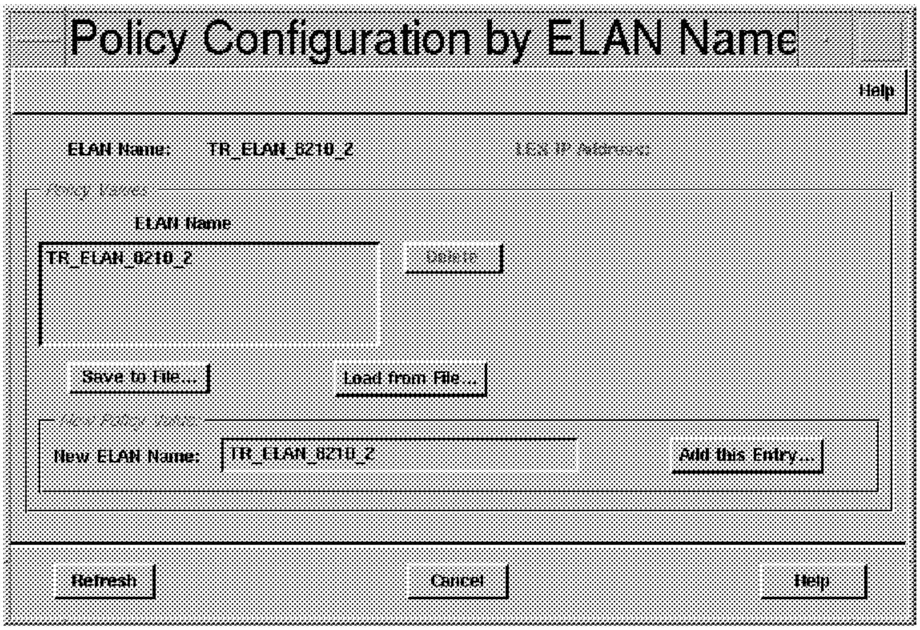

Figure 64. Configuring Policy Values for This ELAN

The LECS upon reception of LE_CONFIGURE requests will check the ELAN name field of this request and whenever it contains the value TR_ELAN_8210_2 it will return the LEC ATM address of our LES instance.

We can add more than one ELAN name, in the same policy value table If two LECs have different ELAN names in their LE_CONFIGURE request, but if these ELAN names have been entered in the same policy value table, both LECs will be sent the same LES ATM address and consequently belong to the same ELAN.

Now that the ELAN TR_ELAN_8210_2 ELAN is defined we can add our LAN Emulation clients.

4.3.9 Configuring the IBM 8281 ATM Bridge

To interconnect our legacy LAN network to the ELAN network we configured the IBM 8281 LAN Emulation capability. We must configure the bridge LEC in such a way that it will join TR_ELAN_8210_2 ELAN.

Note: Here we could have used the OS/2 8281 configuration tool to set up our 8281 bridge.

From the 8281 ATM port configuration we get to the ATM Virtual Token-Ring Port Configuration.

Using the 8281 PSM we configured the LAN Emulation to join the correct ELAN.

From the PSM submap double-click on the PSM icon representing the 8281 bridge. This will show screen Figure 65 on page 109.

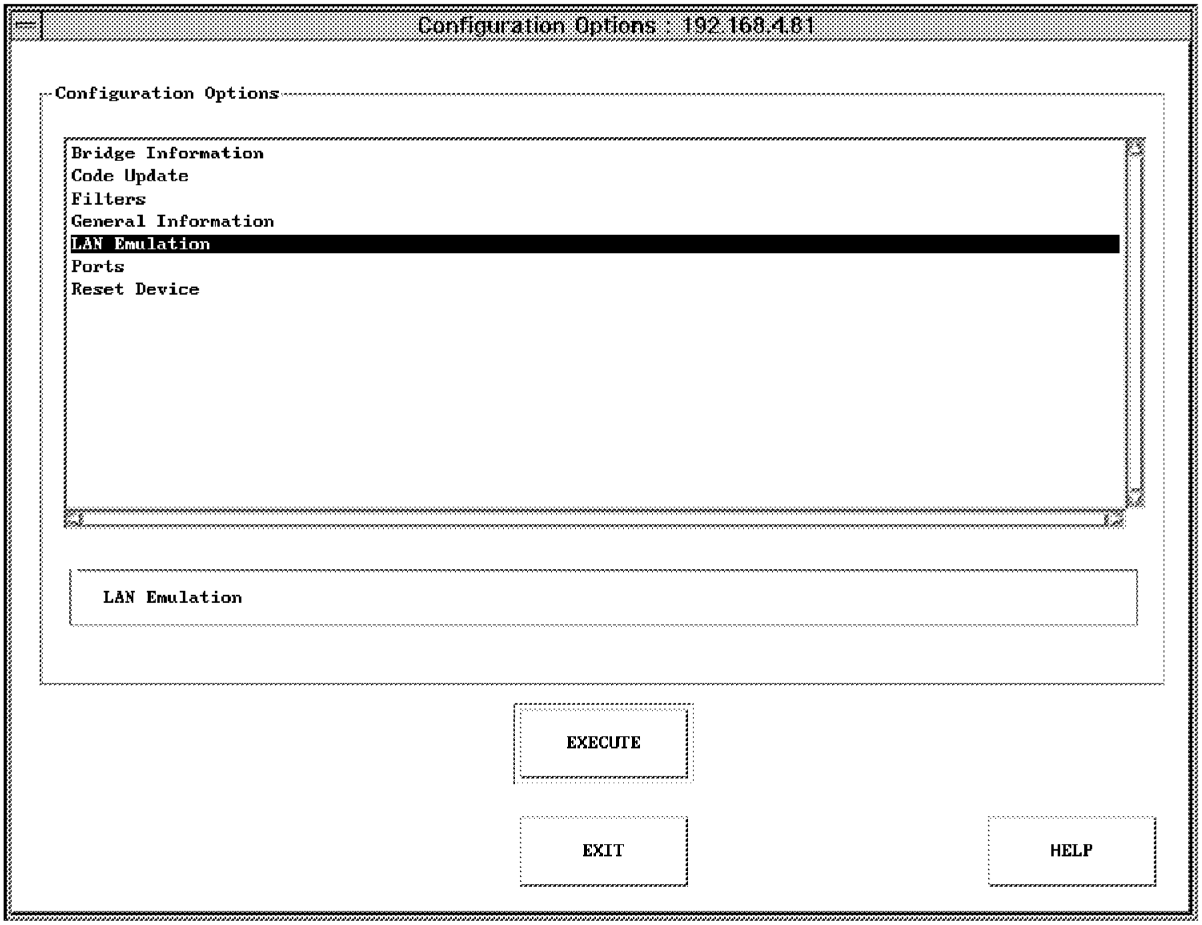

Figure 65. 8281 Bridge Configuration

The bridge was defined with the parameters shown in Figure 66 on page 110.

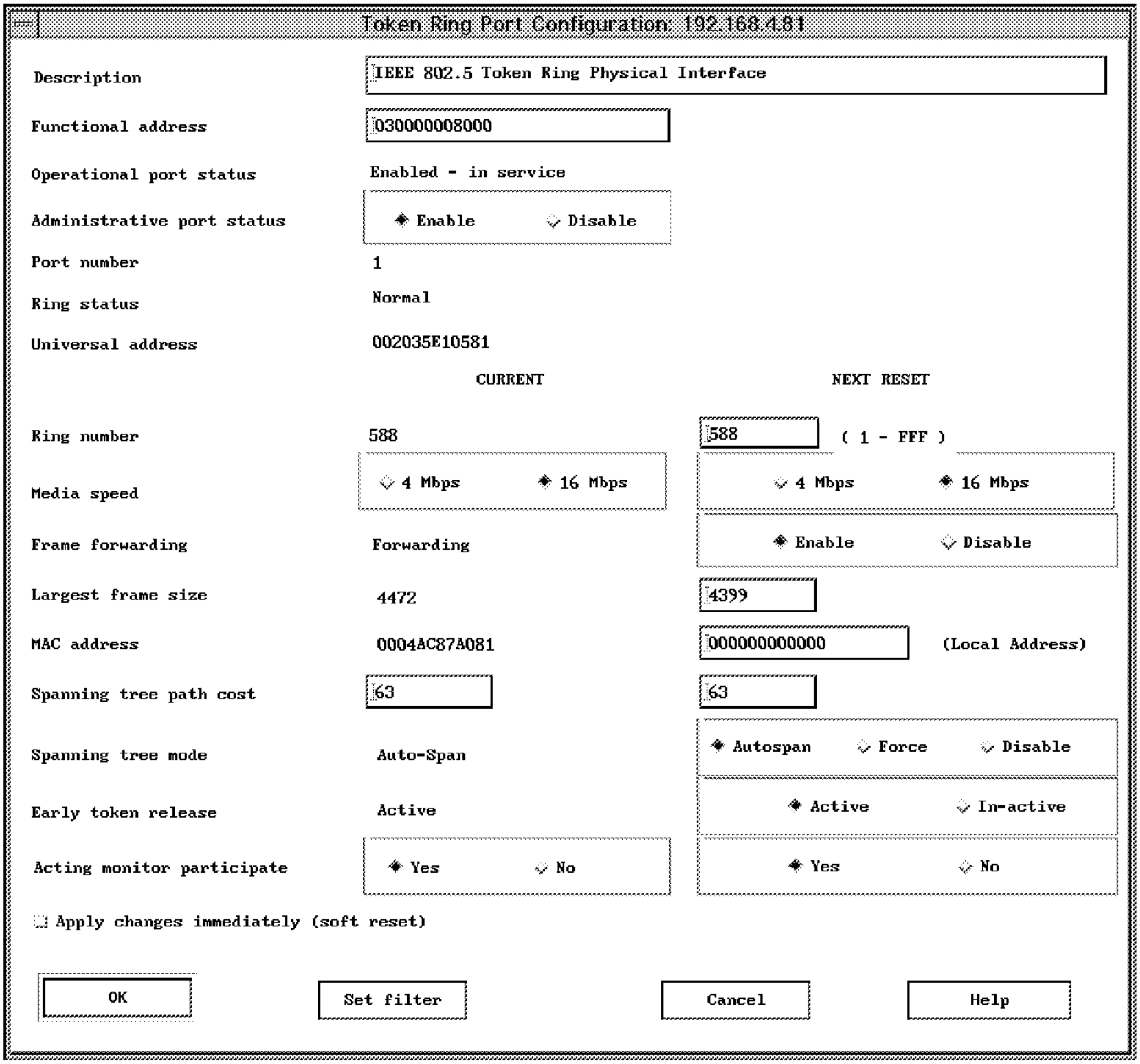

Figure 66. 8281 Bridge Settings

By selecting **LAN Emulation** and clicking on **Execute**, Figure 67 on page 111 is displayed.

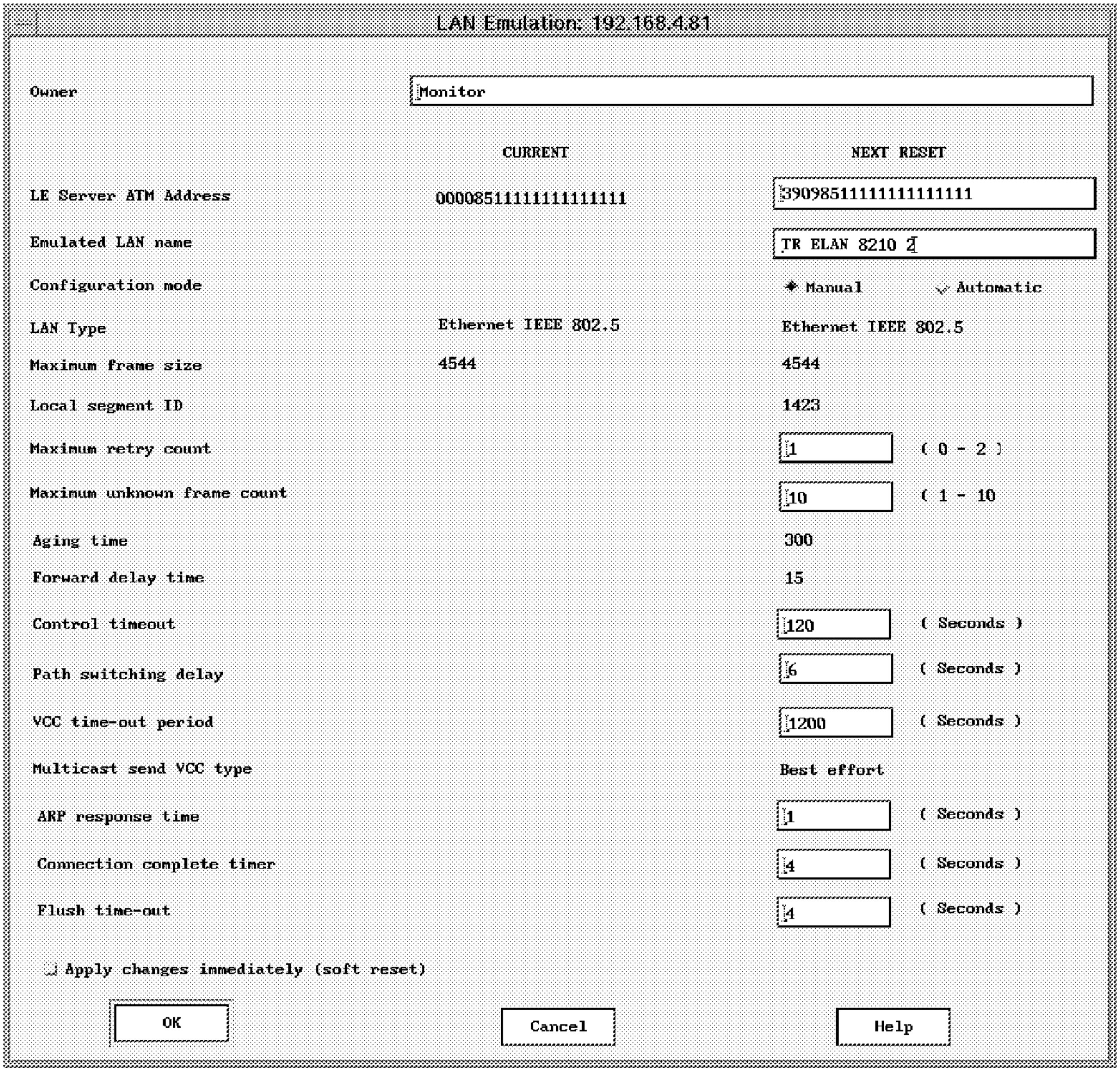

Figure 67. 8281 Bridge Configuration LAN Emulation Settings

The bridge is configured with a locally administered address of 40:00:82:81:BB:BB.

We then entered the LES ATM address of our TR_ELAN_8210_2:

39:09:85:11:11:11:11:11:11:11:11:01:01:40:00:40:00:82:10:00:00:A2.

The ELAN name of our ELAN to the 8281 bridge LEC was set to TR_ELAN_8210_2. The bridge was assigned the IP address of 192.168.4.81 and a host name of 8281b.

4.3.10 Configuring The OS/2 Workstation LEC

Using LAPS we set up the LAN Emulation adapter on the OS/2 ELAN token-ring station. This station was configured with a TURBOWAYS 25 OS/2 LAN Emulation for ISA adapter.

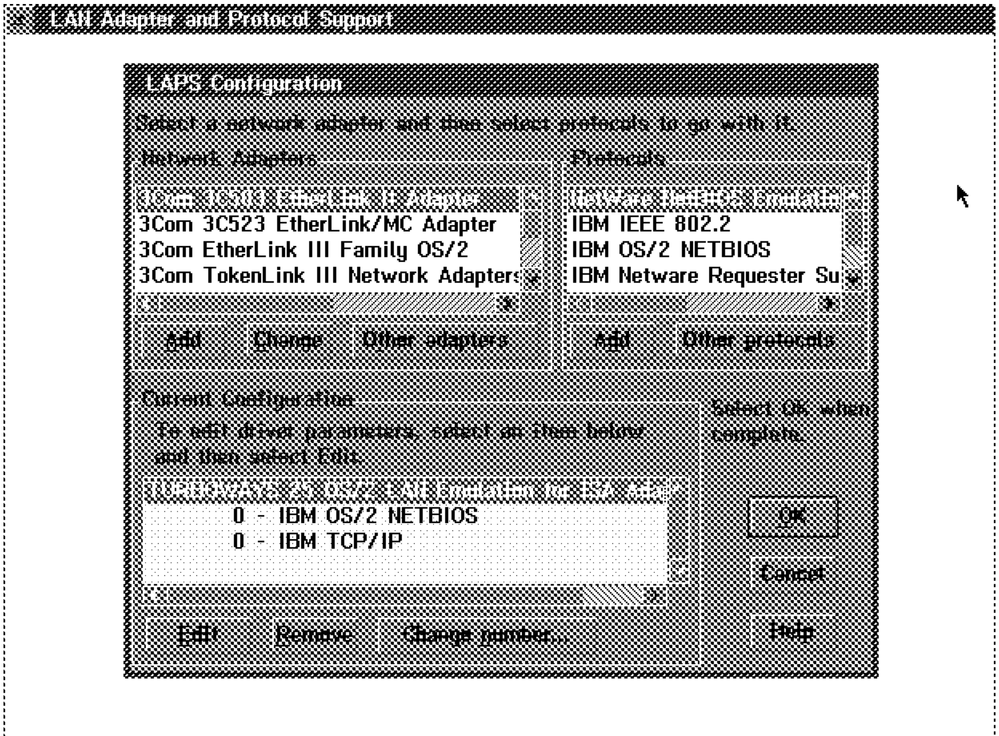

Figure 68. Configuring the ELAN Station

We set the locally administered ESI for the ATM adapter address to to 4000dddd0000 and the ELAN name of TR_ELAN_8210_2.

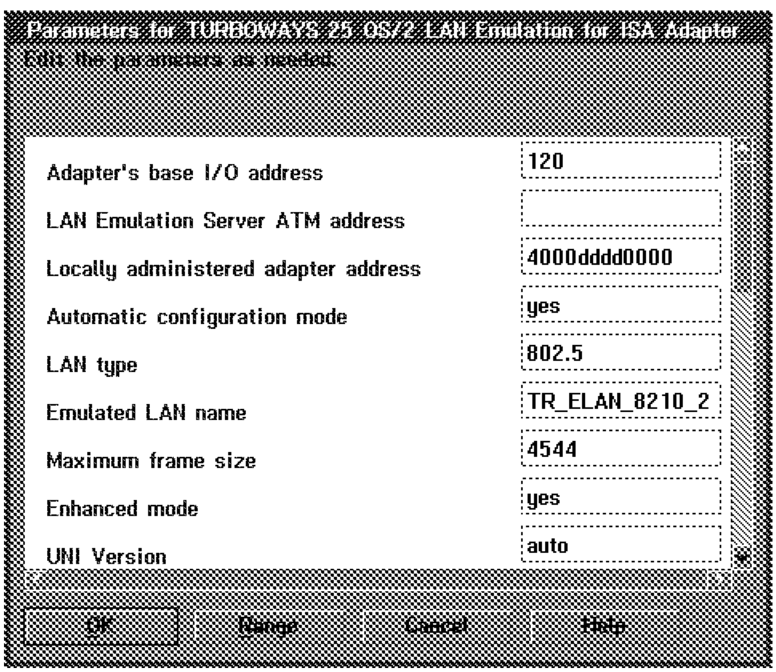

Figure 69. Workstation ELAN Definition

The devices were re-booted.

4.3.11 The ELAN Submap for 192.168.4

We refreshed the ELAN submap for the TR_ELAN_8210_2 and now the LECs for the three devices appeared:

1. 8281 LEC icon (8281b)
2. IBM 8210 server LEC (192.168.20.10-2)
3. ELAN station LEC (4000DDDD000081)

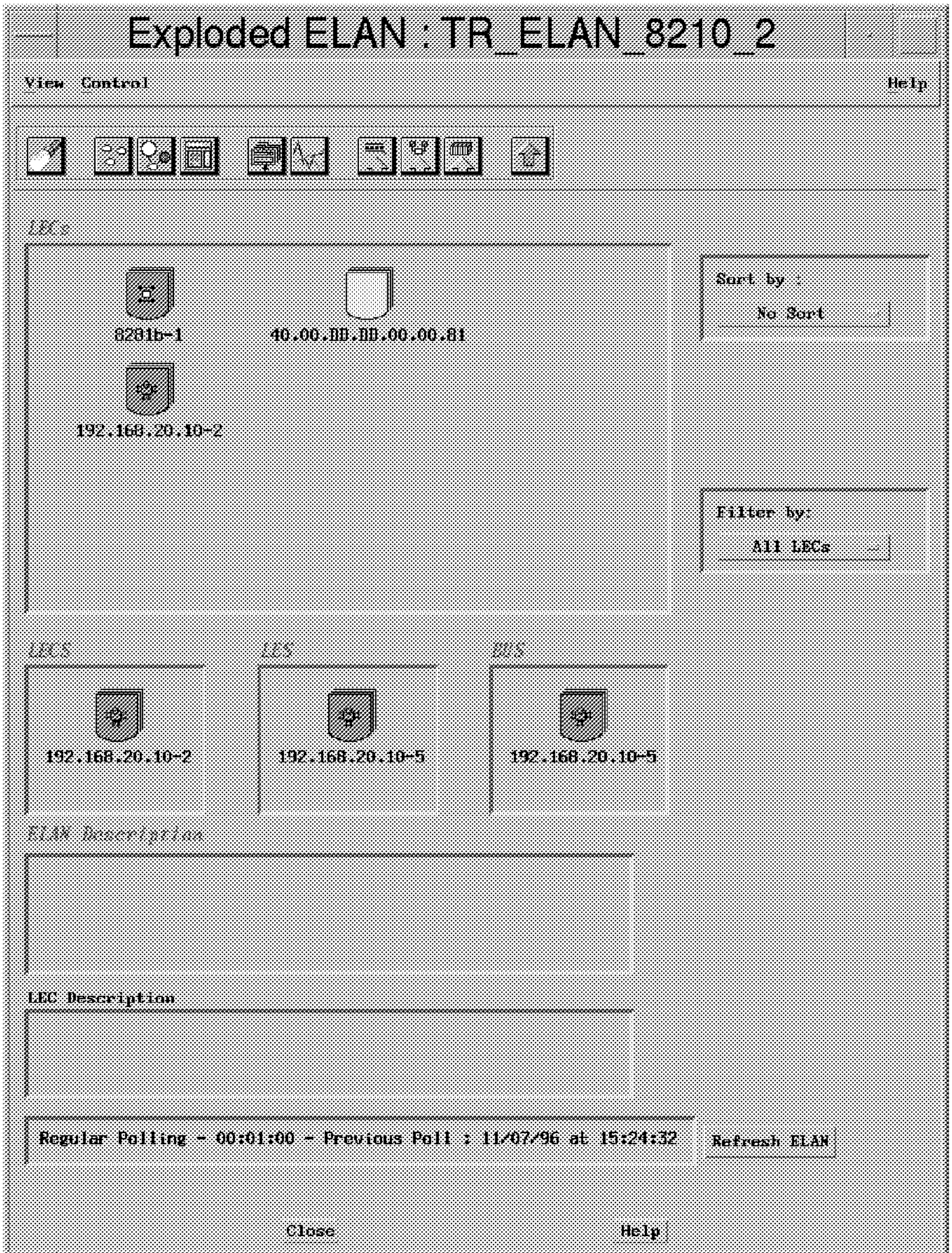

Figure 70. TR_ELAN_8210_2 ELAN Window

Figure 70 depicts the LECs attached to our ELAN and also shows the associated LECS and LES/BUS entities.

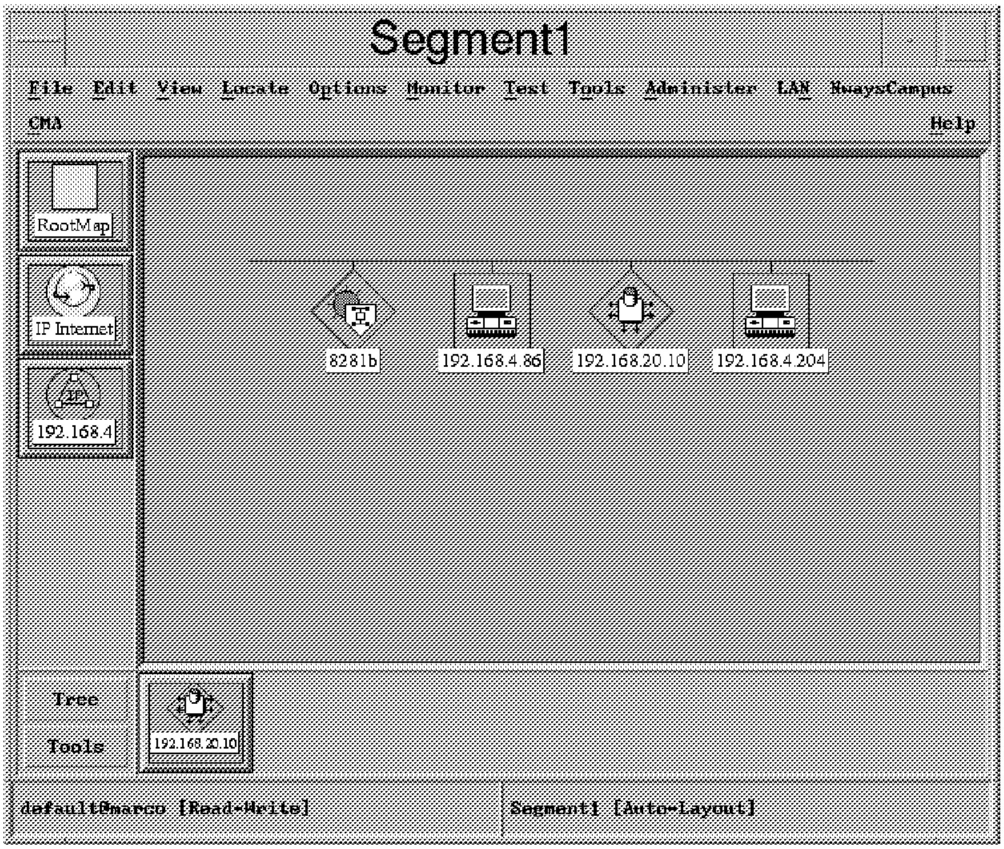

Figure 71. The 192.168.4 IP Subnet

The IP representation of this ELAN is shown in Figure 71.

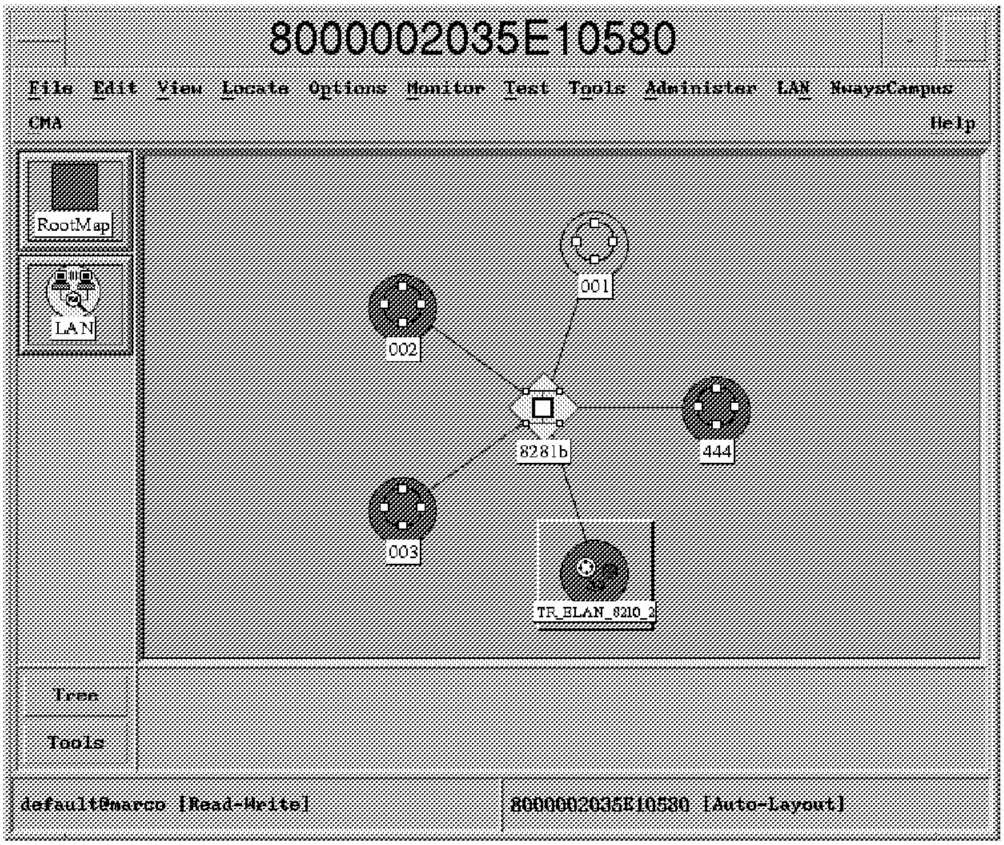

Figure 72. The LNM View

The LNM segment view shows the IBM 8281 ATM bridge 8281b (192.168.4.81), the TR_ELAN_8210_2 Emulated LAN and the token-ring legacy LAN.

Chapter 5. LAN Emulation Redundancy

This example deals with LAN Emulation redundancy and shows how to define the redundancy using the Nways Campus Manager ATM. The redundancy is achieved by duplicating the LAN Emulation service entities (LECS, LES, BUS). On one IBM 8210 MSS Server one LECS, LES and BUS instance is defined. A second 8210 MSS Server also has one LECS, LES and BUS defined, but the LES and BUS instance are configured as *backup* entities.

If the first MSS server becomes in-operable, all of its LAN Emulation components become unavailable and LAN Emulation clients no longer join their respective ELAN.

To continue to service the LECs we will define the redundancy capability on both IBM 8210 devices. When redundancy is enabled a data direct VCC is established from the first LES instance (primary) to the second LES instance (backup). Whenever the first MSS device fails, the data direct VCC is deleted, and the backup LES instance in the second MSS device knows that its primary connection is no longer available.

The second LES instance will service LE_JOIN_REQUESTs sent by LAN Emulation clients. But before sending their LE_JOIN_REQUESTs to the LES the LAN Emulation clients must know the backup LES ATM address. Our LAN Emulation clients are configured to use an LECS service to get this LES ATM address (automatically). These LAN Emulation clients use ILMI to get the LECS ATM address.

To perform this we have to enter in the IBM 8260 CP-Switch all the LECS instances ATM addresses so whenever the first LECS becomes unavailable a LAN Emulation station will try to connect to the second one. Having connected to the new LECS (on the second MSS device), our stations get the new LES ATM address and join it. The sequence of operations is the following one:

```
Entry set.
8260ATM1>
8260ATM1> show lan_emul configuration_server
Index            ATM address
-----------------------------------------------------------------------
  1           39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.00.00.
  2           39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.22.22.
8260ATM1>
```

Note: When entering the LECS ATM address with this command you are prompted to set this LECS ATM address as either active_wka or inactive_wka.

1. Checking that LAN Emulation clients join this ELAN and can exchange data through established data direct VCCs.
2. Defining a domain and an ELAN in the second IBM 8210 MSS Server.
3. Setting redundancy for the primary LES in the first IBM 8210 MSS Server.
4. Setting redundancy for the backup LES in the second IBM 8210 MSS Server.
5. Disconnecting the first IBM 8210 MSS Server from the ATM network (from the IBM 8260 CP-Switch).

6. Reconnecting the first IBM 8210 MSS Server to the ATM network.

The policy definition is for the TR_ELAN_8210_2 is By ELAN Name.

5.1.1 Checking LAN Emulation Clients Have Joined This ELAN

From Figure 73 double-click on the ELAN symbol to reveal the attached LECS.

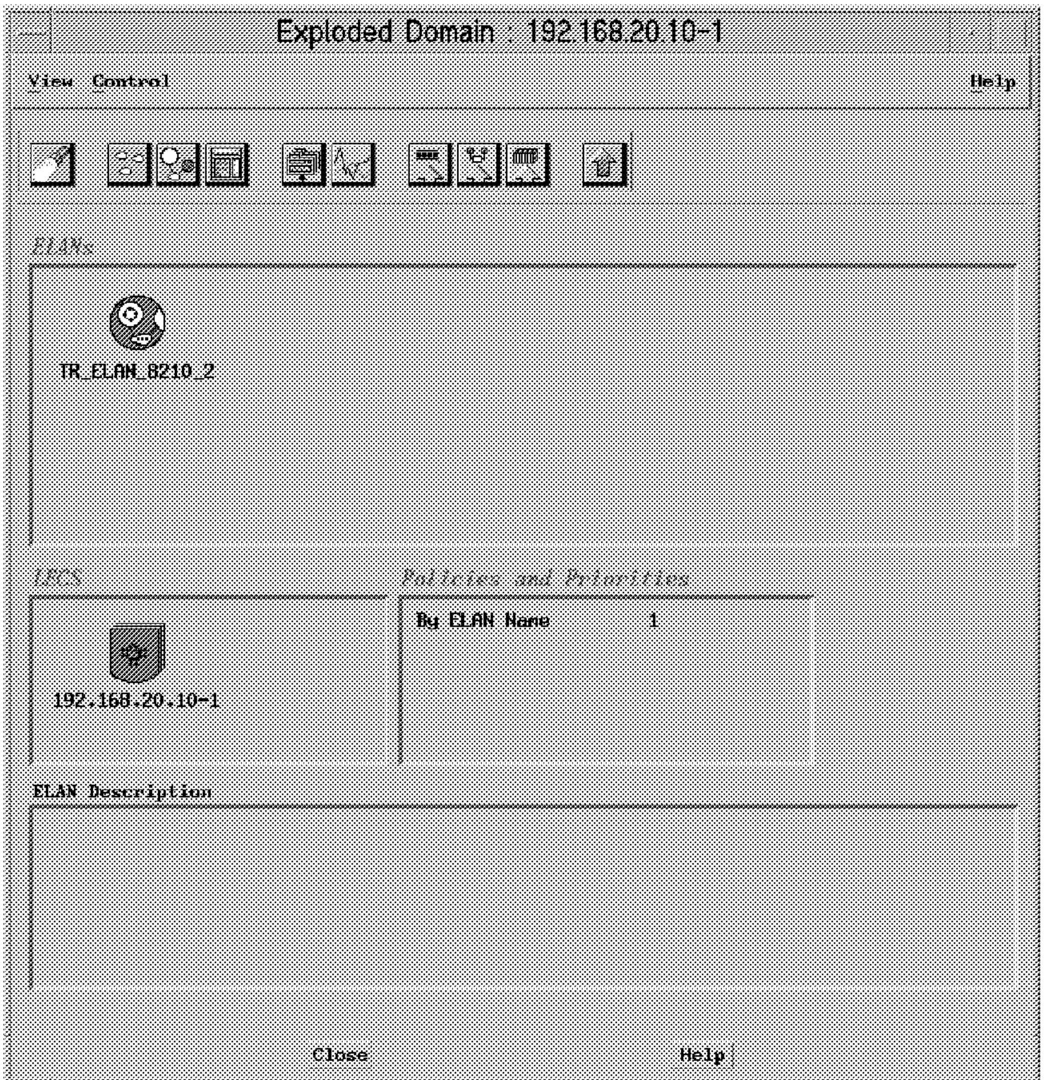

Figure 73. The Exploded Domain: 192.168.20.10-1 Submap

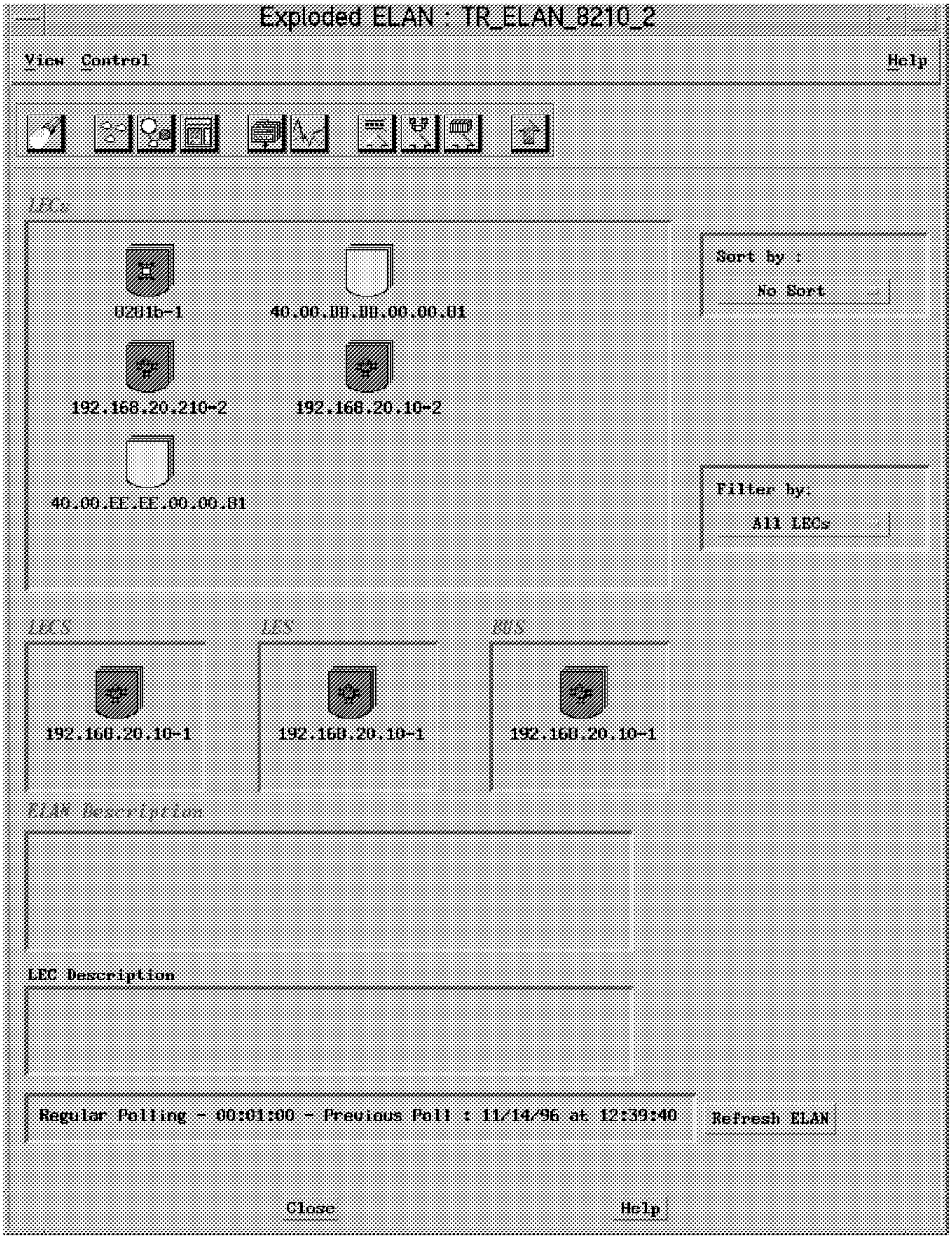

Figure 74. The Exploded ELAN: TR_ELAN_8210_2 Submap

There are five LECs currently attached to our ELAN.

The next step is to define an ELAN in the backup IBM 8210.

5.1.2 Defining a Domain and an ELAN in a Second IBM 8210 MSS Server

We introduced the second MSS server with an IP address of 192.168.20.210 and defined the domain as shown in Figure 75.

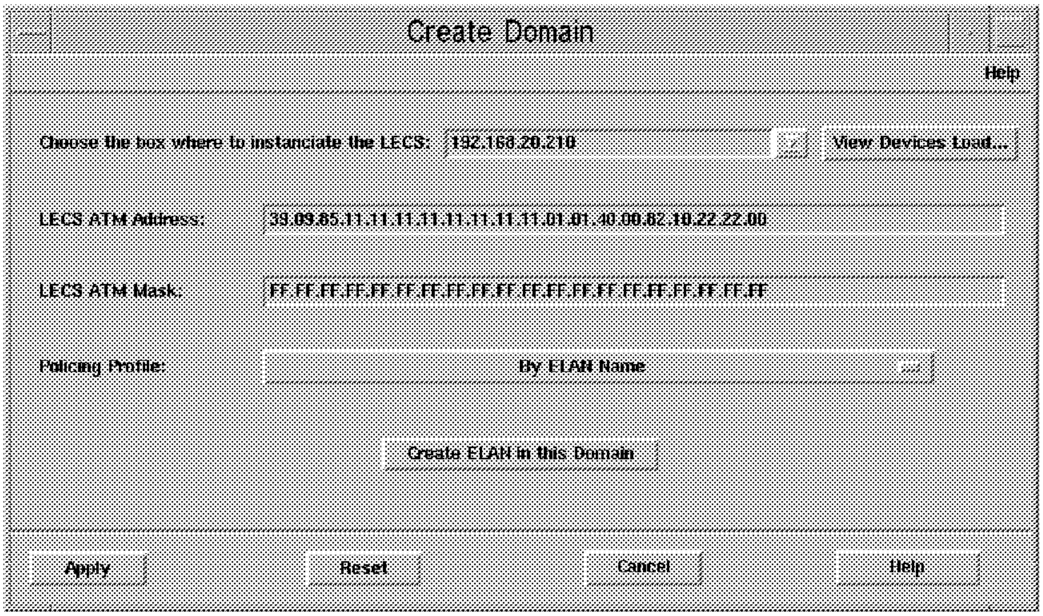

Figure 75. Defining a Domain in the Second MSS

The LECS ATM address is defined with the ESI of 40.00.82.22.22.00 and a selector byte of 00.

Finally we select a policy profile **By ELAN Name** for this domain. Next we clicked on **Create ELAN in this Domain** (see Figure 76 on page 121).

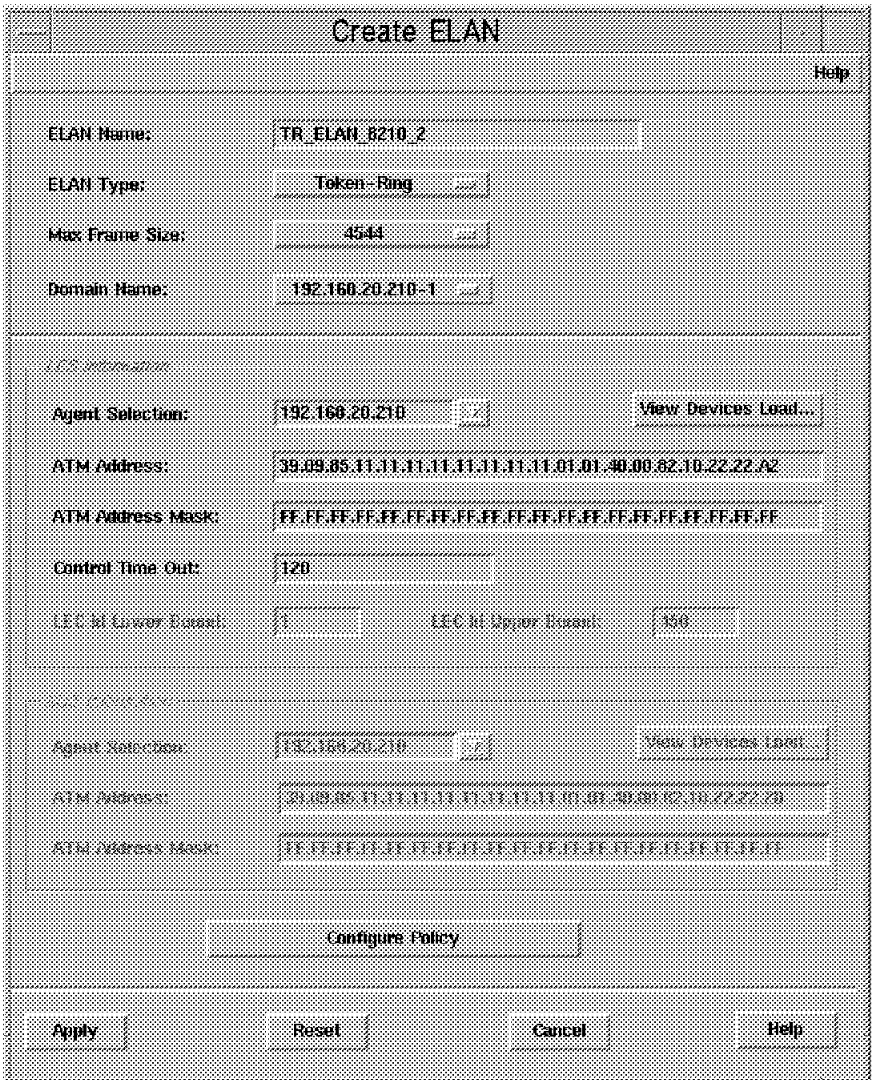

Figure 76. Configuring an ELAN in the Second Domain

The ELAN we defined in the second 8210 is the same as the ELAN defined in the first 8210.

The domain name is defined as 192.168.20.210-1 and the agent identifier (IP address) where we want to instantiate the LES/BUS also (192.168.20.210).

Once again we associate the ELAN name(s) to the administrative ELAN name TR_ELAN_8210_2 and set the same ELAN name for the policy value TR_ELAN_8210_2.

Now we can view the LAN Emulation submap, we can see the newly created domain icons 192.168.20.10-1 and 192.168.20.210-1 (see Figure 77 on page 122).

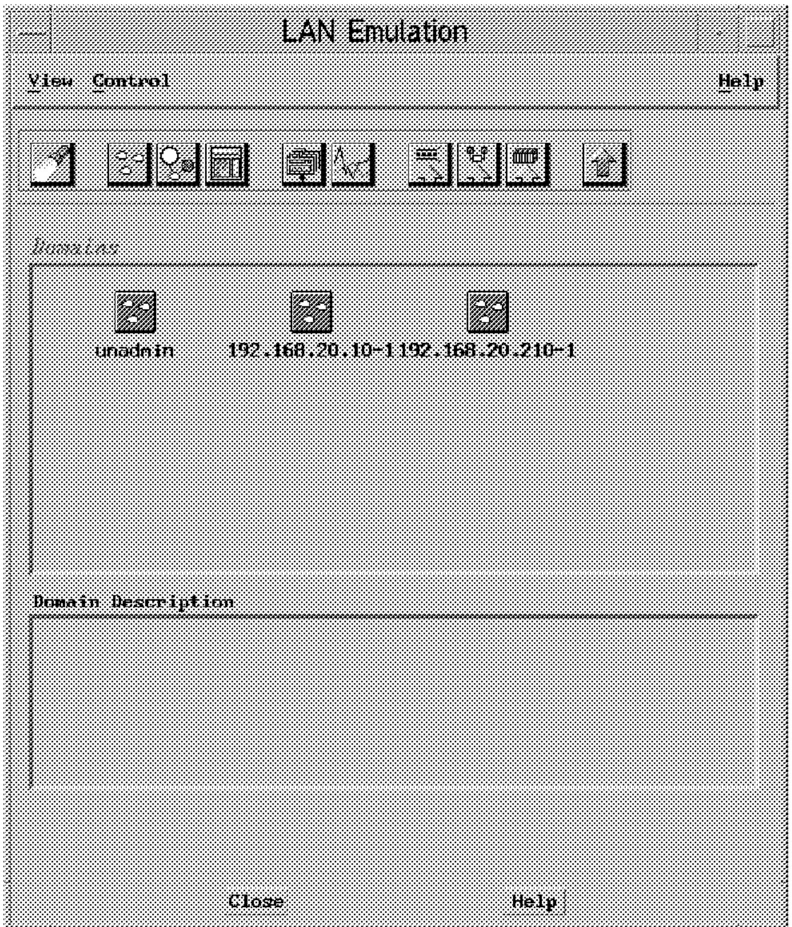

Figure 77. The new LAN Emulation Network Submap

If we double-click on **192.168.20.210-1**, its LAN Emulation administrative domain submap is displayed and one ELAN icon, TR_ELAN_8210_2, shows up (see Figure 78 on page 123).

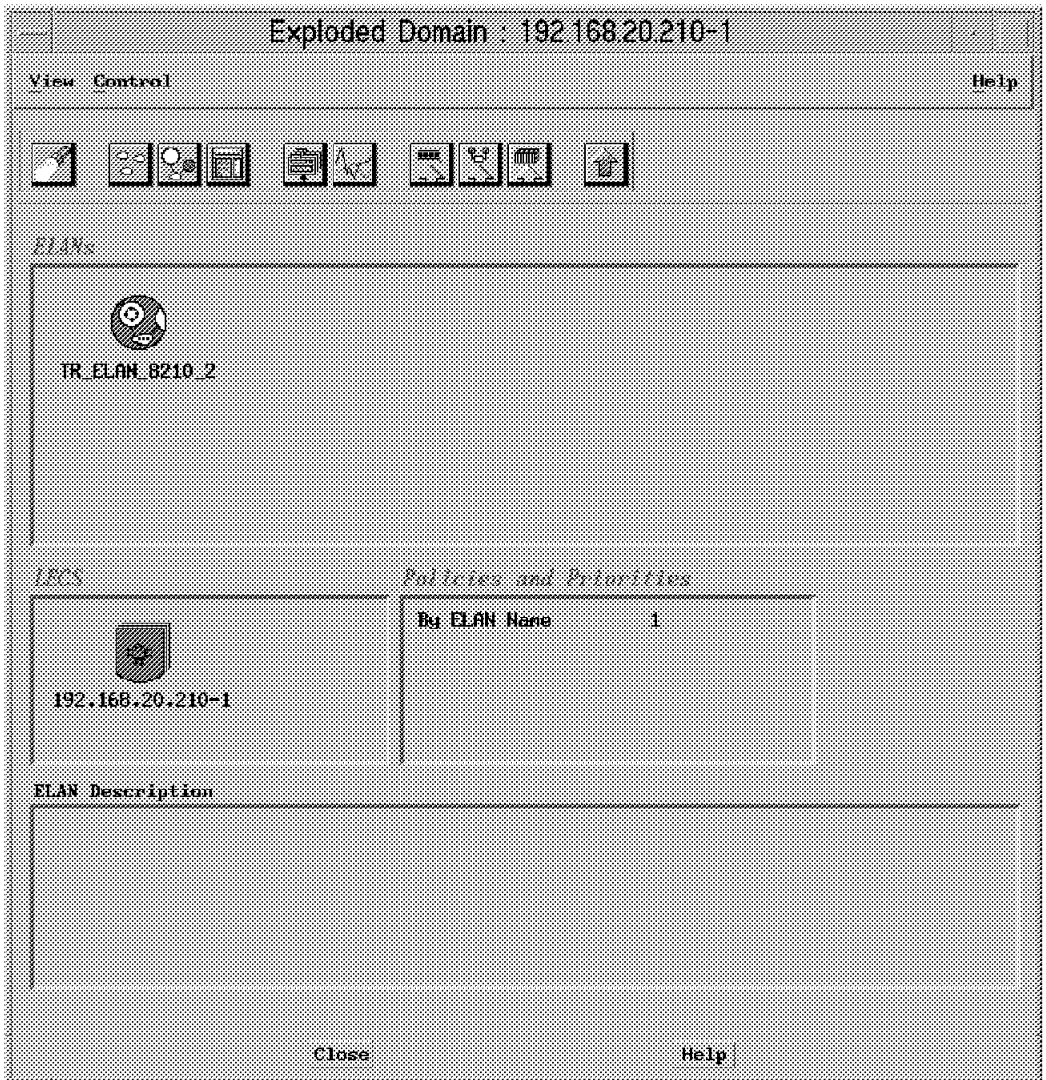

Figure 78. The Second Domain Administrative Submap

At first glance this view seems identical to the first domain′s corresponding view but let′s analyze it more. The title of this exploded view is different (192.168.20.210-1 instead of 192.168.20.10-1) and the identifier of the LECS icon at the left bottom of the view has a different identifier (192.168.20.210-1 instead of 192.168.20.10-1). If we double-click on this ELAN icon, we find no LECs at all (see Figure 79 on page 124).

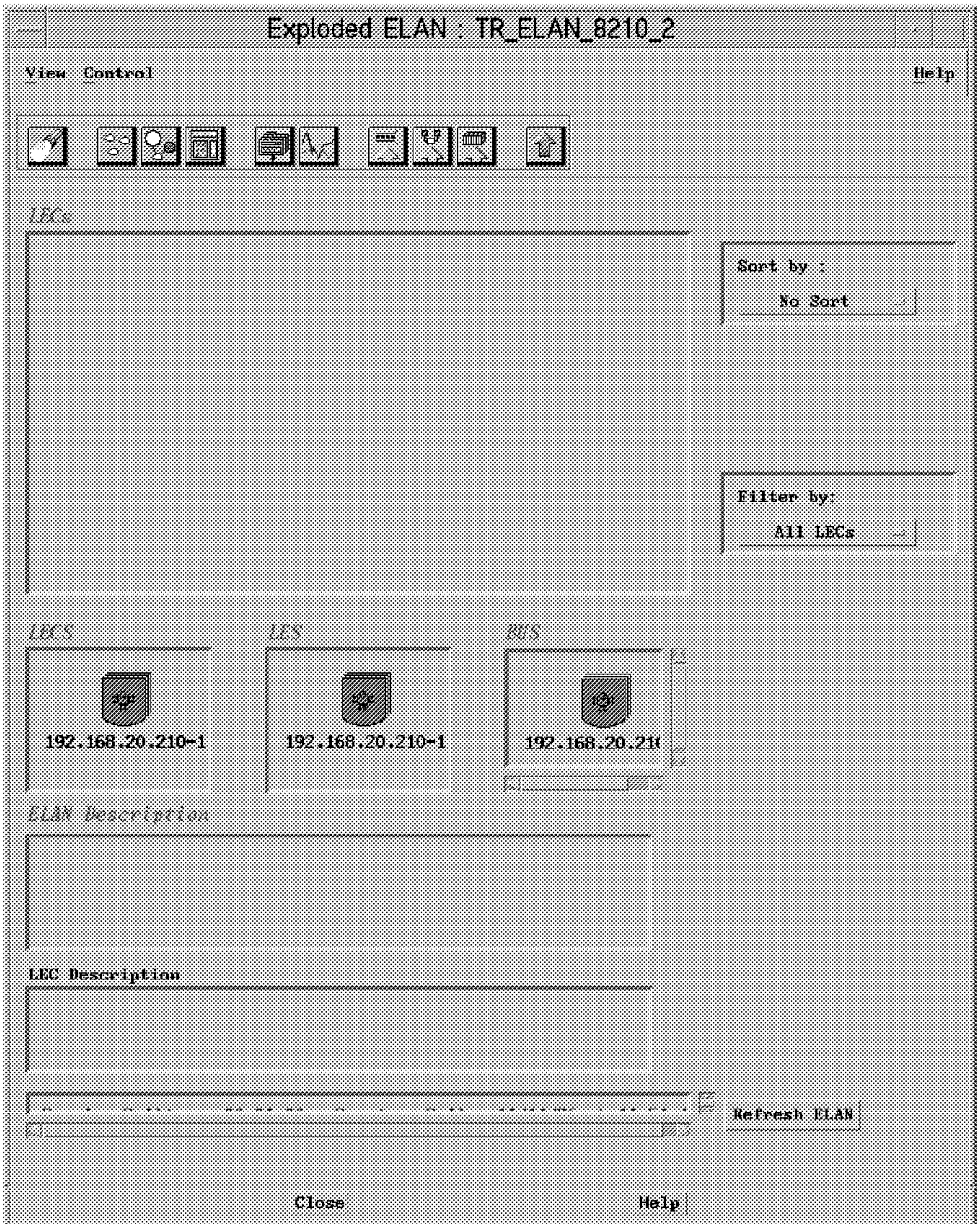

Figure 79. The Second Domain ELAN Submap

This domain's assigned LECS address (39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.22.22.00) is only the second entered in the IBM 8260 ATM switch and as the first LECS (39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.00.00.00) is still OK, all the automatic LECs have connected to it and received from it the ATM address of the LES instance located in the first MSS (39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.00.00.A2).

5.1.3 Setting Redundancy for the Primary LES in the First IBM 8210 MSS

In summary, for the current two domains defined on two MSS devices and for each domain, an ELAN has been administratively defined with exactly the same parameters. The first ELAN LAN Emulation service entities (LES/BUS) are instantiated on the first MSS device, and the second ELAN LAN Emulation service entities are instantiated in the second MSS device. For each ELAN, the LECS instance, the administrative definitions and the LES/BUS instances are collocated in the same IBM 8210 device.

If the first LECS becomes unavailable, then new LECs will connect to the second LECS (on the second MSS box) because of the contents of the 8260 ATM switch ILMI table.

If the first LECS becomes operational again, the new LECs will connect to the first LECS. This is why redundancy must be enabled.

The redundancy is enabled from the configuration screen shown in Figure 80 on page 126.

Figure 80. The 192.168.20.10 MSS Device Configuration Panel

We can see the list of LES and BUS definition for this MSS device. Select the LES entry and click on **Configuration**. The LES Configuration panel is shown (see Figure 81 on page 127).

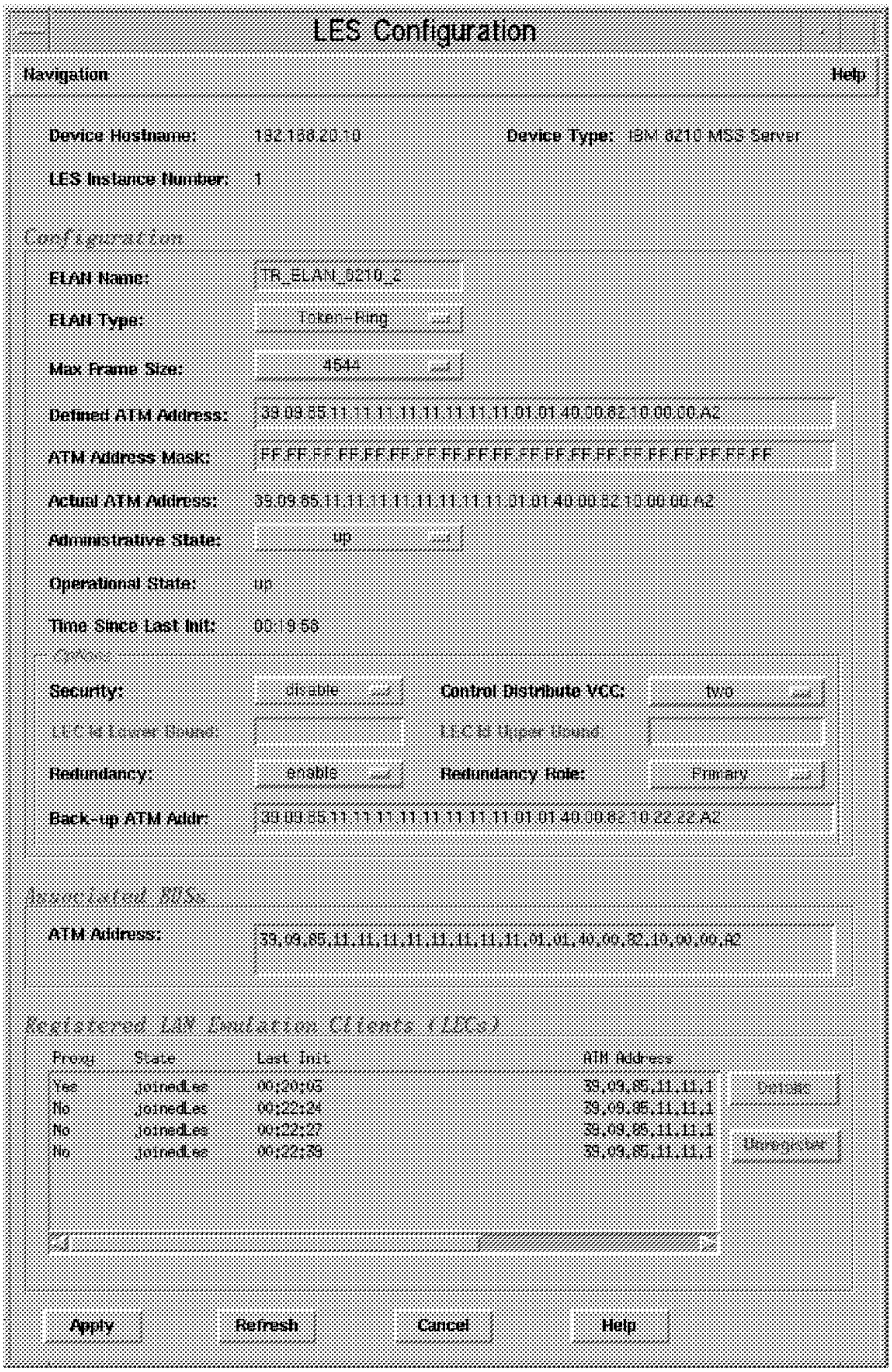

Figure 81. The First MSS LES Configuration Panel

Enable redundancy and define this LES instance behavior as *primary*. Add the address 39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.22.22.A2 for the Back-Up ATM Address field.

This backup LES is located in the second MSS box (192.168.20.210). Now we select **Apply** and redundancy is set for this LES instance as primary. Let's set it on the backup LES also.

5.1.4 Setting Redundancy for the Backup LES in the Second IBM 8210 MSS

From the configuration screen for the second 8210, the LES details are shown in Figure 82.

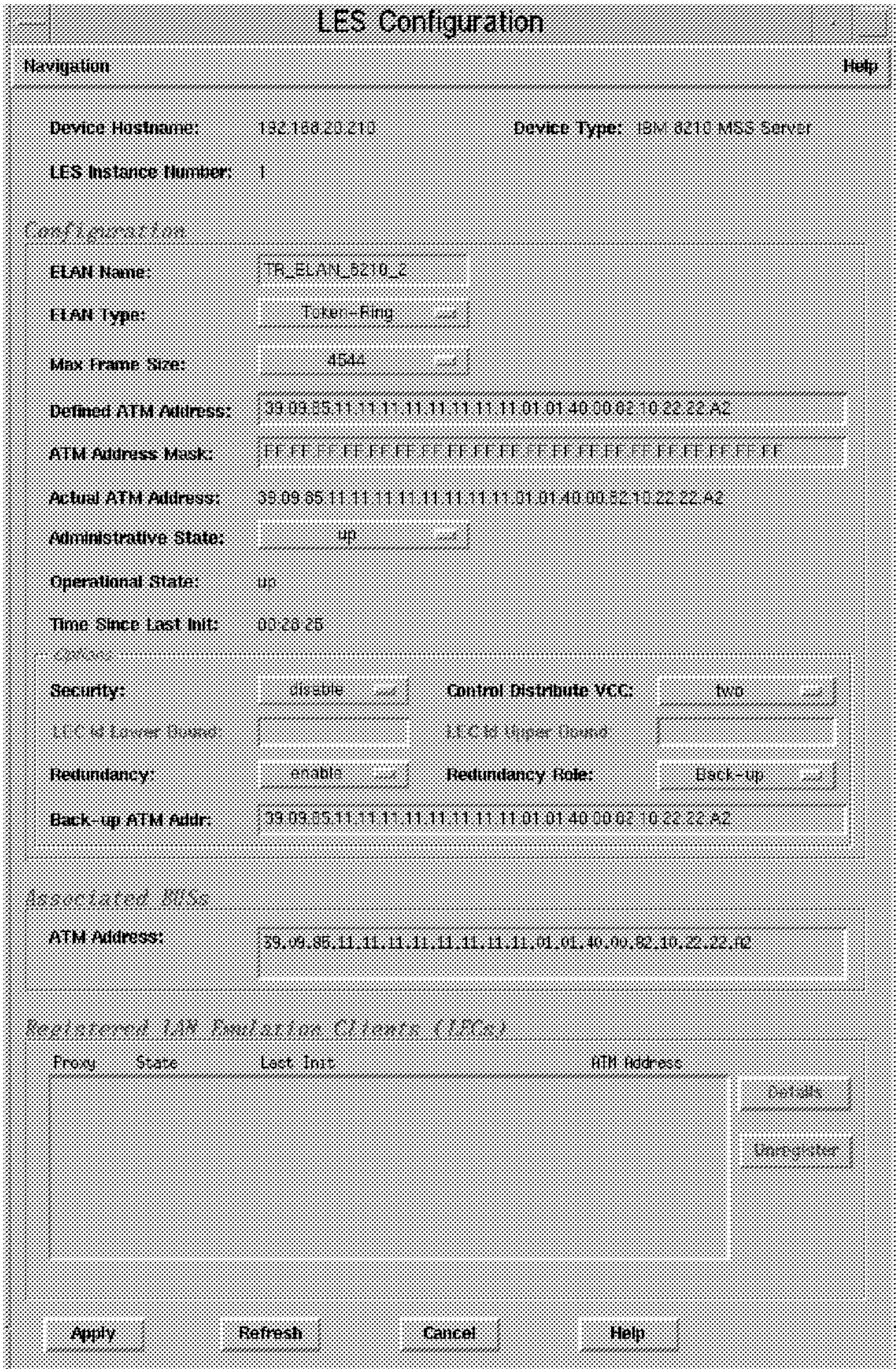

Figure 82. The Second MSS LES Configuration Panel

The Redundancy field was enabled and the role set to backup. As far as the Backup ATM Address field is concerned it seems that we don't have to enter this backup ATM address as it's this current LES ATM address; however we did enter:

39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.22.22.A2.

We finally selected **Apply**.

Now the TR_ELAN_8210_2 ELAN icon for the second MSS administrative topology submap shows the LES and BUS icons with a small white triangle indicating these LES/BUS instances are backup ones (see Figure 83).

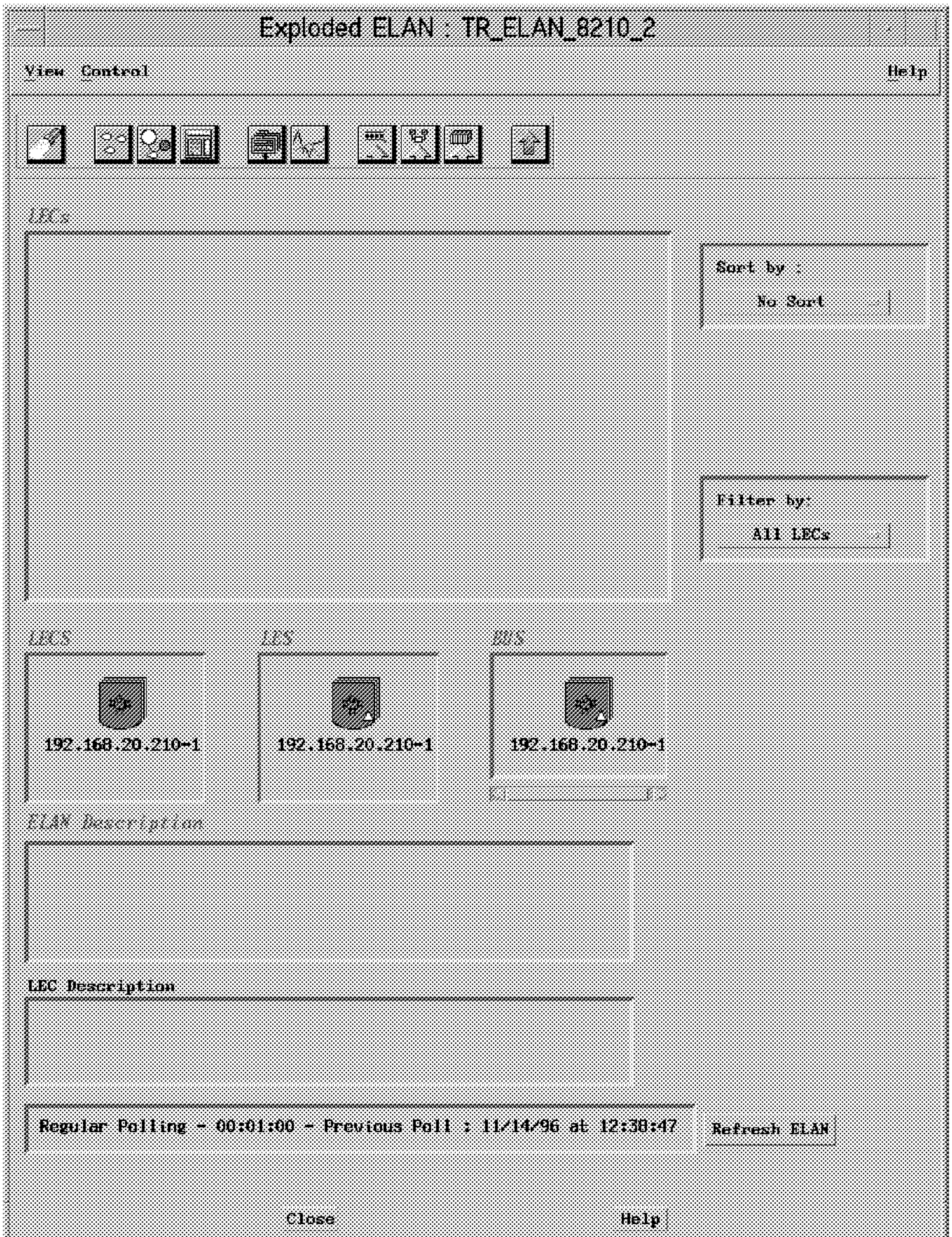

Figure 83. ELAN Topology Submap in Second MSS after Redundancy Setup

Redundancy is now enabled.

5.1.5 Disconnecting the First IBM 8210 MSS Server from the ATM Network

Now we can remove the cable connected to the first MSS device from its 8260 ATM switch port to simulate this device going down. We also re-booted the LAN emulation clients.

After a short time we re-opened the ELAN submap for the first 8210 (see Figure 84).

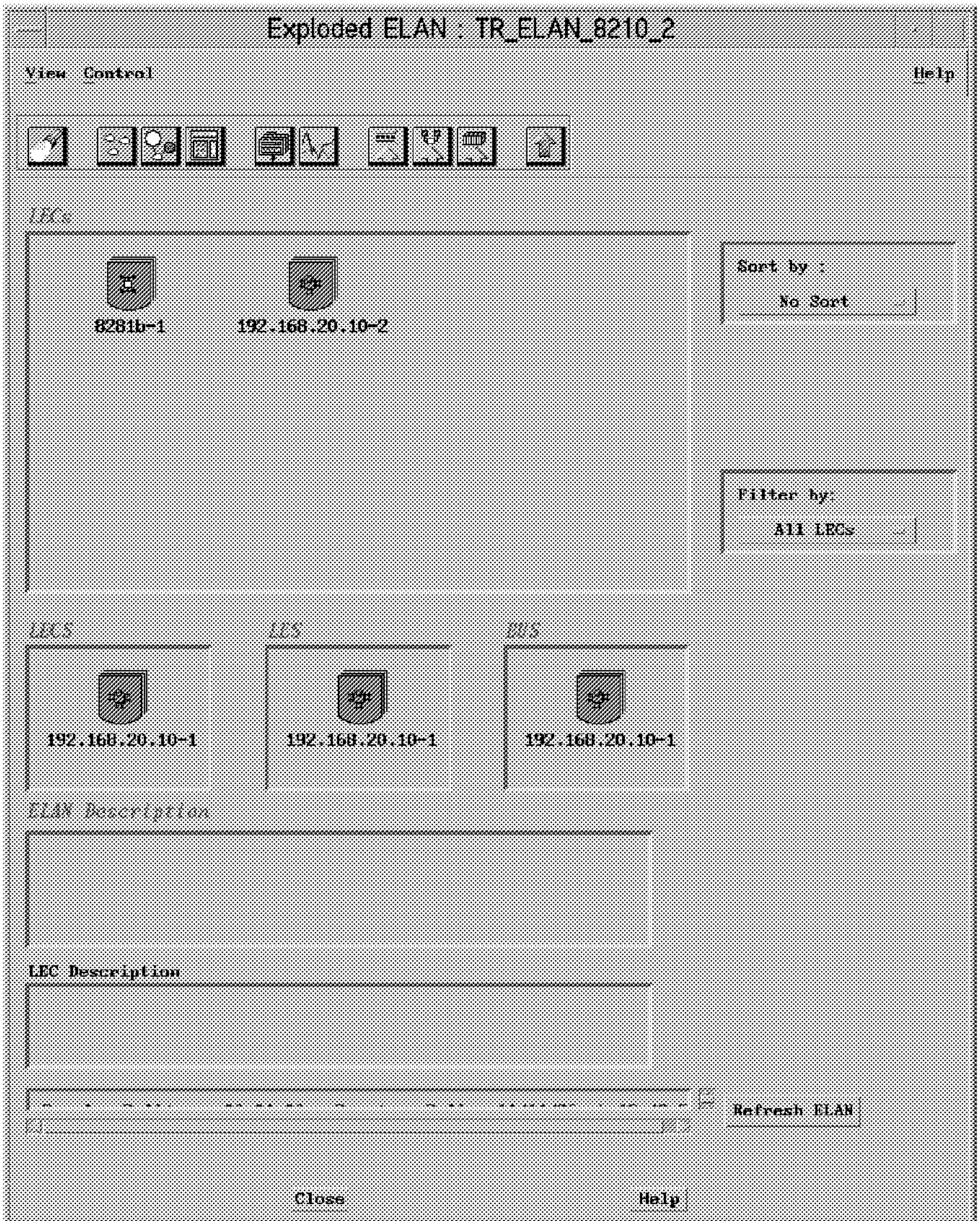

Figure 84. ELAN Topology Submap in First MSS after Cable Is Removed

The LECS, LES, and BUS icons turned red implying a status of down.

The two workstation LECs have disappeared from this view, along with the local LEC icon (192.168.20.210-2).

This is because the LECs have joined the backup LES.

The 8281b-1 icon represents our 8281 ATM bridge that is configured in manual mode. (It was configured with the primary LES ATM address.) As soon as we removed the first MSS cable, its configured LES can no longer be reached; this 8281 ATM bridge had no method to automatically locate its new LES ATM address (backup).

The 192.168.20.10-2 icon represents the first MSS internal LEC; as this LEC cannot get the new LES ATM address anymore it cannot join the new LES and consequently disappears from any LES LECs table.

The second 8210 domain screen (Figure 85 on page 132) shows the active clients.

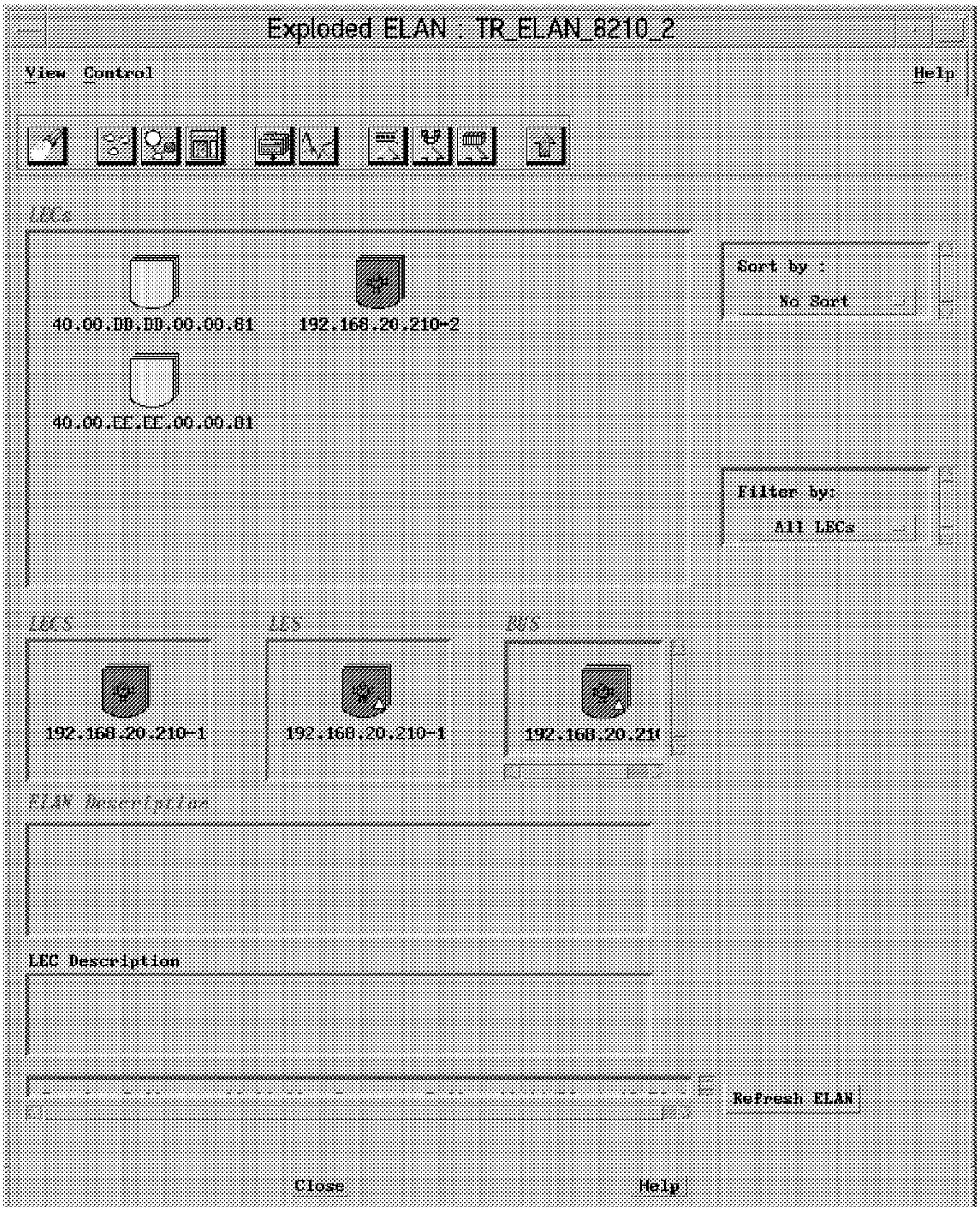

Figure 85. ELAN Topology Submap in Second MSS after Cable Is Removed

The have joined the new LES backup by seeing their VCCs to the primary LES/BUS go down and attempting to retrieve their LES address from the first LECS. When this LECS cannot be reached the ILMI is used.

The connection to the second LECS succeeds. The three LECs joined the ELAN successfully.

We verified this by pinging from the first station to (40.00.DD.DD.00.00.81) the second station (40.00.EE.EE.00.00.81). It works. (These two stations have IP addresses 192.168.4.86 and 192.168.4.87.)

5.1.6 Summary

When redundancy was enabled, the primary LES established a direct VCC to the backup LES. When the cable was removed, the VCC connection was broken, and at this time the backup LES knew it had to accept LE_JOIN_REQUESTs from LECs as its primary was probably down.

The process was:

- The LECs noticed that their VCCs where disconnected (control direct VCC, control distribute VCC, multicast send VCC, multicast forward VCC).
- Connect to the second LECS collocated with the backup LES. This LECS first analyzed the nature of its collocated LES, and realized it was a backup LES. But the LECS had knowledge that the inter-LES VCC was down and consequently delivered the ATM address of its collocated backup LES. Then the LEC stations re-joined the ELAN.

Next we reconnected the first MSS box to its 8260 ATM switch.

5.1.7 Reconnecting the First IBM 8210 MSS Server to the ATM Network

The first MSS LECS is now active again and the first MSS primary LES will re-establish immediately its VCC connection to the backup LES in the second MSS.

Reboot LEC stations to remove their cache. Now by re-opening the first MSS ELAN submap we can verify all that re-joined the first primary LES.

5.1.8 The Solution

Seeing the inter-LES VCC re-established by the primary LES, the backup LES released all its LAN Emulation service VCCs so the LECs tried to re-connect to the second LECS (still their current one) to get a LES ATM address. This LECS found that its collocated LES was a back-up and that the inter-LES VCC was OK, so it sent back to the LECs the ATM address of the primary LES on the first MSS. Then the LECs could then re-join the primary LES.

Chapter 6. LAN Emulation Security

In this scenario we address security. There is a risk that unauthorized stations may connect to the LES/BUS and attempt to use its services. Since LECs may be configured with LES ATM addresses, the optional configuration protocol is not a reliable ELAN security mechanism. To control ELAN membership, an LES configured in an 8210 can validate LE_JOIN_REQUESTs.

When receiving LE_JOIN_REQUESTs from the LECs, the LES forms an LE_CONFIGURE_REQUEST on behalf of the LEC using information contained in the LE_JOIN_REQUEST. This LE_CONFIGURE_REQUEST includes the Source LAN Destination, Source ATM Address, ELAN Type, Max Frame Size and ELAN Name from the LE_JOIN_REQUEST, along with an IBM Security TLV. The security request is transmitted to the LECS by a multiplexing component called the LECS interface, and the LECS must validate the request using the policy values table.

6.1.1 Defining Security

The sequence of operations will be the following:

1. Define the LECS instance using the command console.
2. Customize the LECS instance.
3. Define the LECS interface (security component).
4. Create an ELAN.
5. Define policy values for automatic LECs only.
6. Configure security.
7. Add policy values for manual LECs.

6.1.2 Defining an LECS Instance

We chose to configure the LECS directly from the 8210 console because the LECS interface security component locates the LECS dynamically using the ILMI and well-known address.

After the VCC to the LECS is established, the LECS interface issues a local query to determine whether the LECS is located on the same MSS server.
If the LECS is collocated, a local interface is used to validate joins without transmitting the requests onto the ATM network.

We used talk 6 to set up the LECS and LECS interface configuration as follows:


```
*
*t 6
Config>net 0
ATM user configuration
ATM Config>le-services
LAN Emulation Services user configuration
LE Services config>lecs
LAN Emulation Configuration Server configuration
LECS config>
LECS config>add
  (  1) Use burned in ESI
  (  2) 40.00.82.10.00.00
  (  3) 50.00.82.10.00.00
End system identifier [1]? 2
LECS added to configuration
Enable standard Error Logging System for LECS? [Yes]:
Standard ELS activated for LECS
```

```
LECS config>policies
LECS POLICIES configuration
LECS POLICIES config>?
LECS POLICIES config>add
Priority of Policy [10]?
Policy type
        (1) byAtmAddr
        (2) byMacAddr
        (3) byRteDesc
        (4) byLANType
        (5) byPktSize
        (6) byElanNm

Enter Selection:  [1]?
Added policy 'byAtmAddr' at priority 10
Selection "Add assignment policy" Complete
LECS POLICIES config>list

Policy Listing...

Enabled  Priority  Type
=======  ========  ==========
    Yes        10  byAtmAddr
LECS POLICIES config>exit
```

```
LECS config>list
LECS Detailed Configuration
   Lecs is                                      Enabled
   ATM Device number:                           0
   ESI:                                         40.00.82.10.00.00
   Selector:                                    0x00
   Validate Best Effort PCR:                    No
   Configuration Direct Max Reserved BW (Kbps): 0
   Maximum number of simultaneous VCCs:         128
   Idle VCC Timeout (in seconds):               60
   Trace ATM address value: 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.0
0.00.00
   Trace ATM address mask:  FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.F
F.FF.FF
```

6.1.3 Customizing This LECS Instance

The LECS instance has a default Validate Best Effort PCR set to no. We modified this as follows:

```
LECS config>set validate yes
LECS validates PCR of best effort connections
Selection "Validate best effort VCC's PCR modification" Complete
LECS config>set reserved 155
Maximum reserved bandwidth of config direct VCC is 155 Kbps
Selection "Maximum reserved bandwidth for VCCs modification" Complete
LECS config>list
LECS Detailed Configuration
   Lecs is                                       Enabled
   ATM Device number:                            0
   ESI:                                          40.00.82.10.00.00
   Selector:                                     0x00
   Validate Best Effort PCR:                     Yes
   Configuration Direct Max Reserved BW (Kbps): 155
   Maximum number of simultaneous VCCs:          128
   Idle VCC Timeout (in seconds):                60
   Trace ATM address value: 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.0
0.00.00
   Trace ATM address mask:  FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.F
F.FF.FF
```

The LECS instance is ready to receive VCC from the LECS interface. We are now going to set up this LECS interface.

6.1.4 Defining the LECS Interface (Security Component)

This LECS interface cannot be defined from the Nways Campus Manager ATM or all the LECs having already joined the ELAN will loose access to the ELAN and no new LEC will be able to join.

Note: Setting the security means two things:

1. First defining the LECS interface
2. Enabling it for a given ELAN

We used talk 6 to enable the LECS security.

```
LECS config>exit
LE Services config>security
LECS Interface configuration
LECS INTERFACE config>add
  (  1) Use burned in ESI
  (  2) 40.00.82.10.00.00
  (  3) 50.00.82.10.00.00
Select ESI [1]? 2
Selector x00 is generally reserved for use by the LECS,
Selector x01 is generally reserved for use by the LECS Interface.
LECS Interface Selector (in hex) [1]?
LECS INTERFACE config>list
LECS Interface Detailed Configuration
   LECS Interface Enabled/Disabled: Enabled
   ATM Device number: 0
   ESI: 40.00.82.10.00.00
   Selector: 0x01
   Configuration Direct VCC Traffic Type: Best Effort VCC
   Configuration Direct VCC PCR in Kbps: 155000
   Configuration Direct VCC SCR in Kbps: 0
LECS INTERFACE config>
```

Note: In the new LECS interface list, the LECS interface is default Enabled. This means that after saving this new configuration and reloading it, the LECS interface will be active. This doesn't mean that the security is enabled for a given ELAN; this is performed manually.

Let's save this new configuration and reload it.

```
LECS INTERFACE config>exit
LE Services config>exit
ATM Config>exit
Config>write
Config Save: Using bank B and config number 3
Config>
*
reload
Are you sure you want to reload the gateway?
(Yes or [No]):y
```

After reloading the new configuration becomes active. To verify we checked the MSS configuration using talk 6.

```
t 5
+net
Network number [0]?
ATM Console
ATM+le-services
LE-Services Console
LE-SERVICES+security
LES-LECS Security Interface
LES-LECS interface+
LES-LECS interface+list
Status of LES-LECS Security Interface
  ATM Device Number:     0
  State:                 Operating normally(110)
    Time of last state change:      00.00.03.73
    Elapsed time since last change: 00.58.11.04
  Error Log:             no err(0)
  ATM address:           39098511111111111111111010140008210000001
  UNI version            UNI Version 3.1
  Most recent LECS ILMI list: 1 entries
    (0) 39098511111111111111111010140008210000000(current)
  Connected LECS:        39098511111111111111111010140008210000000(local)
  VCC characteristics:
    Configuration direct VCC type:      Best Effort
    Configuration direct VCC PCR:       155000
```

Note: Here the security interface (LECS interface) has established its VCC to the LECS (State: Operating normally (110) but it may happen that the VCC couldn′t be created. In this case an error message is displayed. Restart the LECS interface through the restart command. Whenever the VCC is down we′ve experienced that the LECS itself is invisible in both t 5 and SNMP.

6.1.5 Creating an ELAN

Once the MSS console definition is completed and operational we created an ELAN with the parameters shown in Figure 86 on page 140.

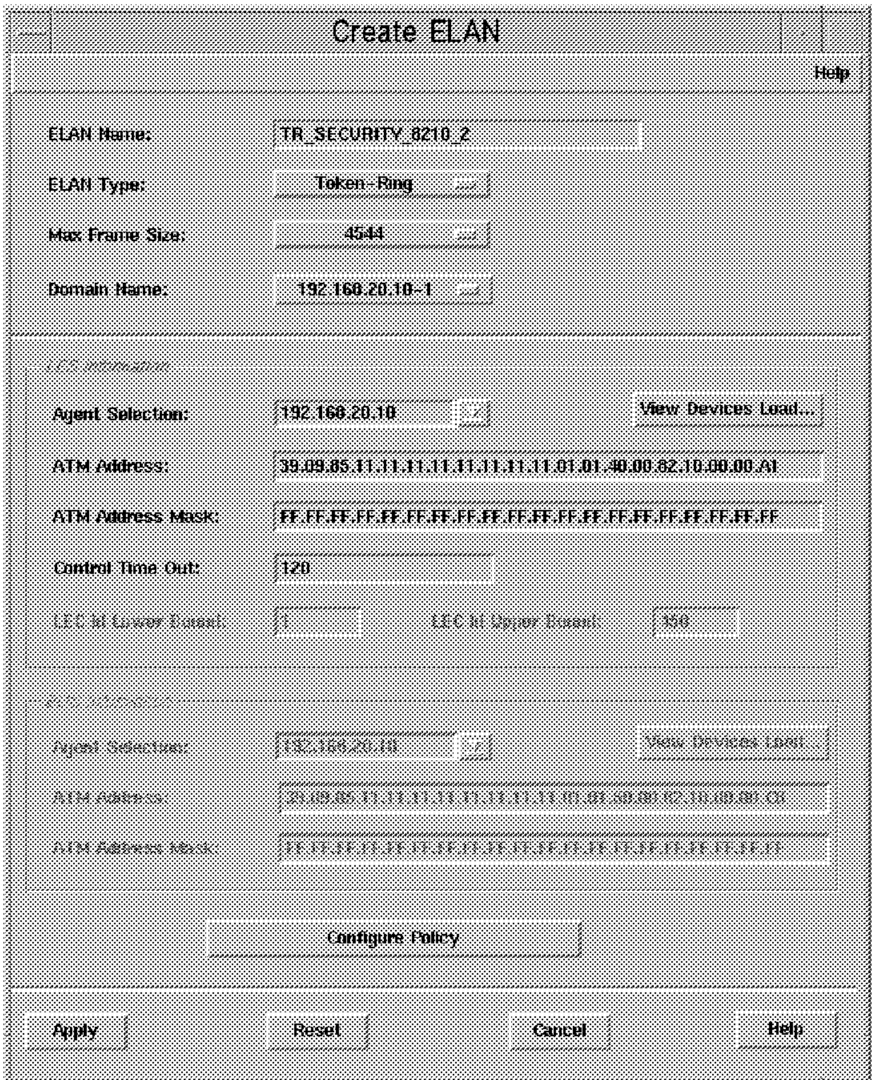

Figure 86. ELAN TR_SECURITY_8210_2

The policy definition shown in Figure 87 on page 141.

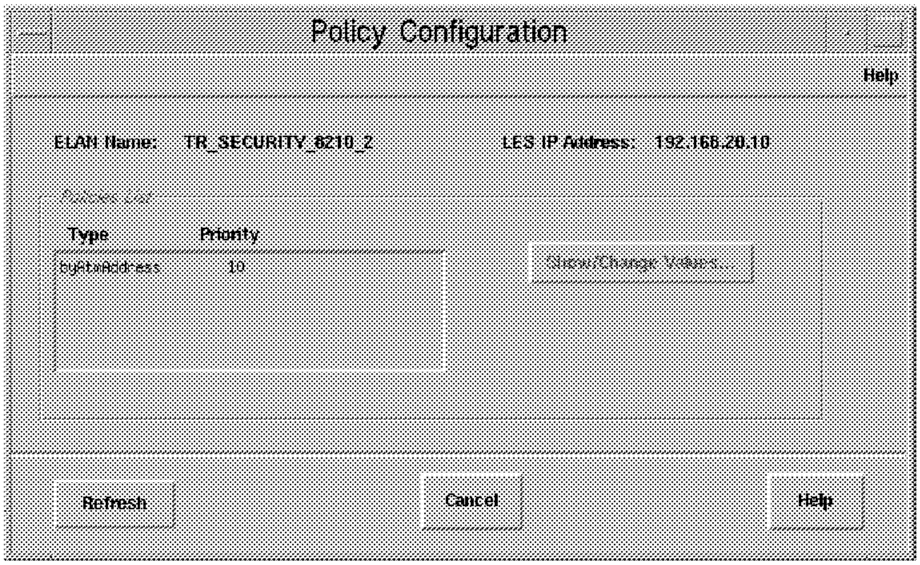

Figure 87. The Policy Configuration Panel

6.1.6 Defining Policy Values for Automatic LECs Only

To enable security for TR_SECURITY_8210_1 ELAN we added an LEC by adding its ATM address to the policy value table 39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.00.00.04 (see Figure 88).

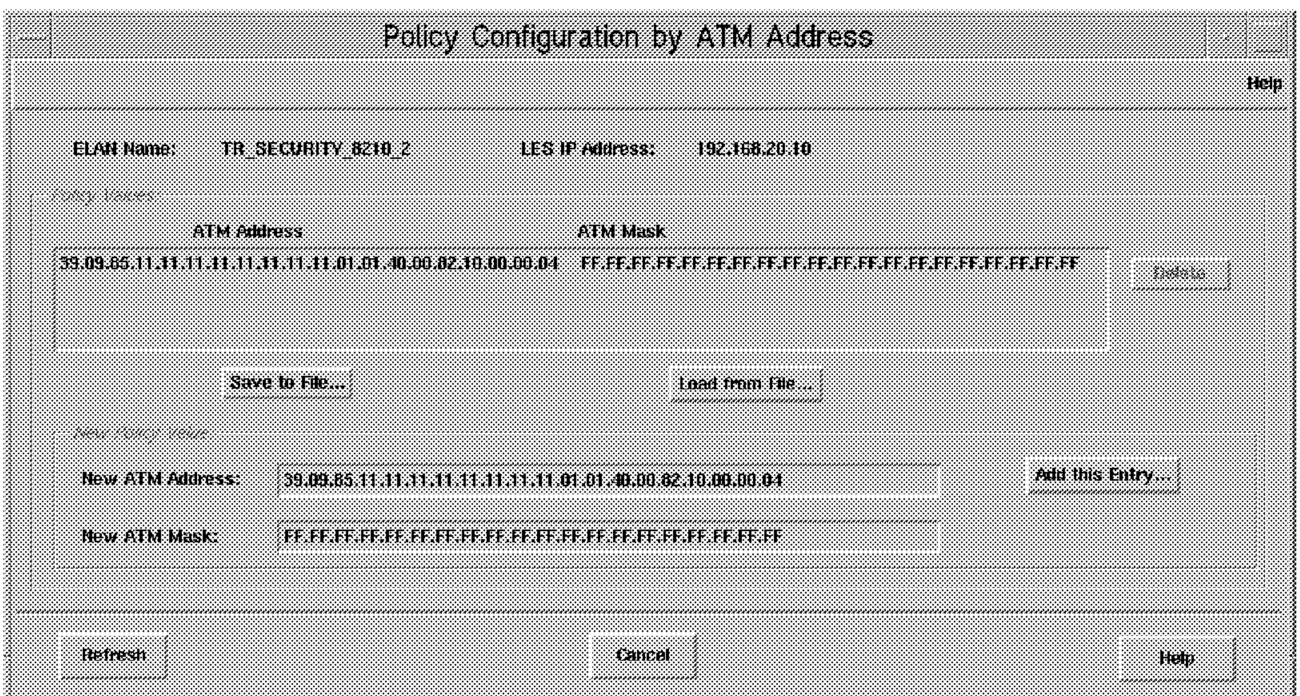

Figure 88. The Policy Configuration by ATM Address Panel

In the LAN Emulation domain submap the TR_SECURITY_8210_1 ELAN icon appears.

If we double-click on the **TR_SECURITY_8210_1 ELAN** icon we see that three LECs have already joined the ELAN, one automatic and two manual:

1. The MSS automatic internal LEC (192.168.20.10-2), that we've just defined in the TR_SECURITY_8210_1 policy values table.
2. A workstation manual LEC (40.00.EE.EE.00.00.81) whose LES ATM address field contains the TR_SECURITY_8210_1 LES ATM address.
3. An 8281 ATM bridge manual LEC (40.00.82.81.0B.0B.00) whose LES ATM address field contains also the TR_SECURITY_8210 LES ATM address.

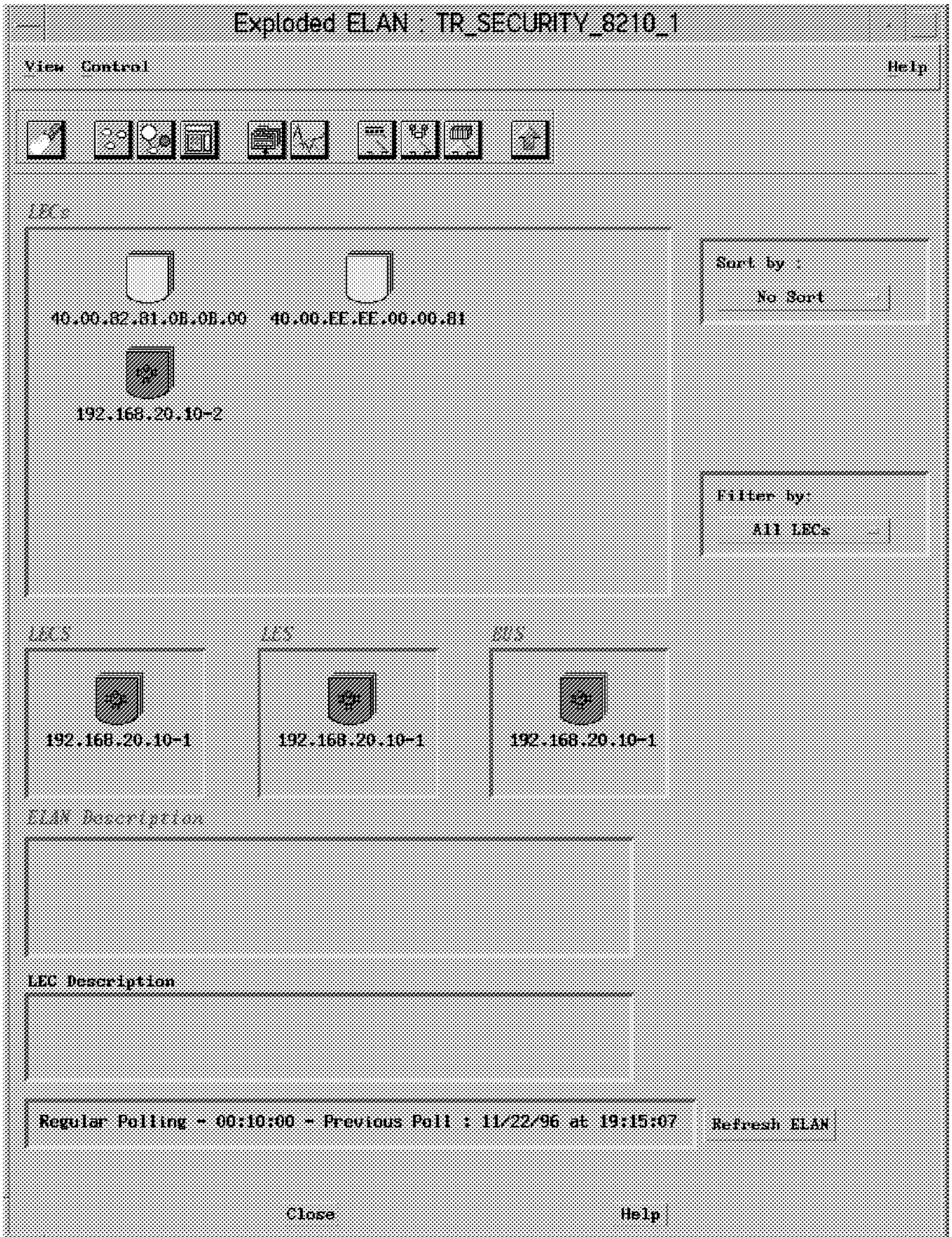

Figure 89. The TR_SECURITY_8210_1 ELAN Topology

The LES Configuration panel mirrors perfectly this situation by displaying three entries in the Registered LAN Emulation Clients (LECs) (see Figure 90 on page 143).

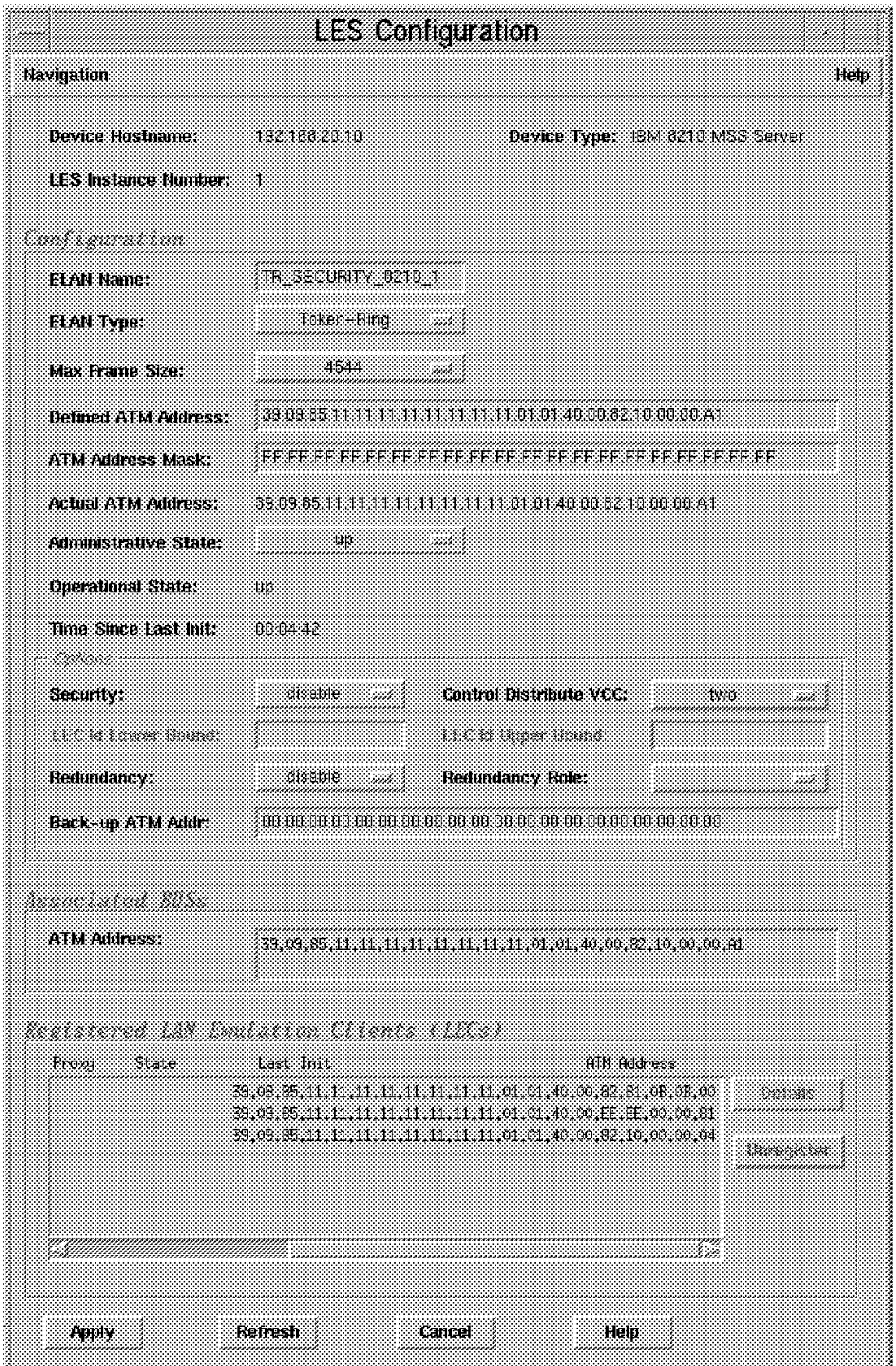

Figure 90. The LES Configuration Panel before Security Is Enabled

6.1.7 Setting Security

From this panel we enabled security. Immediately the three LEC entries disappear. Nways Campus Manager breaks down all the LEC′s LAN Emulation service VCCs so previously joined LECs have to restart joining the ELAN.

Note: When security for an ELAN is enabled from the MSS console it doesn′t break down all previously established VCCs, but rather controls access of new LECs (see Figure 91).

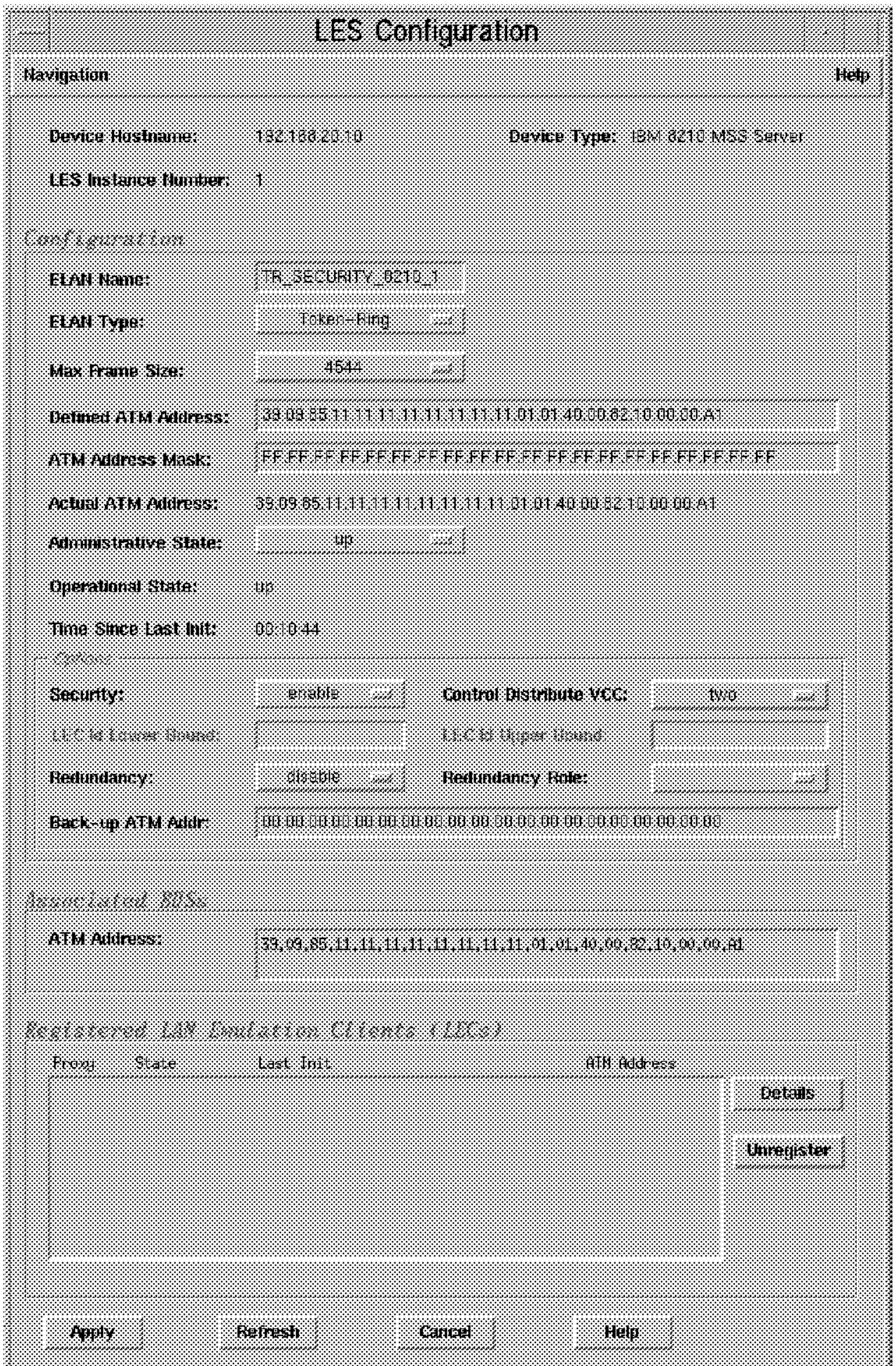

Figure 91. The LES Configuration Panel Just after Security Is Enabled

After a short period of time the automatic LEC joins the ELAN but not the manual LECs. The LES Configuration panel displays only one entry for the MSS internal LEC (see Figure 92 on page 145).

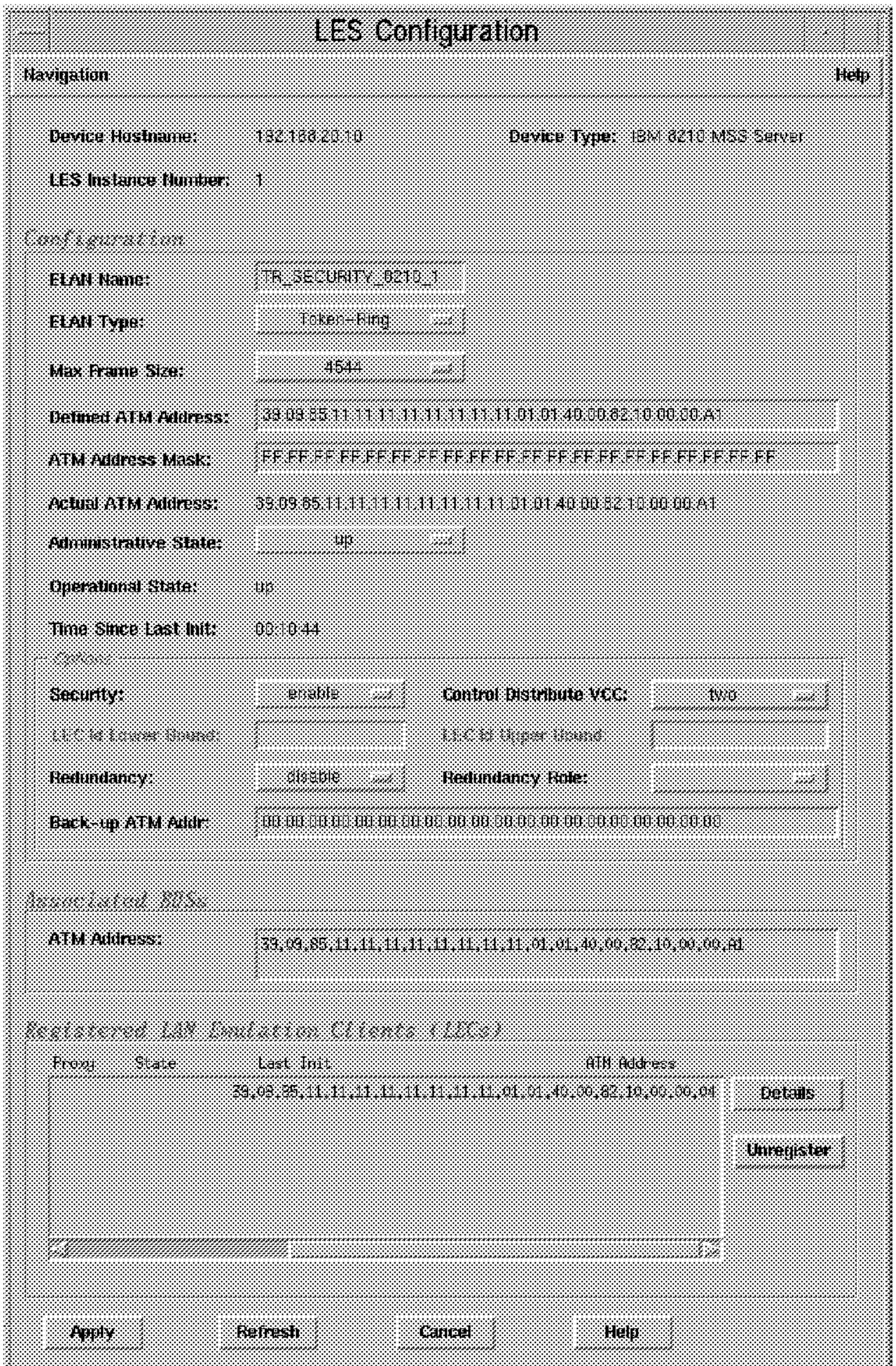

Figure 92. The LES Configuration Panel after a While

From the TR_SECURITY_8210_1 ELAN screen the two manual LECs icons have turned gray due to the fact that they cannot join the ELAN because the LES has translated their LE_JOIN_REQUESTs into LE_CONFIGURE_REQUESTs and sent them to the LECS through the LECS interface. The LECS has rejected these requests as no matching entries were found in the policy value table (see Figure 93 on page 146).

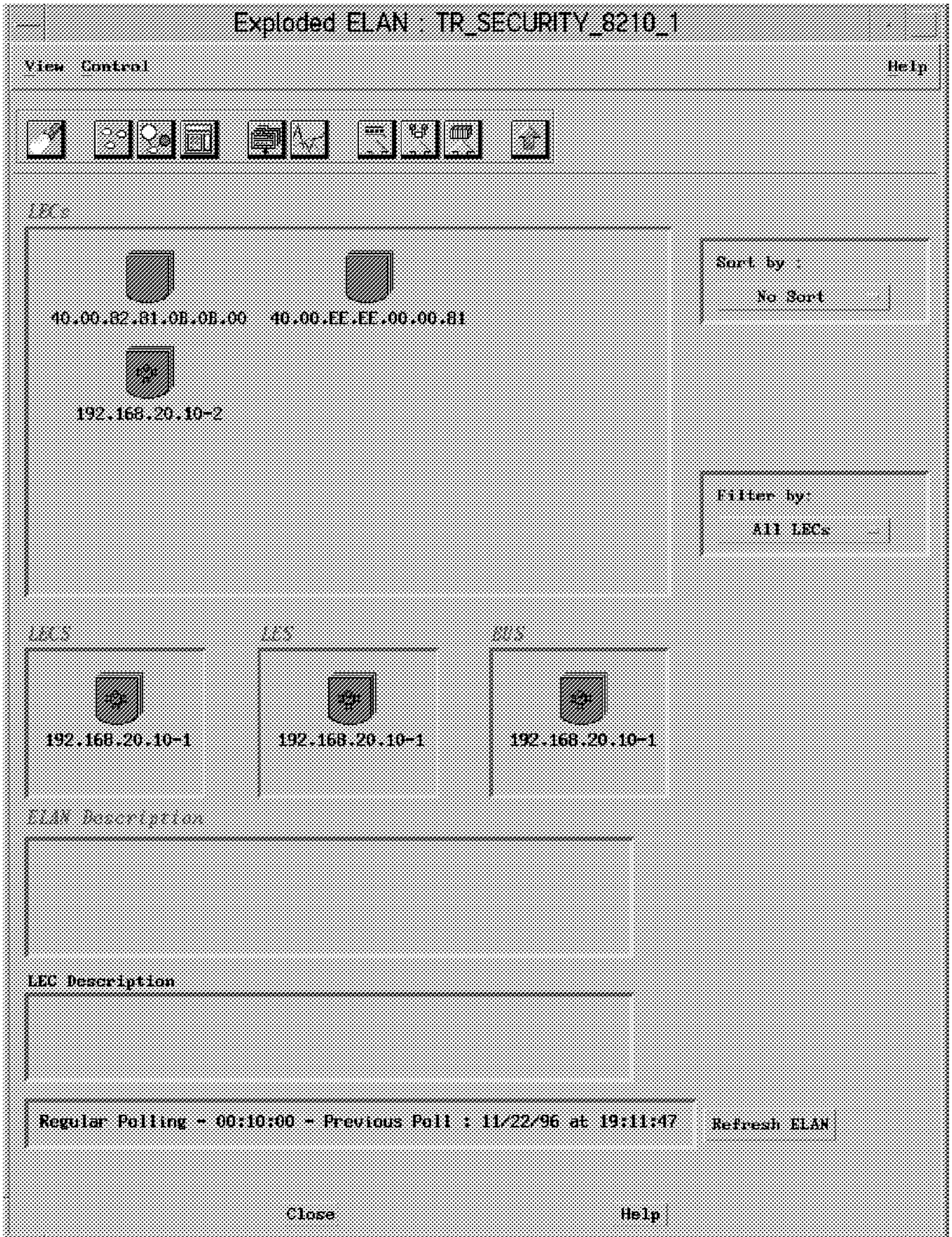

Figure 93. The TR_ELAN_8210_7 after Reverse Drag and Drop Is Completed

6.1.8 Adding Policy Values for Manual LECs

The policy value table is amended to add the ATM addresses of the two manual LECs.

Select the LES ATM address in the ATM Address field. The **Policy Details** push button highlights; click on it and the Policy Rule panel appears. Select the entry and click on the highlighted **Show** push button; the Policy Configuration by ATM Address panel is shown. Now add the two manual LECs ATM addresses (see Figure 94):

```
39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.81.0B.0B.00.00
39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.EE.EE.00.00.00.81
```

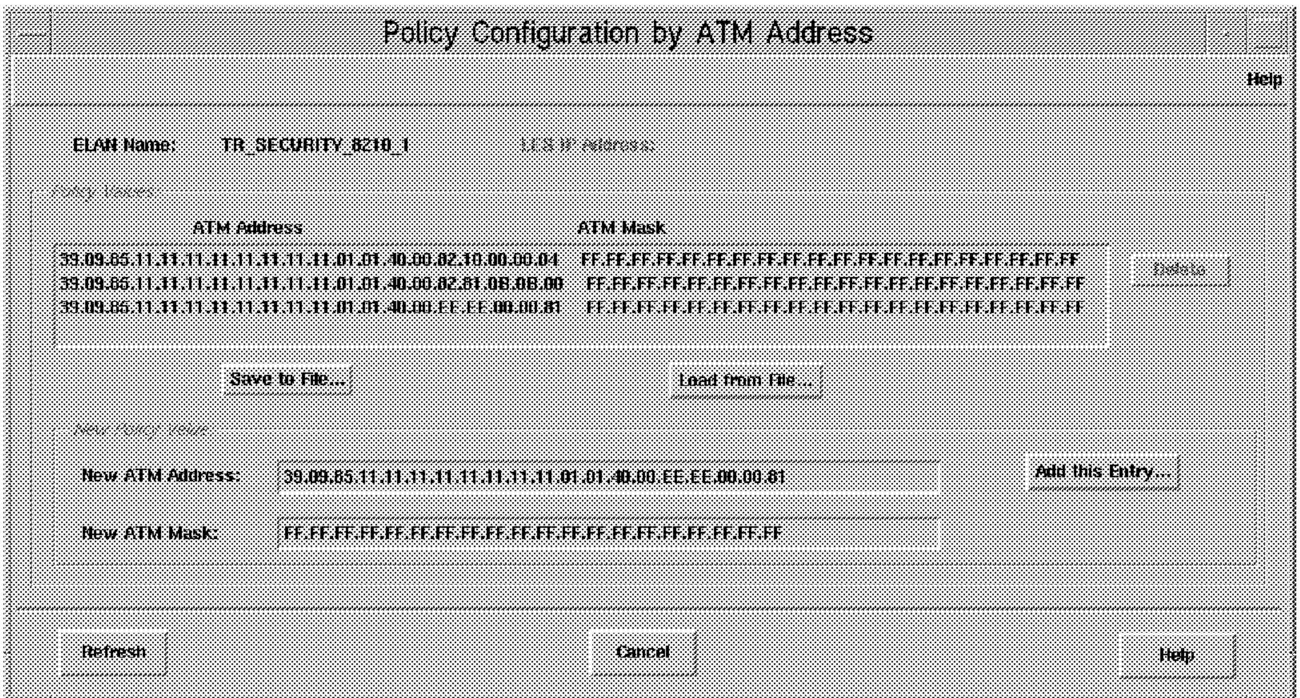

Figure 94. Adding the Manual LECs ATM Addresses to the Policy Value Table

Now the two manual LECs have joined the ELAN. Applying security will change the manual LECs into automatic LECs. The following events will happen:

- The LECs sent LE_JOIN_REQUESTs to the LES.
- The LES translated them into LE_CONFIGURE_REQUESTs and sent them to the LECS through the LECS interface.
- The LECS could assign both manual LECs to the LES thanks to new policy value table entries.
- The LECS sent back positive LE_CONFIGURE_RESPONSEs.
- The LES translated them into positive LE_JOIN_RESPONSEs and sent them to the LEC.
- The LECs joined the ELAN.

6.1.9 Comments on Security

To maximize security, the MSS security function is not enough. The most reliable policy rule to enforce security is by ATM address as ATM addresses are more difficult to emulate than other LE_CONFUGURE_REQUEST and LE_JOIN_REQUEST frame fields:

- ATM switches reject the same ESI ILMI registration on two different ports (IBM 8260 ATM Switch 2.0.4).
- Some ATM switches (not the IBM 8260 ATM Switch), offer an Address Screening function that forces ATM stations to use their actual ATM addresses (registered through ILMI) in call setups.
- Even if the ATM switch (IBM 8260 ATM Switch) let ATM stations use for their call setup an ATM address (ESI) different from their actual ATM address, the pirate station wouldn′t join the ELAN. The ELAN LES will issue a call setup to add the pirate station to its point-to-multipoint control distribute VCC; upon reception of the call setup the ATM switch will route the call to the regular ATM station. To route call set up to its local ports an ATM switch uses the ESI part of the call setup destination ATM address; as for it this ESI is associated to a regular ILMI registered ESI it routes the call setup to the corresponding port.

All the comments above assumes, that the premise housing the ATM switch is locked and the regular station is not powered off. Otherwise the pirate station could regularly register the stolen ESI, and join the ELAN.

Chapter 7. Using Router and Bridge Manager Version 2.2

This chapter gives a brief overview of the functions available with Router and Bridge Manager Version 2.2. and provides an insight into its capabilities to help manage our ELAN network, for monitoring and problem determination.

Further reading for the Router and Bridge Manager application can be found in the *Router and Bridge Manager Version 2.2 User's Guide*. In addition there is a readme contained in the installation package of Router and Bridge Manager called:

```
/usr/rabmv2/usr/OV/doc/rabmv2.README
```

Some of the key changes in Release 2.2 are:

- Customization of MIB objects, thresholds, and traps.

  Router and Bridge Manager defines a hierarchy of managed objects. You can customize each level of the hierarchy to monitor only those MIB objects in which you are interested in.

  The hierarchy of managed objects allows you to group objects for interface types, protocols, or system capabilities. These objects are associated with the defined node.

- Distributed polling using the Mid-Level Manager (MLM)

  A function of Systems Monitor to reduce overall SNMP-related traffic detects that SNMP thresholds are exceeded, and notifies the centralized management station running Router and Bridge Manager.

- Enhanced user interface using NetView for AIX submaps.

  A new submap called router and bridge manager appears on the TME 10 NetView root map, which you use to add nodes (that is, networking devices) that you wish to monitor. By assigning templates to these nodes, you can control which thresholds are defined and active and what traps are configured. As these network events occur the status of each node will change according to the condition.

This chapter is divided into the following sections:

1. Exploring the default configuration
2. Defining our nodes
3. Using Router and Bridge Manager software
4. The Mid-Level Manager configuration

7.1 Exploring the Router and Bridge Manager Configuration

The Router and Bridge Manager definitions are located from the NetView interface by the pull-down menus shown in Figure 95 on page 150.

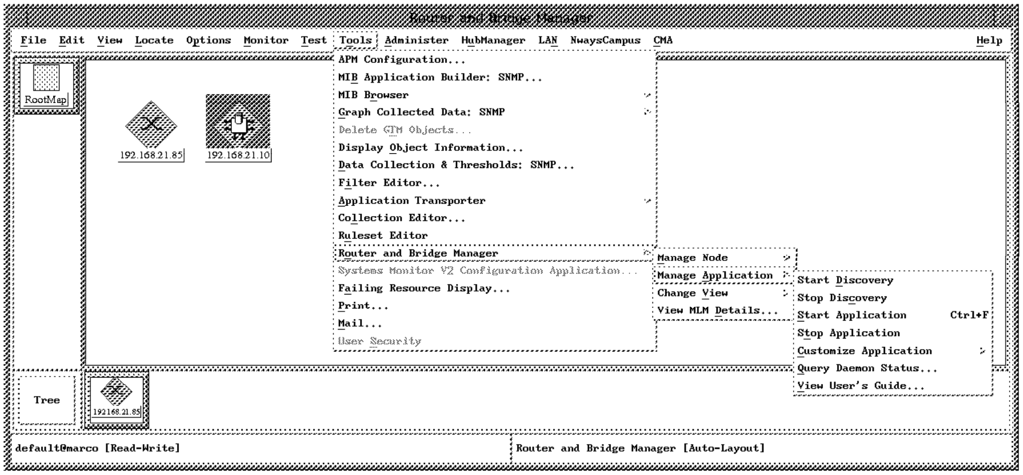

Figure 95. How to View the Default Definitions

The default definitions are viewed by selecting **Tools->Router and Bridge Manager->Manage application->Customize Application** from the NetView pull-down menu. From here you can now view the templates and resources. First we take a look at the default templates.

7.1.1 Template Definitions

Each of our managed components will have a template assigned to it. For each template there are a number of predefined resources; these resource have associated thresholds and traps.

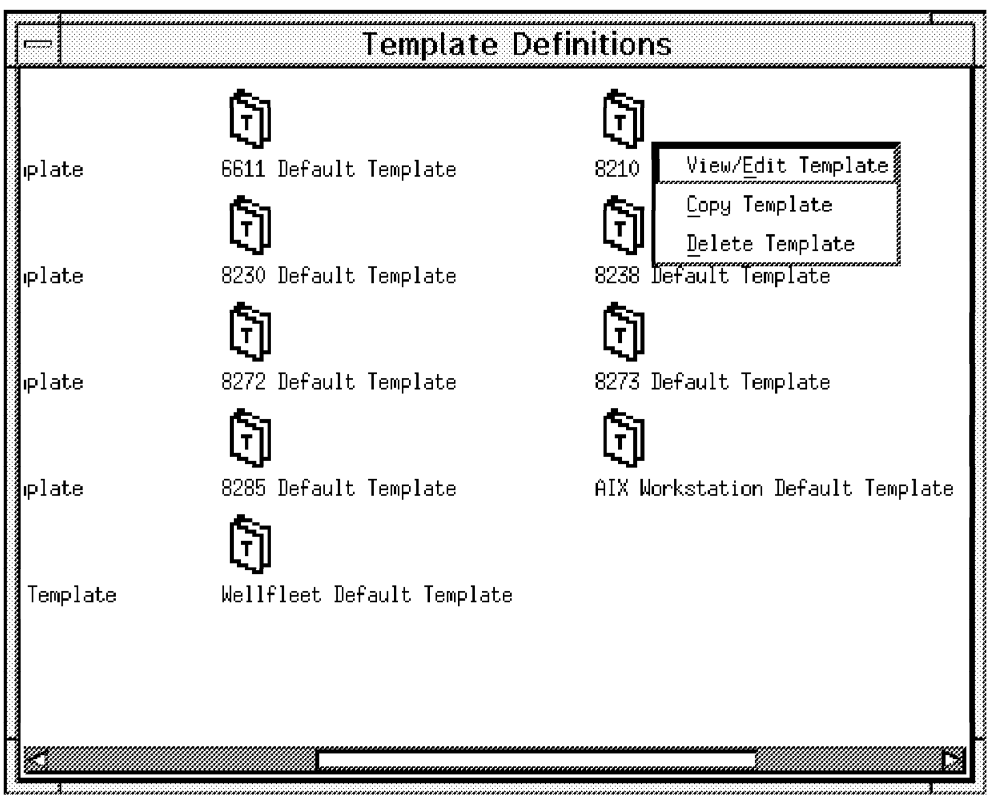

Figure 96. Default Templates

Figure 96 shows the pre-loaded templates installed by Router and Bridge Manager. To display this screen select **Define a Template** from the customize application pull-down menu.

For each specific device there are both interface and capability resources defined.

For our ATM environment we have resources defined for the LAN Emulation entities and ATM interfaces.

To see the predefined resources for the IBM 8210 use the right-hand mouse button to select the 8210 icon followed by **View/Edit Template**. Figure 97 will appear.

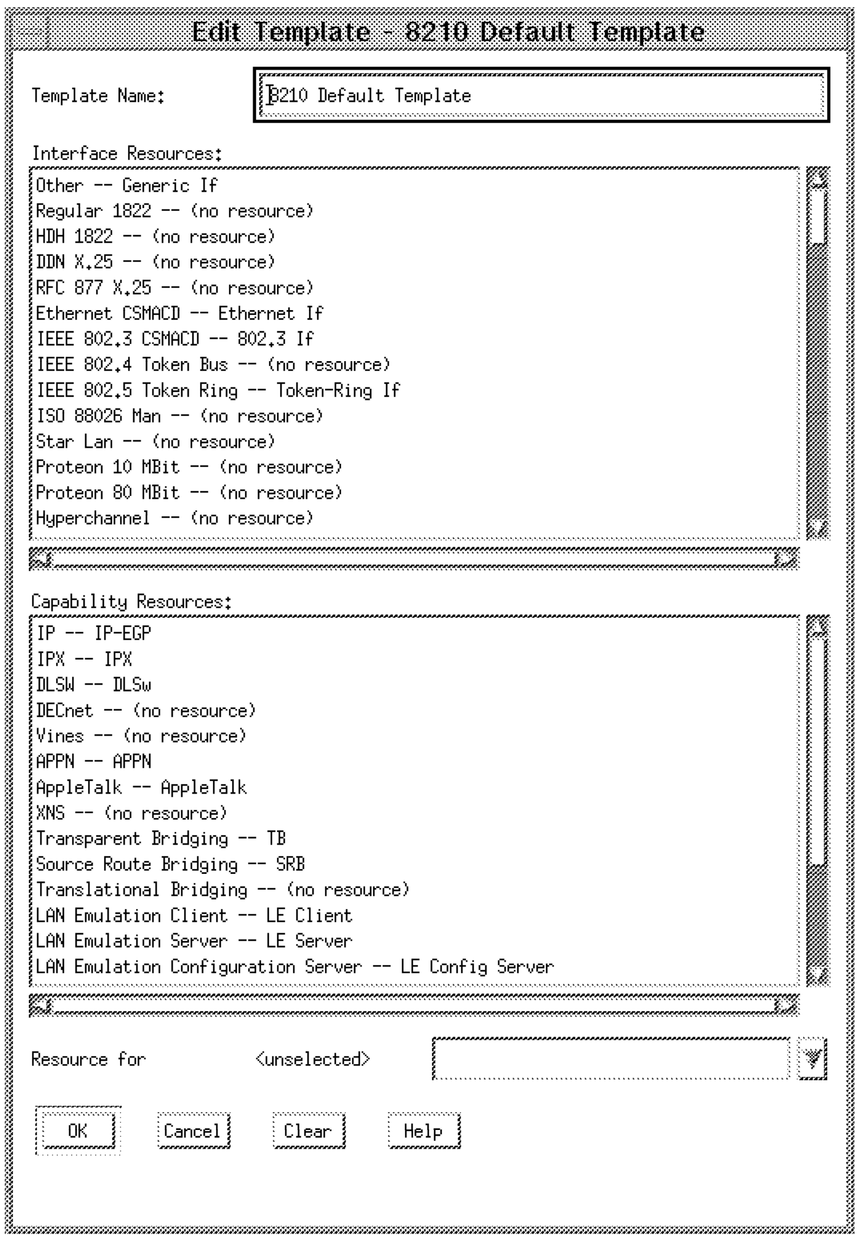

Figure 97. Associated Resources for the 8210

This screen shows what resources are defined for the 8210. The fields marked with (no resource) signify that there are no definitions contained within Router and Bridge Manager for this device.

We can see that there are resource definitions for the 8210 for LAN Emulation Server. To view this resource definition select **Define a Resource** from the Customize Application menu.

The tasks that can be performed are:

1. Define/Create Thresholds
2. Defined Traps
3. Defined MIBs

By performing changes to the templates, when we add our nodes to the Router and Bridge Manager configuration the templates will be copied. This means that we only need to make the changes once on a global scale for each specific device requiring management. However, if you only require specific thresholds and traps to be defined for single devices, then the modifications can be made at a later time.

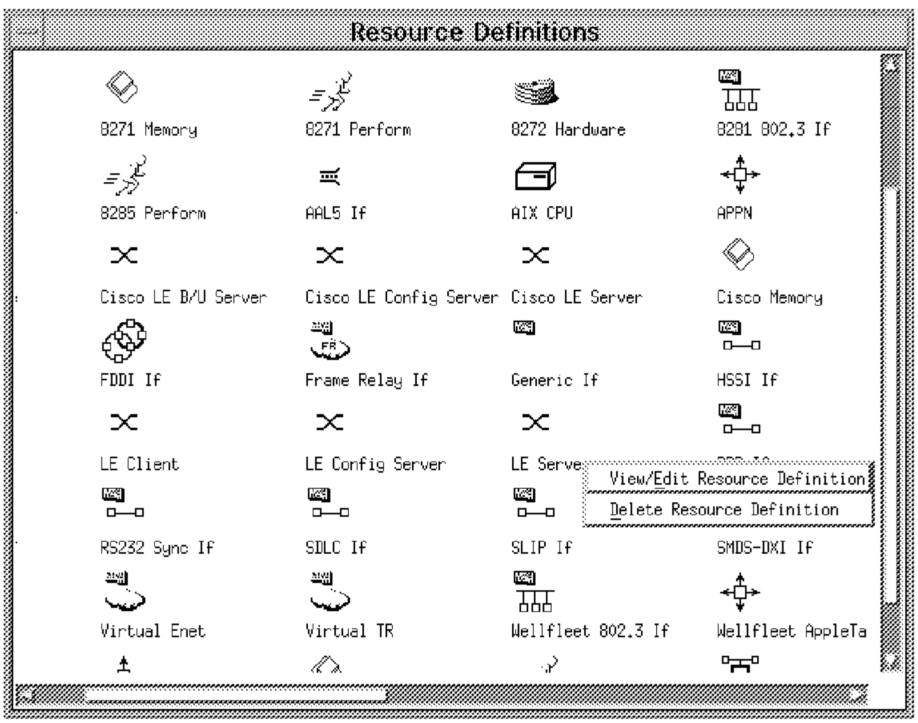

Figure 98. Default Resources for the 8210

The LE Server resource definitions can be viewed by using the right-hand mouse button and selecting **View/Edit Resource** (see Figure 99 on page 153).

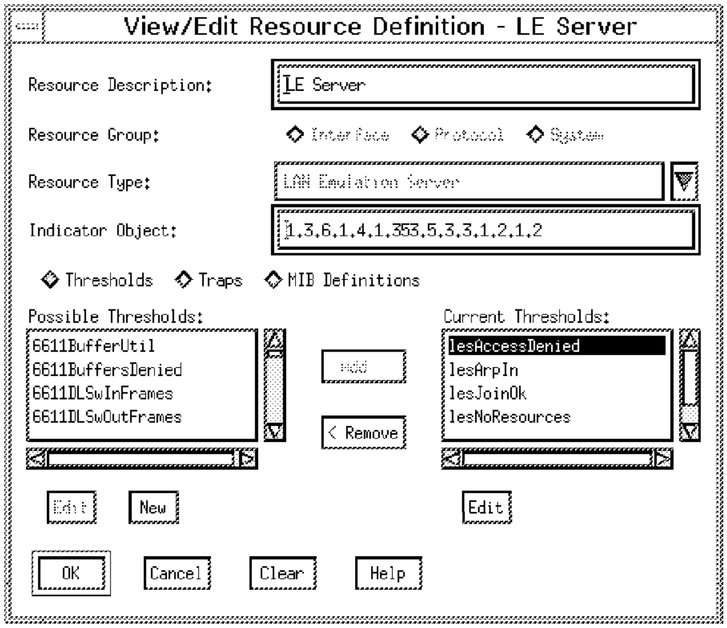

Figure 99. LE Server Definitions

These thresholds must be activated by moving the definition from Possible Thresholds to the Current Thresholds. MIB definitions defined in Router and Bridge Manager can be activated and deactivated but you cannot edit the MIB definitions from here.

Resources themselves cannot be added or deleted but it is possible to change the resource definitions, for instance the associated thresholds and traps. The thresholds defined for our LES resource are:

lesArpIn The number of successful LES ARP requests.

lesJoinOk How many LECs have joined a specific LES.

lesNoResource The LES does not have enough resource left to perform a required action.

By clicking on the trap button you can view the traps defined (see Figure 100 on page 154).

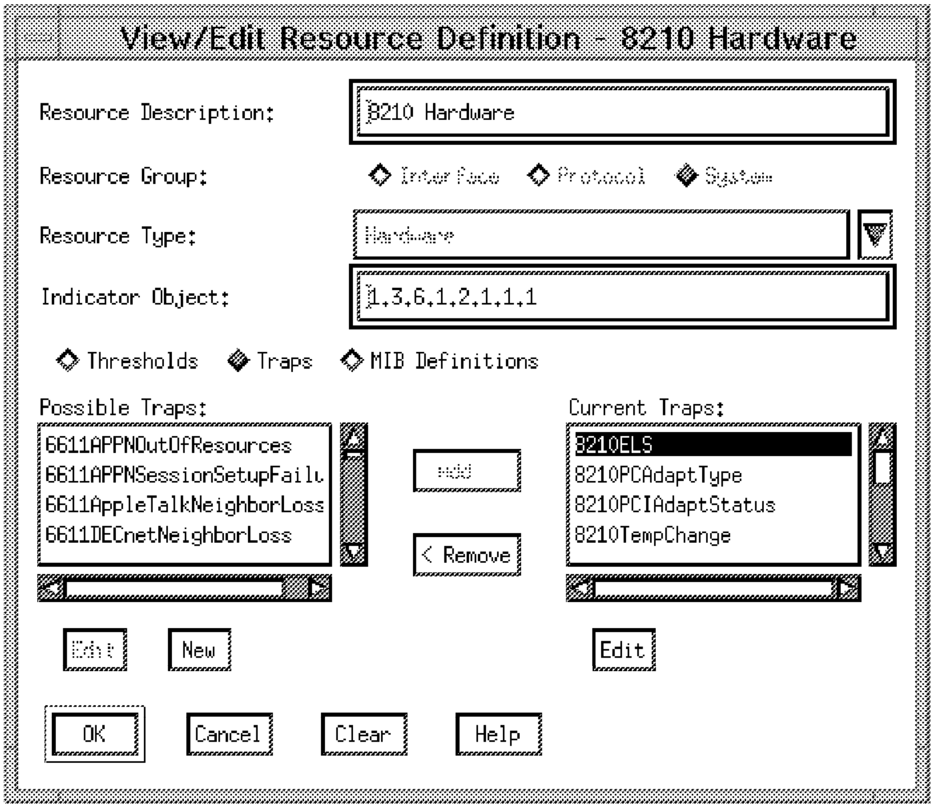

Figure 100. 8210 Trap Definitions

Existing traps can be edited or new traps can be added. The traps that are currently assigned to a resource are shown in the Current Traps area. The traps that can be assigned to a resource are located in the Possible Traps area. To edit an active trap it has to be moved over to the Possible Trap area.

Note: By modifying the default definitions you are modifying the configuration for all other devices of that particular type. Individual devices can be modified as subsequent tasks after the device has been discovered by the Router and Bridge Manager application.

7.1.2 Thresholds

Router and Bridge Manager performs thresholding on the ATM Forum LAN Emulation MIB definitions for LAN Emulation. It is useful to familiarize yourself with these MIBs in order to see what other thresholds can be defined for a managed device. The SNMP MIB definitions can be found in the /usr/OV/snmp_mibs directory. The files are:

```
af1129-ELANLECS.mib
af1129-LES.mib
af1129-BUS.mib
af0044-LEC.mib
```

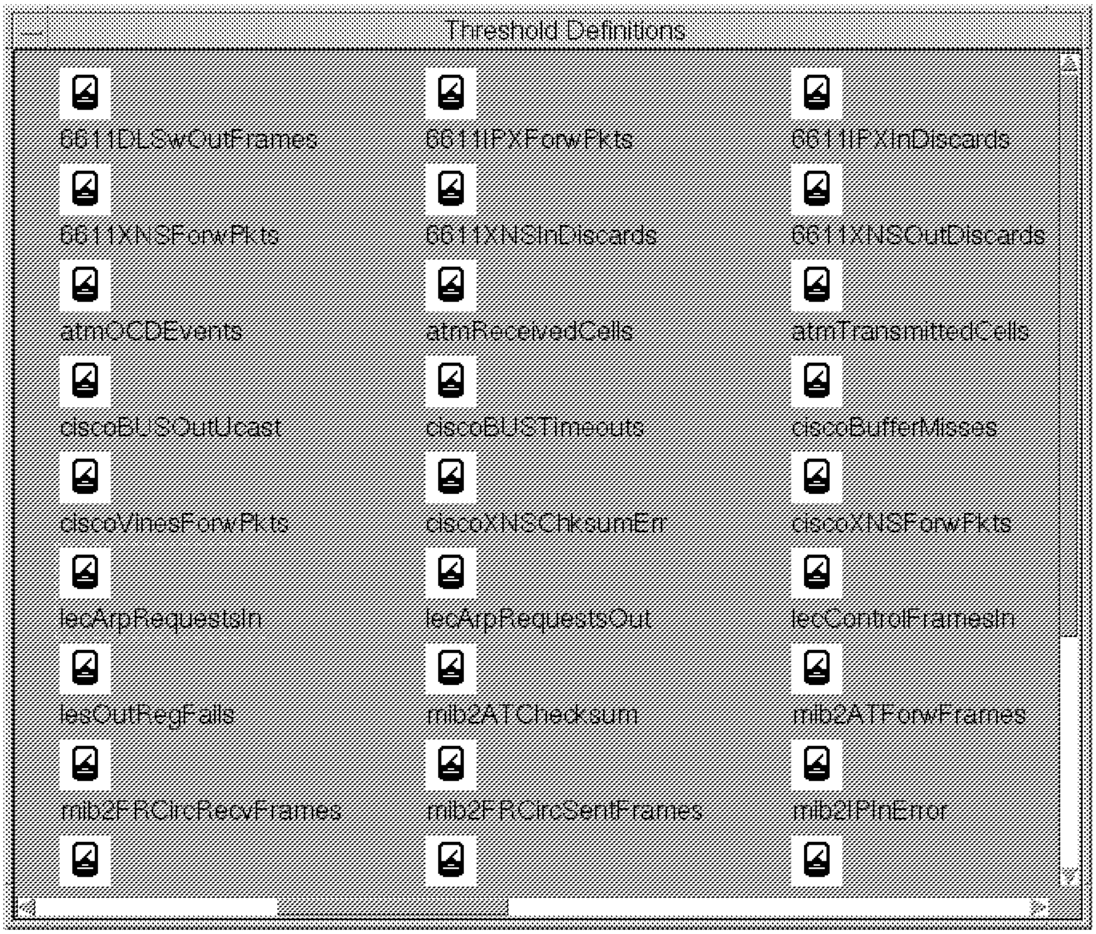

Figure 101. List of Default Thresholds

Figure 101 shows the pre-defined thresholds. To view this screen select **Define a Threshold** from the Customize Application menu.

Select a threshold and click on the **Edit** button to display the window shown in Figure 102 on page 156.

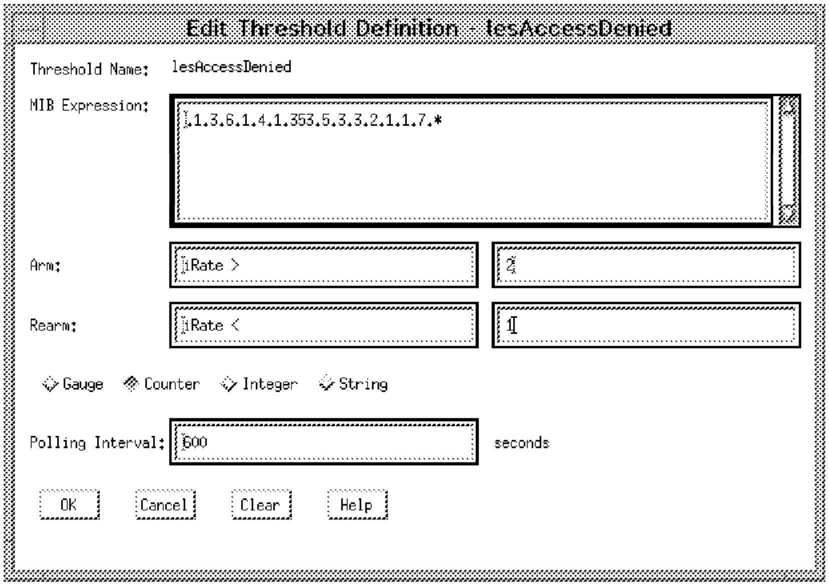

Figure 102. Default Threshold for LES Access Denied MIB

This threshold definition displays the specific MIB variable it will poll, the ARM/REARM values and the polling frequency. These thresholds will become active when the node is defined.

This resource is a MIB. We can view the definition of this MIB using the NetView for AIX MIB browser.

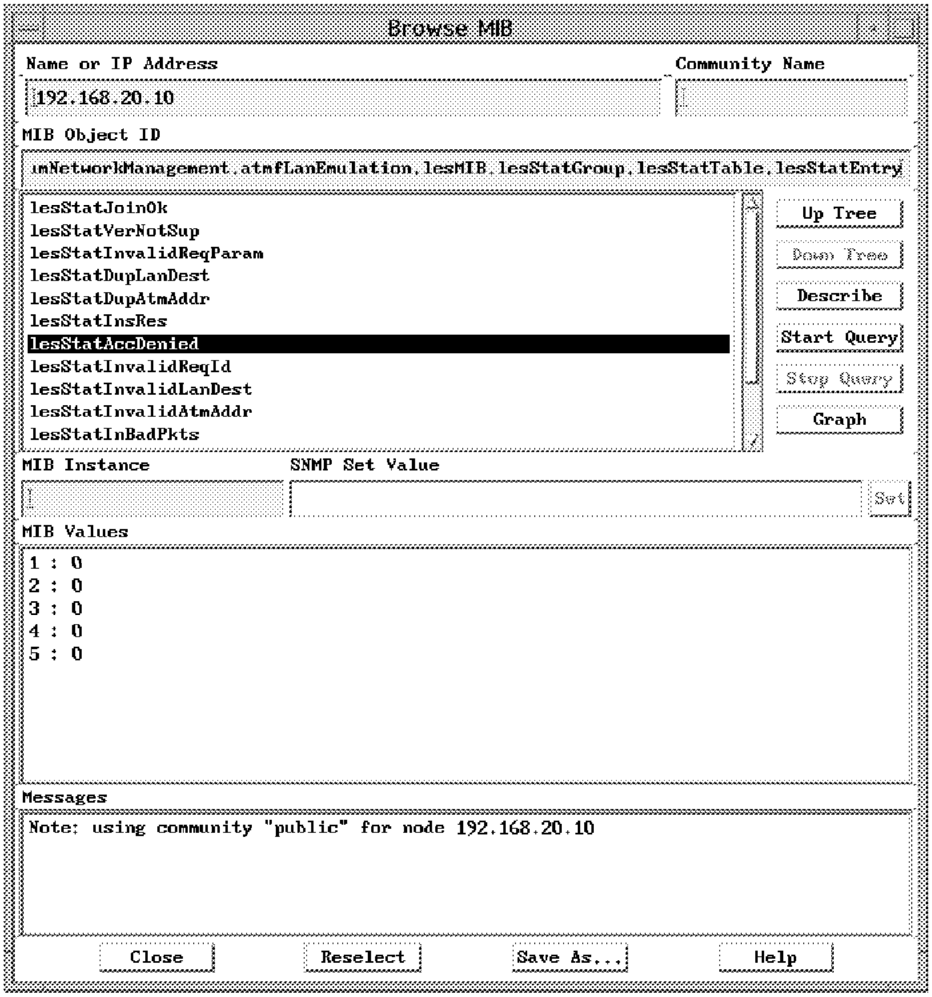

Figure 103. MIB Identifier for lesStatAccDenied

Figure 103 shows the threshold definition for the specific MIB.

7.1.3 Trap Definitions

The pre-defined traps can be viewed by selecting **Define a trap** from the Customize Application pull-down menu (see Figure 104 on page 158).

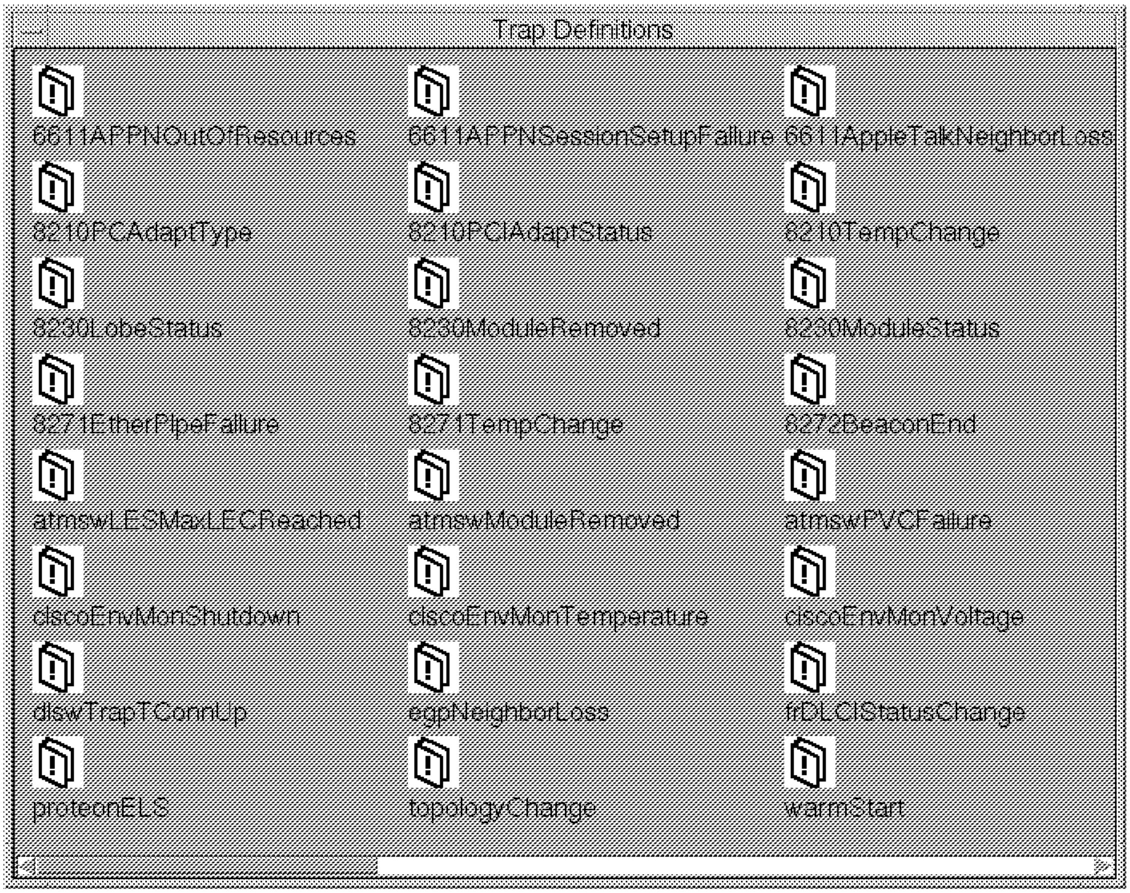

Figure 104. Default Trap Definitions

Select a trap and click on the **Edit** button to display the window similar to screen Figure 105 on page 159.

This trap will be generated from the ATM device, by including this in the template. If this trap is received by NetView, the resource icon representing this resource will change color reflecting a status change.

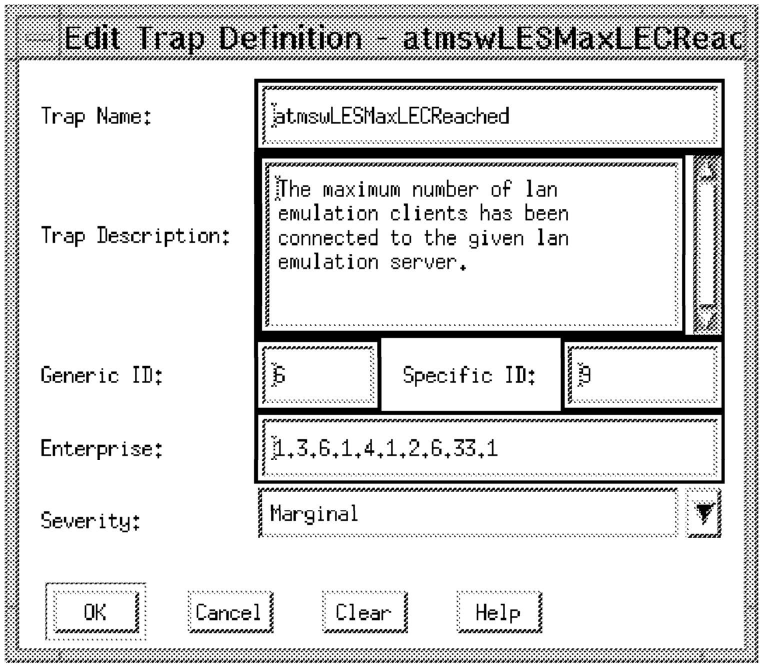

Figure 105. atmswLESMaxLECReached Trap Definition

Figure 105 shows the trap definition for an 8285 which will be sent to the management station when the maximum number of LAN Emulation clients has been exceeded.

Here you can view, edit or delete the trap definition. To view the traps for each managed device you can use the NetView for AIX Event Customization program, and view each available trap for each device.

7.2 Defining the ATM Nodes

For this simple example we add two ATM devices in our network to the Router and Bridge Manager configuration. These are:

- IBM 8210.
- IBM 8285 Switch

The nodes can be added from any submap. We chose to add the devices from the ATM Cluster submap.

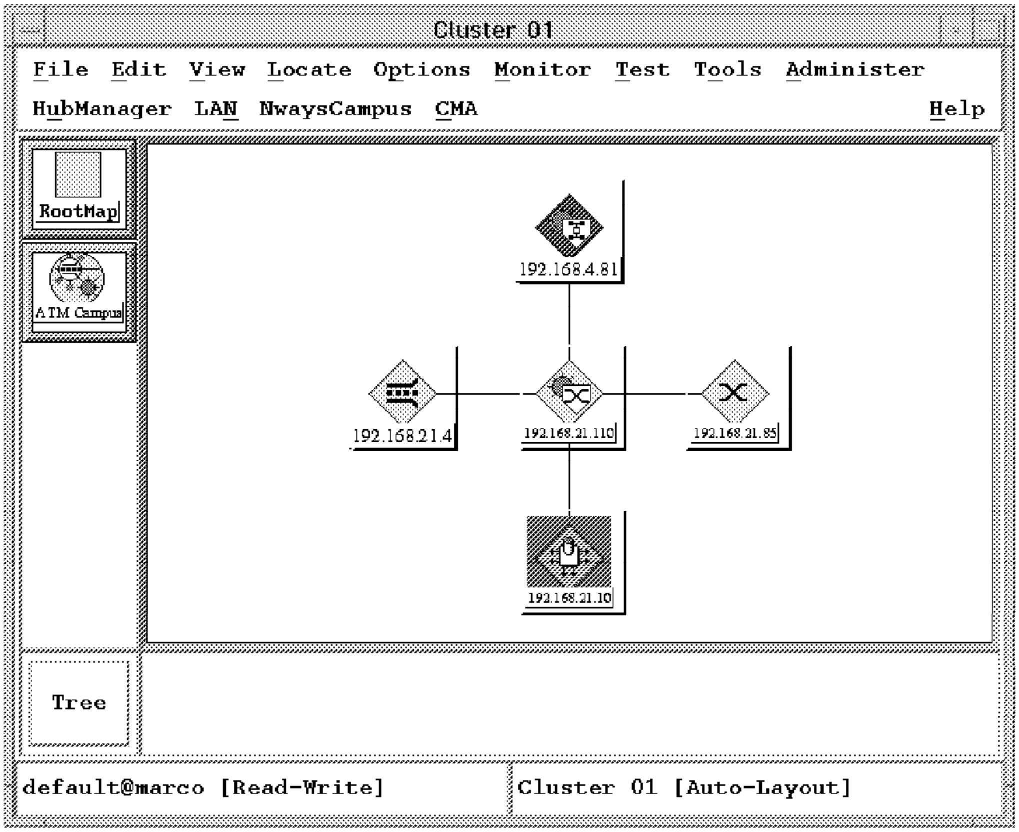

Figure 106. Cluster Map

When we add these nodes to the Router and Bridge Manager submap the default templates are copied and an icon is placed under the Router and Bridge Manager submap for each managed node.

There are two ways to add new nodes to the Router and Bridge Manager. The first is to select the node from one of the TME 10 NetView submaps; the second is to activate the auto-discovery parameter.

To add nodes to be managed by Router and Bridge Manager do the following. (The mode we used was to manually add our nodes.) From the NetView Root map:

1. Double-click on the **ATM Campus** icon. The Cluster submap will appear.
2. Select the node using a single-click on the right-hand mouse button. (In our case we selected an 8210 icon.)

From the NetView pull-down menu:

1. Select **Router and Bridge Manager->Manage Node->Add Node**. This will display screen Figure 107 on page 161.

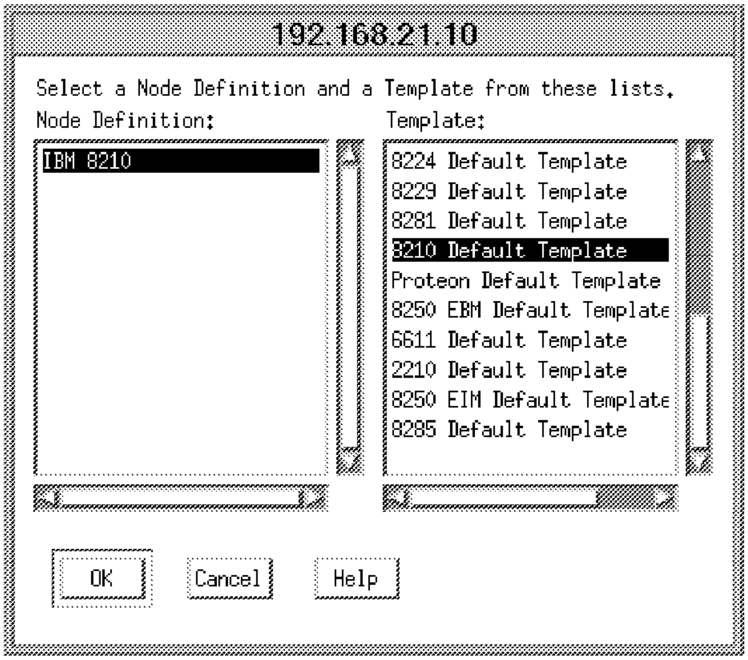

Figure 107. 8210 Definition

2. From here click on **OK**. The node will be added to the Router and Bridge Manager submap.

The auto-discovery method is as follows:

1. From the PSM window select **Edit->Modify/Describe->Map** from the NetView for AIX pull-down menu.
2. Click on **RABM Discovery** followed by **Configure for this Map**. This will show screen Figure 108.

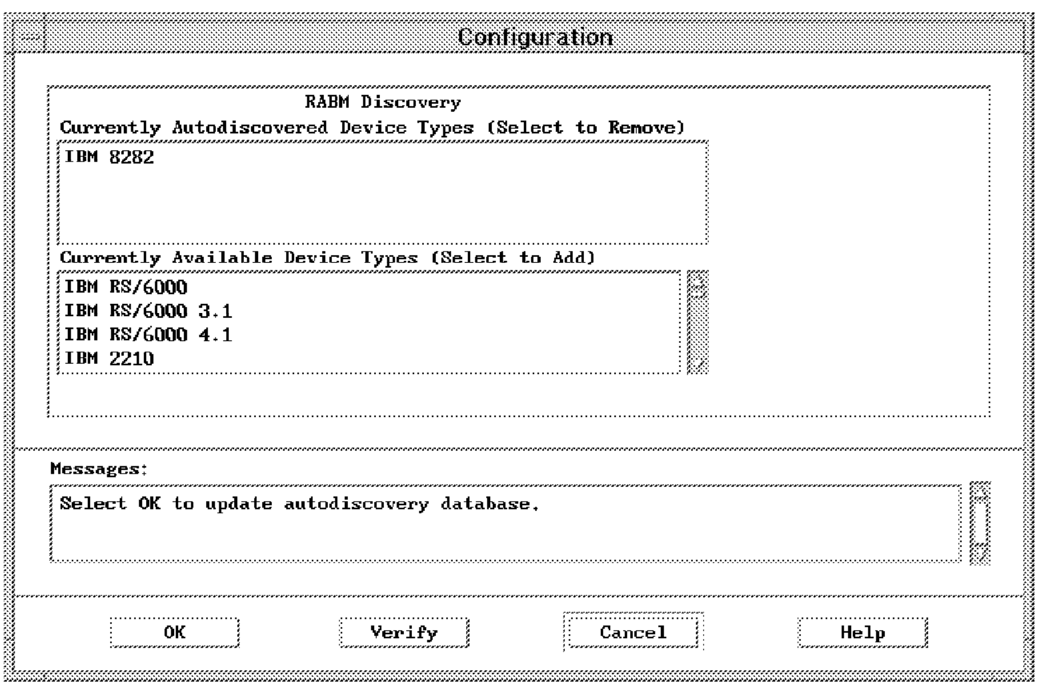

Figure 108. Router and Bridge Manager Modify RABM Auto-Discovery Settings

3. Using the left mouse button select the device type you want to discover, then click on verify. This will move the definition to the Currently auto-discovered device types window. When complete click on **OK**.

7.2.1 Viewing and Managing Nodes

The daemon rabm_discovery must be running. If not, this can be started by selecting **Tools->RABM->Manage Application-> Start Auto-discovery.**

By double-clicking on the **Router and Bridge Manager** icon located on the root submap, Figure 109 is displayed showing our managed devices. At this level you get a global status of all the nodes in the network monitored by Router and Bridge Manager regarding thresholds and traps. The actual status of the resource is indicated by different colors:

- Green = normal
- Yellow = marginal
- Critical = red

The status of the machines is derived from the managed resources shown below this icon.

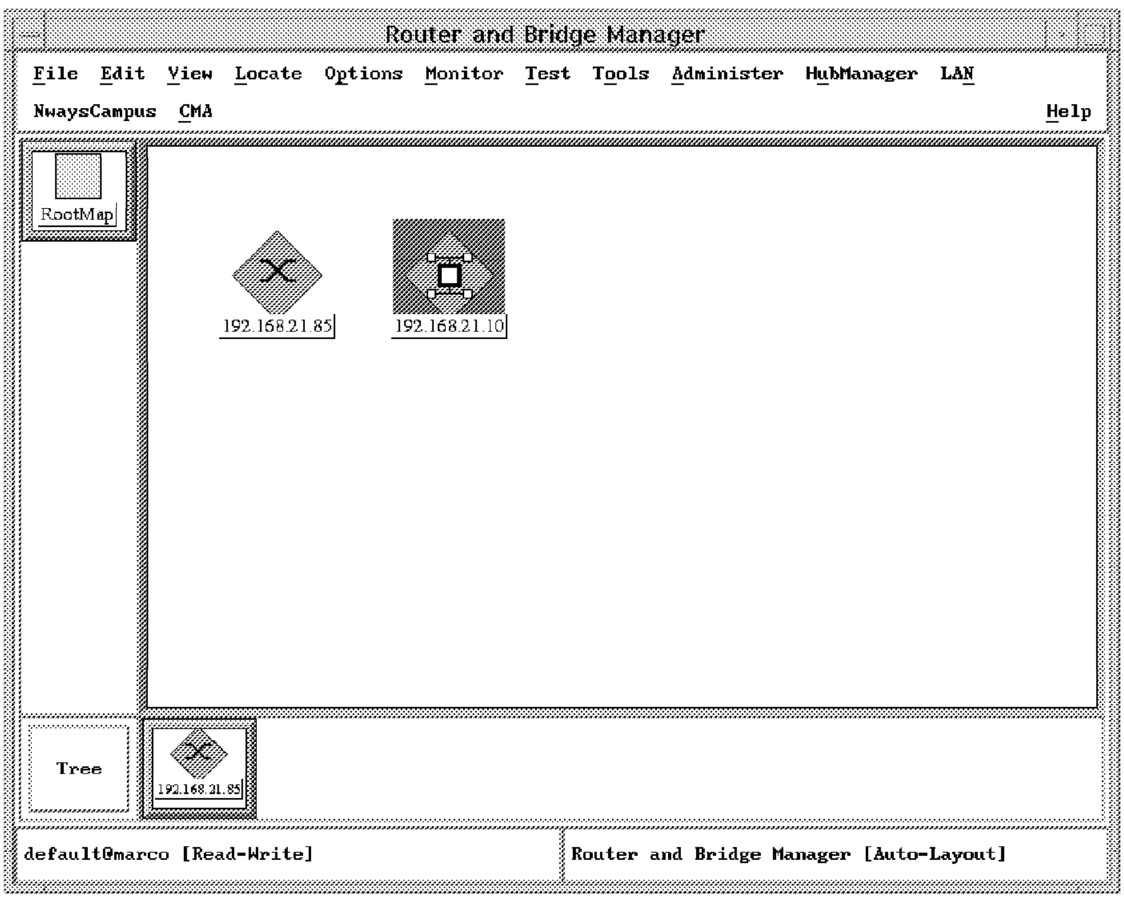

Figure 109. Router and Bridge Manager Submap

From this window, you can do two things:

- Change the node definitions regarding resources, thresholds and traps
- View the status of the monitor resources

7.2.2 Changing Node Definitions

Figure 110 shows how to access the settings for a particular device.

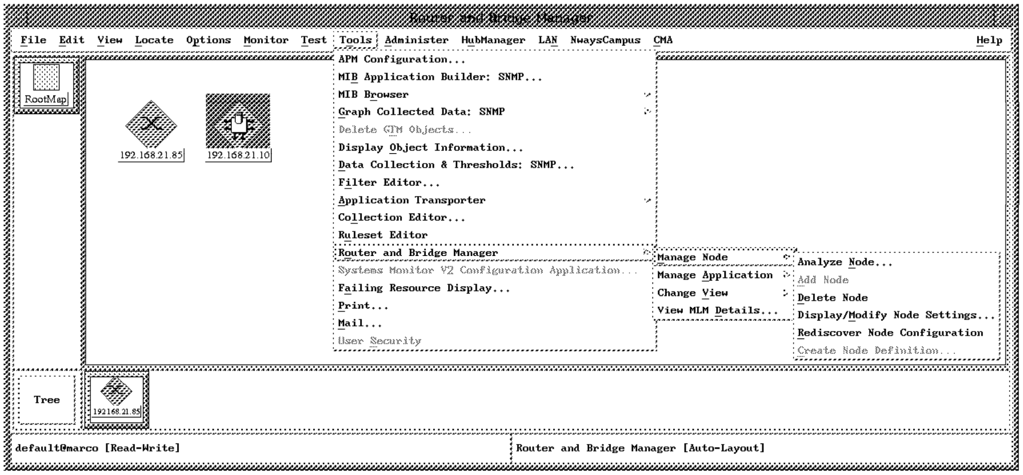

Figure 110. Disply/Modify the Node Settings

The process is described below:

1. Select a node using the right-hand mouse button.
2. Select **Router and Bridge Manager-> Manage Node** from the pull-down menu.
3. Click on **Display/Modify Node Settings**.

The node definition settings screen will appear like the one shown in Figure 111 on page 164.

By clicking on the **Protocols** button you will see the settings for the LAN Emulation Elements (see Figure 111 on page 164).

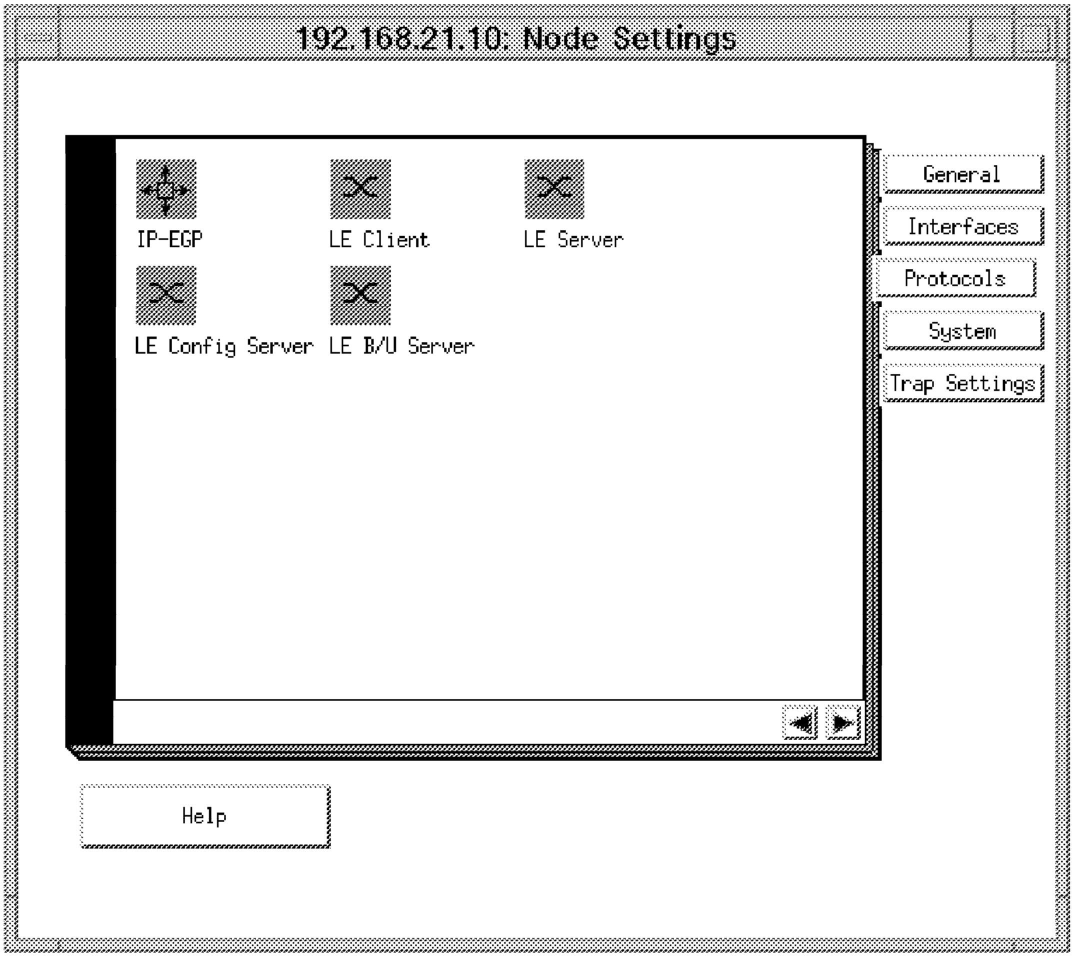

Figure 111. IBM 8210 Protocol Resources

Using the left-hand mouse button click on the **LE Client** icon, then choose **View/Edit Resource**. This will show Figure 112. From here you can view the threshold, trap and MIB definitions for this node.

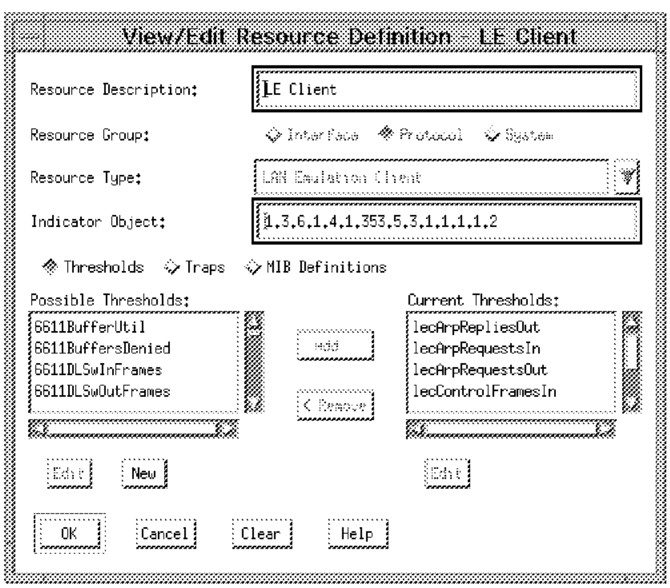

Figure 112. LE Client Resources

This screen will allow the specific settings to be modified for this node, and will not be represented globally.

7.2.3 Monitoring Node Resources

To view the resources of a node from the Router and Bridge Manager submap, double-click on the icon representing the node. The Node Details submap appears, displaying the resources associated with the node (see Figure 116 on page 167).

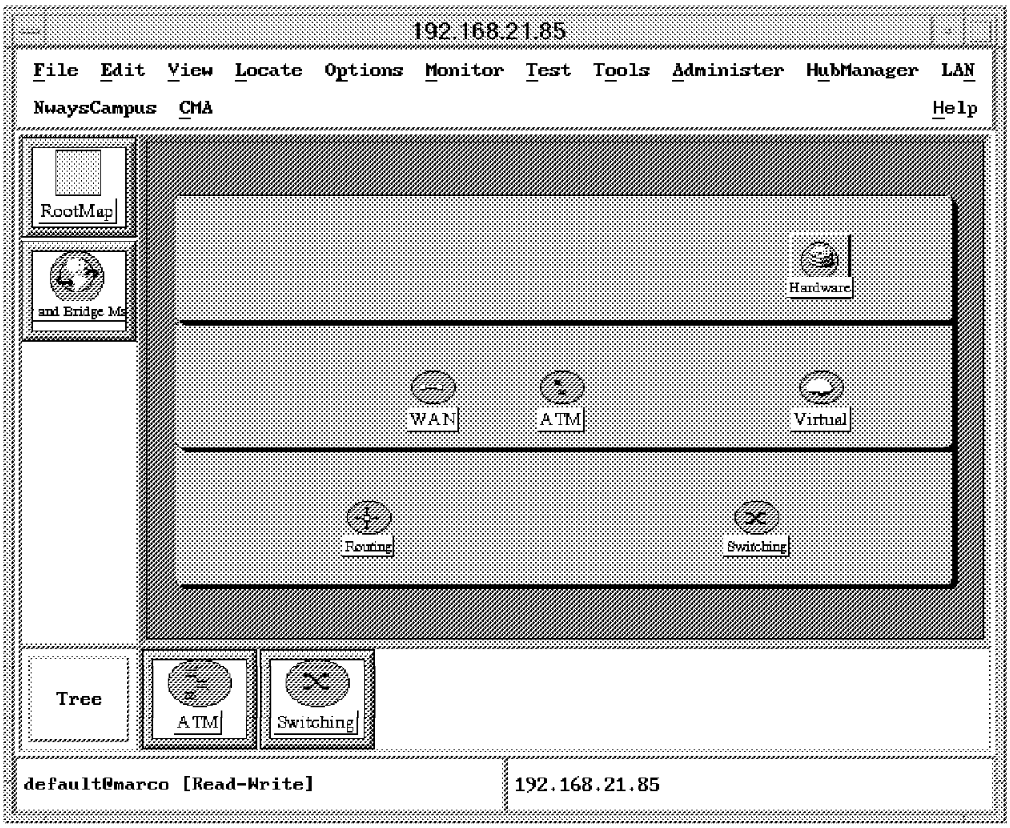

Figure 113. 8210 Managed Resources

The Node Details submap contains three layers. These are:

1. System resources (top row)
2. Interface resources (middle row)
3. Capabilities resources (bottom row)

These sections contain resource symbols that are executable.

If you double-click the resource symbol **Virtual**, Figure 114 on page 166 is displayed.

These icons will change color if any of the resources currently being monitored raise an alert or a threshold is exceeded.

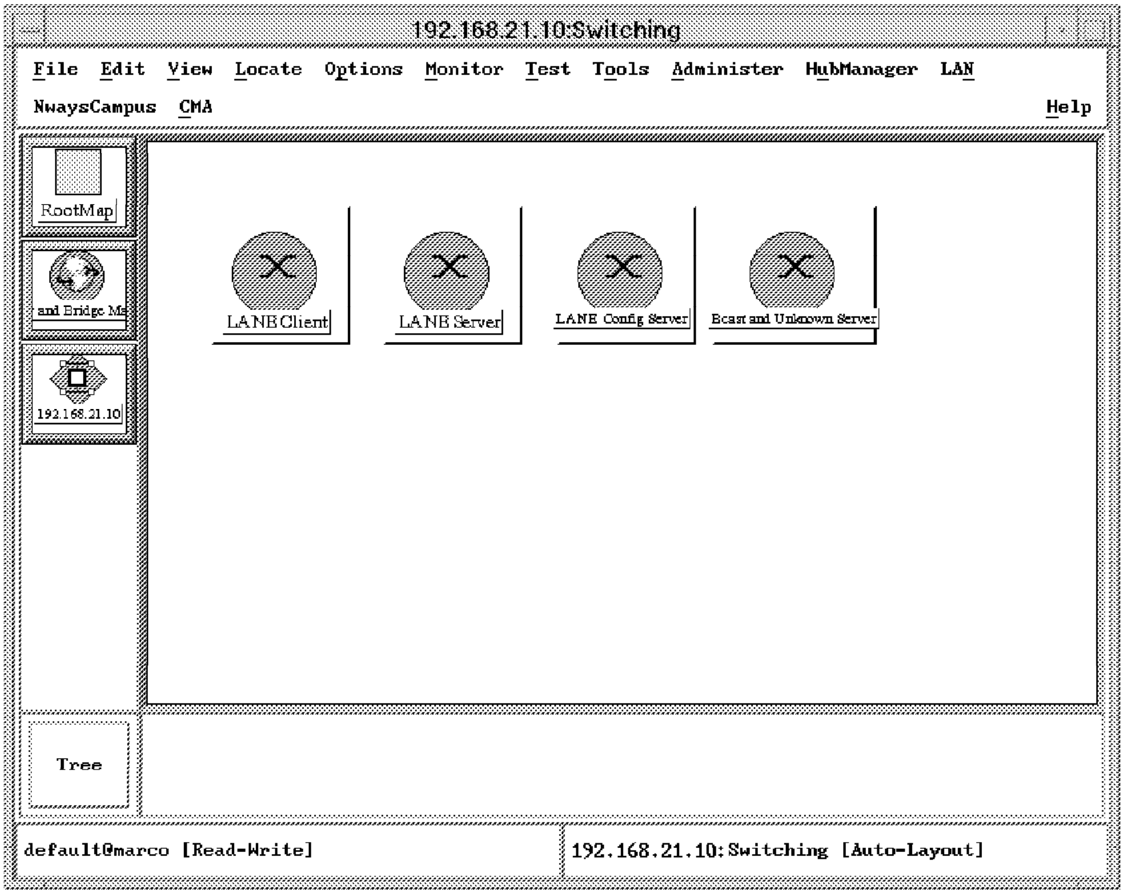

Figure 114. 8210 Switching Group Submap

7.3 Example of Using Router and Bridge Manager for an 8285

In this simple scenario we see what happens when a monitored resource, in this case an interface on the 8285 device, goes down.

To simulate this we disabled the 8285 interface 101. NetView then received the interface down trap (see Figure 115).

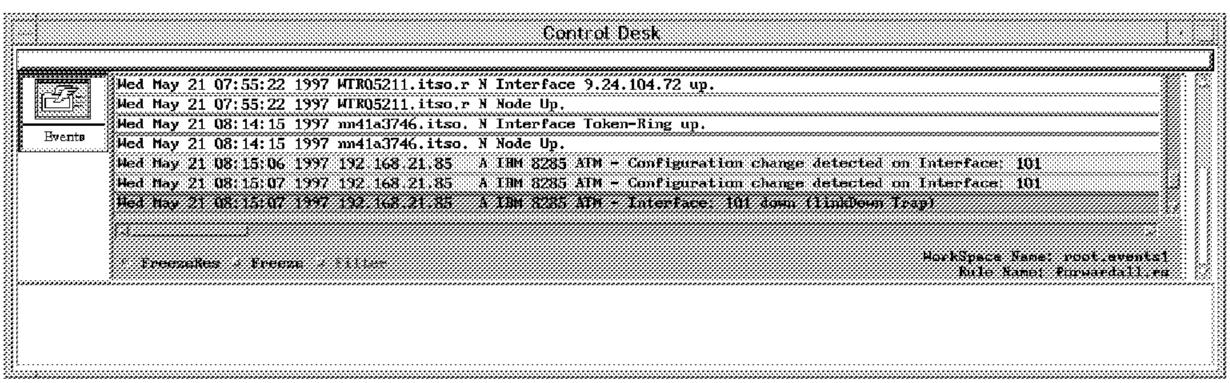

Figure 115. NetView for AIX Events Window

Due to the fact that this was one of the pre-defined monitored resources for the 8285, the icon representing this resource changed to red, signifying a problem condition.

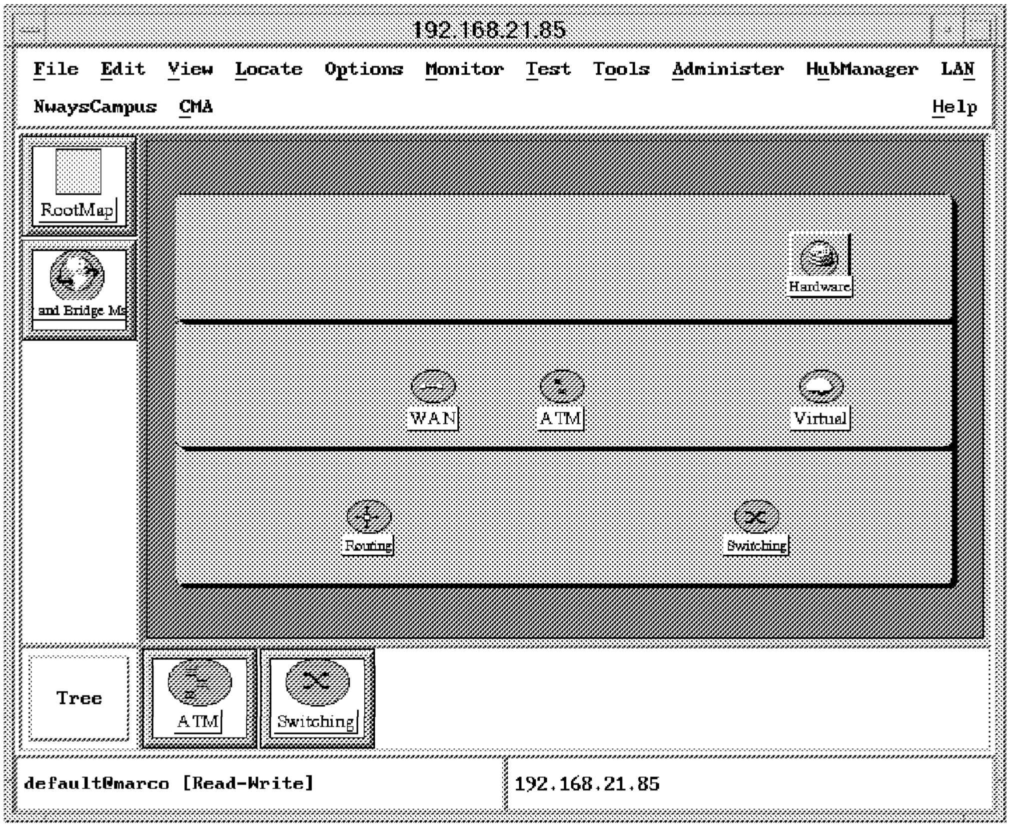

Figure 116. The 8285 Monitored Resources

By double-clicking on the 8285 interface icon Figure 117 on page 168 was displayed.

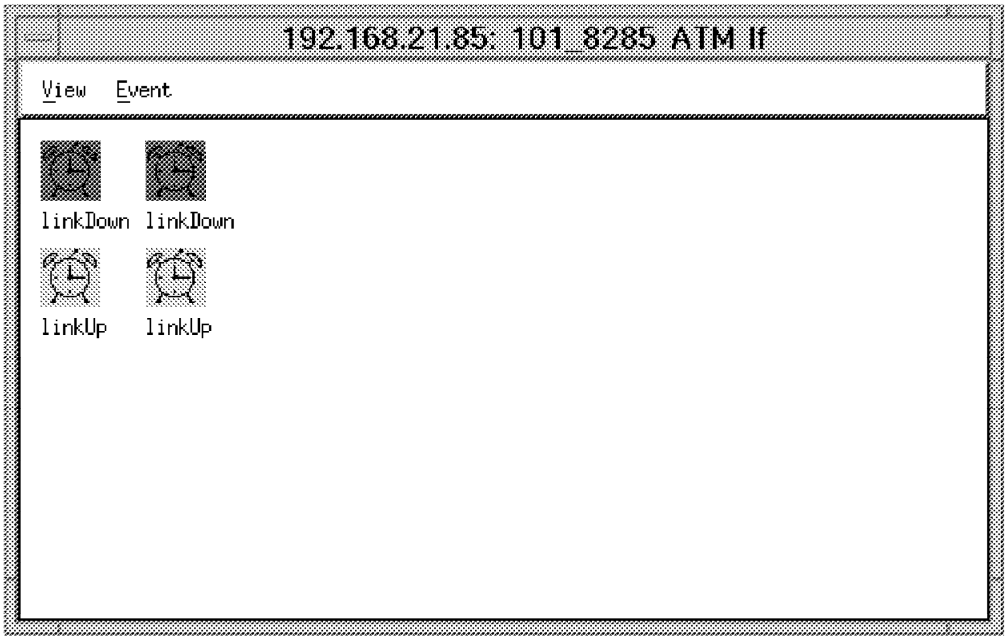

Figure 117. Displaying the Events

From the Event Container window, you can see all of the traps and thresholds received for this resource.

The associated description for this particular trap is shown in Figure 118.

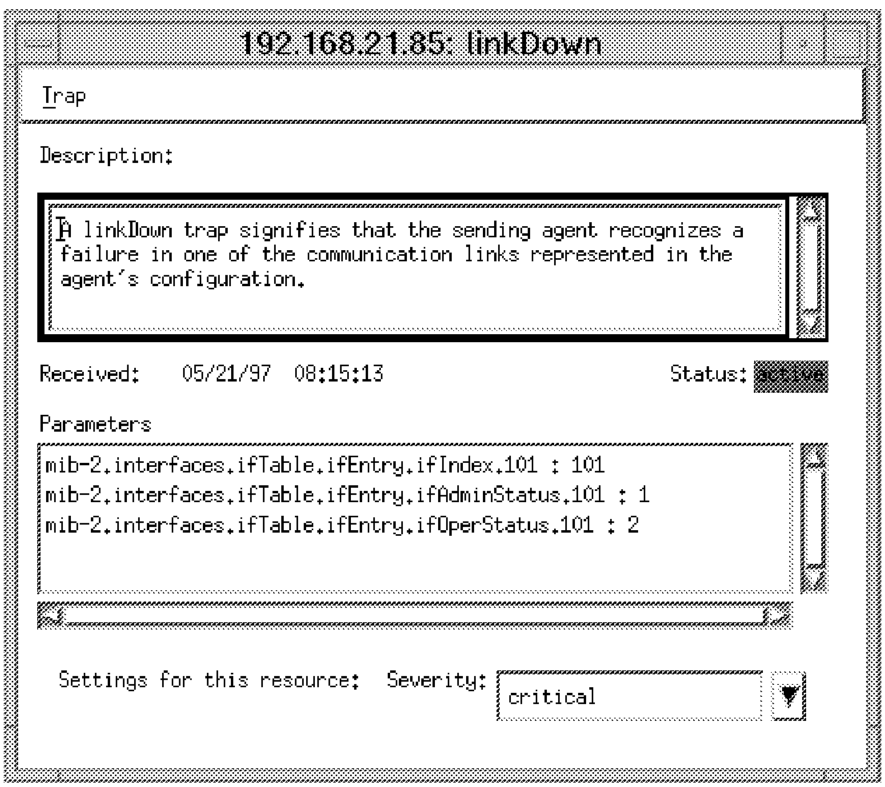

Figure 118. Displaying the Events

7.3.1 Analyzing Event Details

The Event Details window displays all of the data associated with the selected trap or threshold. From the Event Details window, you can acknowledge or clear the selected event. You can also save the details of an event to a report file for later analysis using the following procedure:

1. Select **Trap** for a trap event or **Threshold Event** for threshold event from the menu bar.
2. From the Trap or Threshold Event menu, select **Save to File**.

The event details are saved to a text file.

Router and Bridge Manager provides a graphing tool to analyze collected data. To graph threshold event data select the Figure 118 on page 168 event to show Figure 119 on page 170

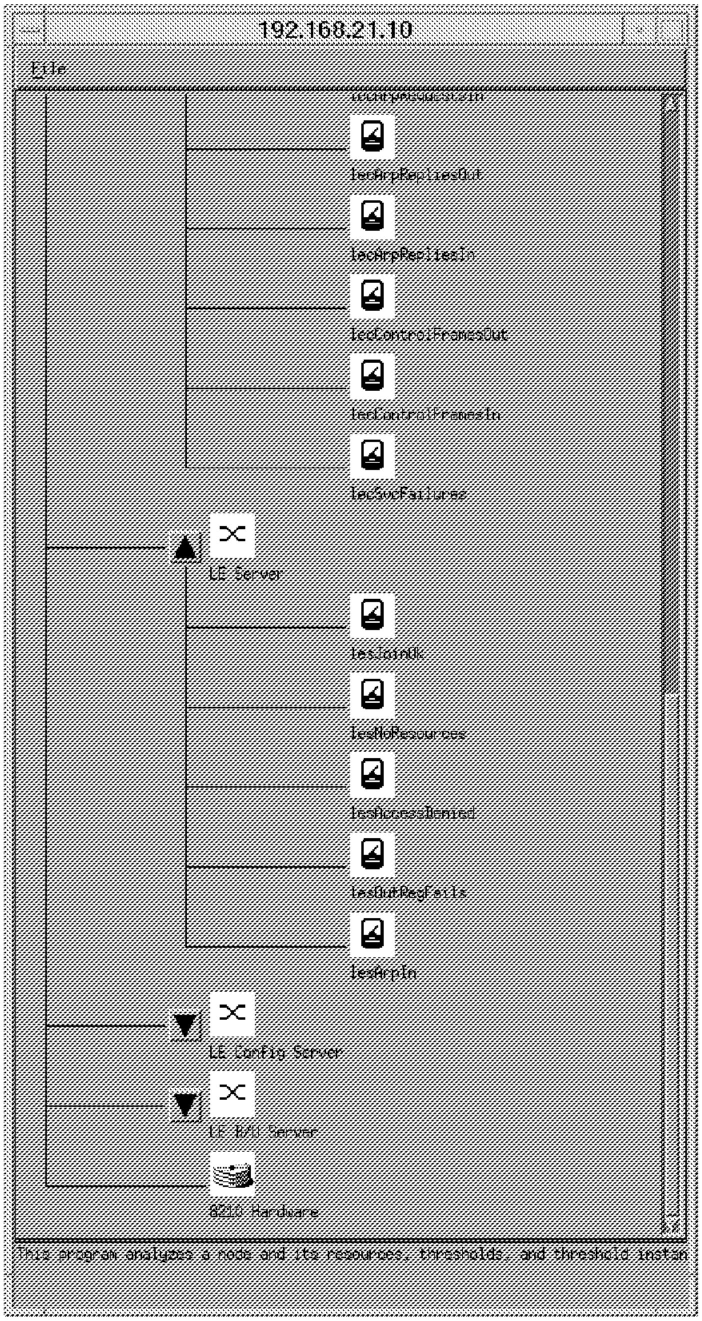

Figure 119. Analyze the Node Definition

From here you can view the all the defined resources for a particular device.

7.3.2 Check Router and Bridge Manager Daemon Status

Router and Bridge Manager Version 2 has two daemons:

- rabmEventServer
- NCMPserver

There are two ways to check the status of those daemons. This should be done whenever something does not work properly:

1. Using the Router and Bridge Manager menu:

- Select **Tools** from the NetView for AIX menu bar.
- Select **Router and Bridge Manager** from the Tools menu.
- Select **Manage Applications** from the Router and Bridge Manager menu.
- Select **Query Daemon Status** from the Manage Application menu.
  This will open a window that shows the actual daemon status.

2. Using the ovstatus NetView command, type:

   ```
   /usr/OV/bin/ovstatus rabmEventServer
   ```

   You can also type:

   ```
   /usr/OV/bin/ovstatus NCMPserver
   ```

   This will display the actual status of the daemons.

To stop the daemons use the following commands in sequence:

```
/usr/OV/bin/ovstop rabmEventServer
/usr/OV/bin/ovstop NCMPserver
```

This will stop the daemons one after the other.

To start the daemons use the following commands in sequence:

```
/usr/OV/bin/ovstart NCMPserver
/usr/OV/bin/ovstart rabmEventServer
```

This will start the daemons one after the other.

Sometimes it happens that the Router and Bridge Manager daemons loose synchronization with the NetView daemons. In this case all daemons (including NetView daemons) have to be stopped and restarted again. This can be done by issuing:

- `/usr/OV/bin/ovstop` - This will stop all daemons.
- `/usr/OV/bin/ovstart` - This will start all daemons.

7.3.3 Router and Bridge Manager Trace Files

The Router and Bridge Manager trace files are located in /usr/OV/log.

The file names are:

- rabmEventServer.trace
- rabm_client.trace
- rabm_grapher.trace
- rabm_seed.trace
- NCMPserver.trace

7.3.4 Router and Bridge Manager Main Directory

The main directory for the Router and Bridge Manager file is /usr/rabmv2.

7.3.5 Router and Bridge Manager Installation Log File

During Router and Bridge Manager installation, everything is logged to /tmp/RabmServer.log.

7.3.6 MLM Files

These following files contain MLM configuration information:

- /var/adm/smv2/log/smMlmCurrent.config
- /var/adm/smv2/log/midmand.log
- /var/adm/smv2/log/smtrap.log

The smMlmCurrent.config file reflects all data collection and threshold definitions done by Router and Bridge Manager or MLM. It also contains all MLM definitions such as the Trap Destination table and Alias table.

The midmand.log is the MLM log file. It logs nearly everything that happens to the MLM regarding problems, thresholds and traps.

The smtrap.log logs all SNMP traffic related to MLM.

7.4 Configuring MLM to Run with Router and Bridge Manager

This section briefly describes the Mid-Level Manager configuration.

For our purpose we only defined one MLM on the same machine as the Network Management software.

We update the /etc/snmpd.conf file with the community name used for the local MLM as shown in the following example to read the SNMP daemon:

```
community  public  0.0.0.0 0.0.0.0 readWrite
```

Refresh the SNMP daemon by issuing the following command:

```
refresh -s snmpd
```

To access the MLM configuration issue the command:

```
/usr/bin/smconfig
```

We disabled the trap reception on the local MLM so that the traps are not initially sent to the MLM agent. The MLM Trap Destination table is configured to forward MLM traps to the Network Management Station.

Add Agent to MLM Domain

By default, all devices in your network that are not assigned to a specific MLM domain will be managed by the local MLM. Therefore, this step is needed only when using distributed polling.

7.5 Managing Nodes with Router and Bridge Manager

In this brief example we show how to quickly get started with Router and Bridge Manager. We do the following steps:

- Add a node
- View and modify the settings of a node
- Change the settings of a node

Traps coming from the network and from MLM are sent to the NetView daemon. From here they will be forwarded to the Event window within the NetView Control Desk. As soon as Router and Bridge Manager has been installed it also looks for those traps. MLM-specific traps will be forwarded to the NCMPserver and all other traps will be forwarded to the rabmEventServer. These are traps such as node up and node down.

All network nodes that are defined as agents within the MLM domain will be polled for threshold and data collection values defined within the Router and Bridge Manager threshold entities. In case of a match, MLM (not the managed note itself) will send a trap to the NetView trapd, and from here it gets to the NCMP server.

Whenever something has been changed at the Router and Bridge Manager EUI, it will be communicated to the MLM.

7.5.1 Using MLM′s Threshold and Collection Table

This table can be used to check if the changes that have been made in the Router and Bridge Manager EUI are reflected to the MLM, because if this is not the case, the definition is not active regarding polling for a match. To get there do the following:

1. Select **Tools** from the NetView for AIX menu bar.
2. Select **Router and Bridge Manager** from the Tools menu.
3. Select **View MLM Details** from the Router and Bridge Manager menu.

This will open a window like Figure 120 on page 174.

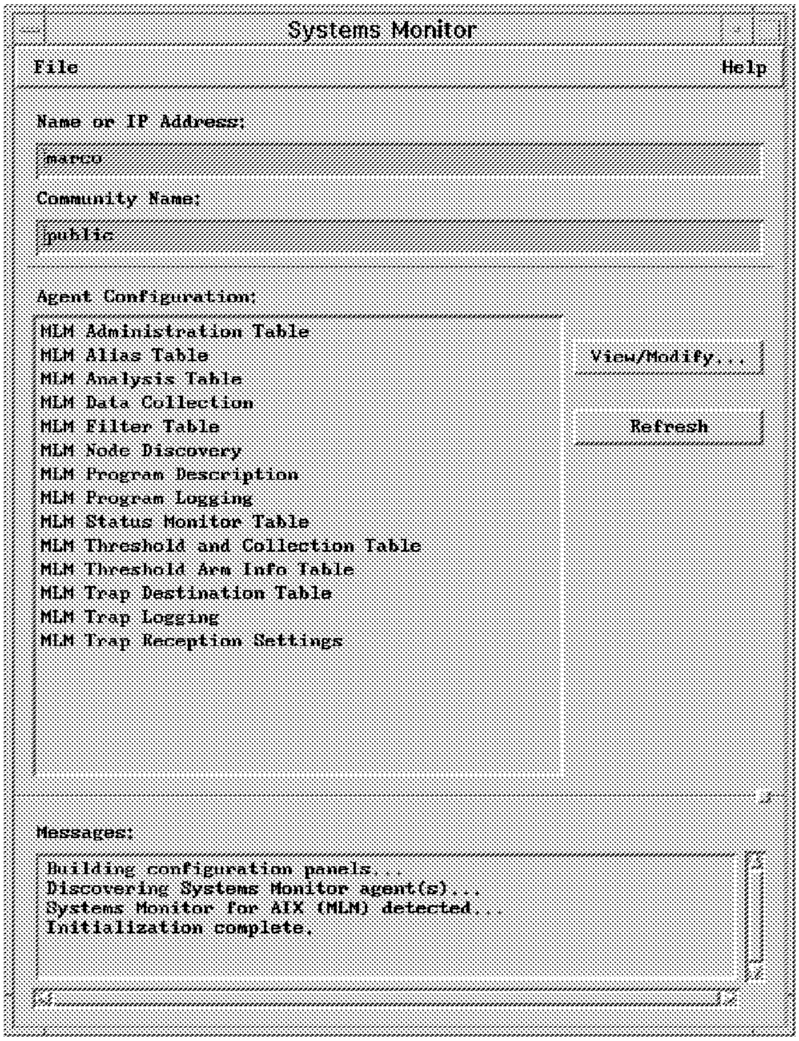

Figure 120. Systems Monitor Config Utility Window

At this point a read community test can be done by typing in a certain community name and refreshing the panel. If the community name used has no read authority, the table remains empty and an error message will occur. The most important tables regarding Router and Bridge Manager are:

- MLM Alias table
- MLM Threshold and Collection table
- MLM Trap Destination table

These tables are updated by the Router and Bridge Manager software. The MLM Threshold and Collection table is most often used. This table contains all data defined for a threshold.

To check the settings for a threshold and if the threshold is active, use the MLM Threshold and Collection table, because the MLM is the active polling device not Router and Bridge Manager.

The MLM Threshold and Collection table is the only place where you can change the traps that will be sent regarding the arm and rearm threshold values.

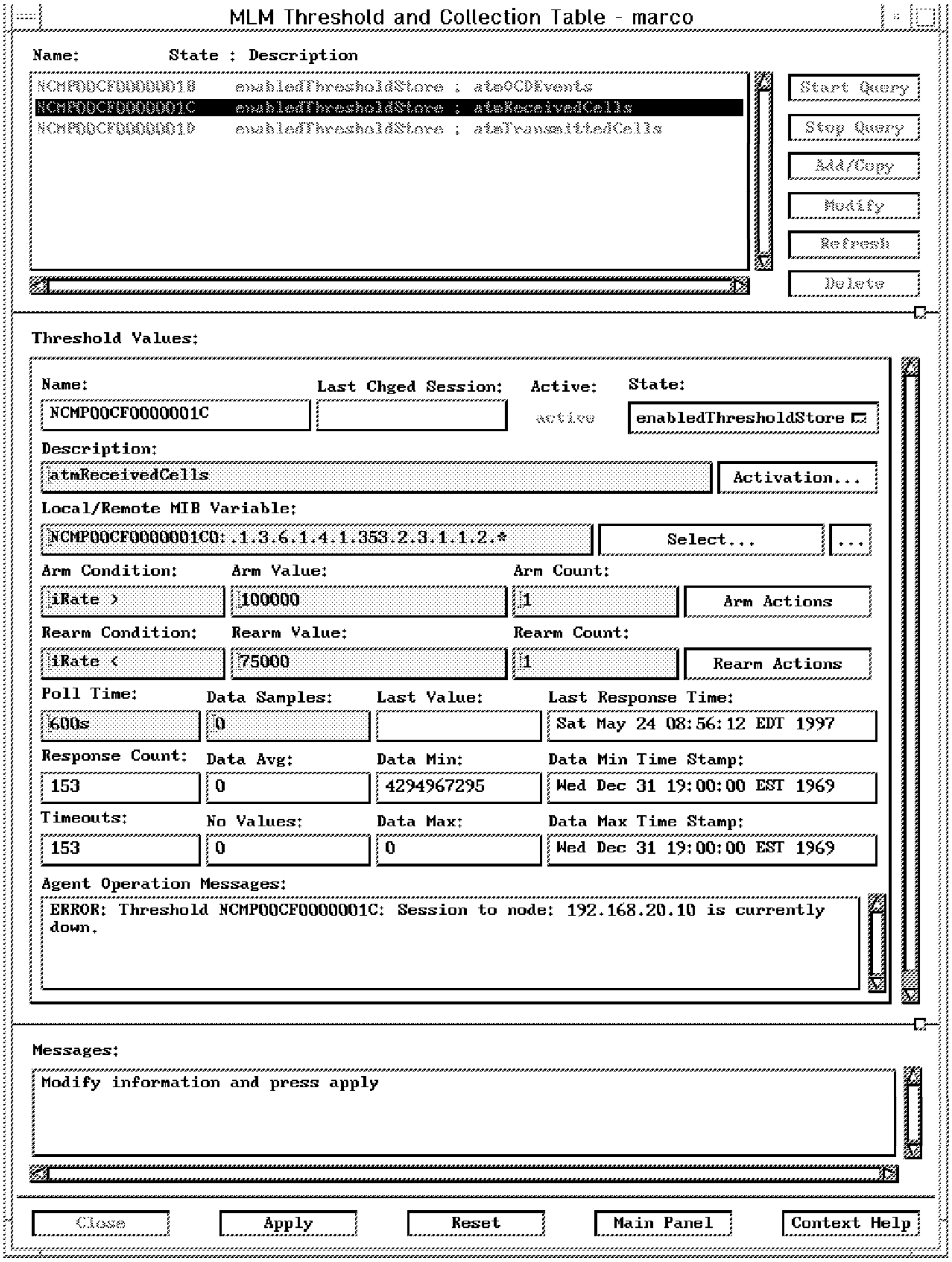

Figure 121. Systems Monitor Threshold and Collection Table

Note: Making changes regarding the threshold values within the MLM Threshold and Collection table will not be reflected to the Router and Bridge Manager threshold definition windows. Doing this will change the threshold policy but you don't see it from the Router and Bridge Manager windows. The only useful change may be changing the arm and rearm action, which are responsible for the traps sent when the threshold value is reached. This is different because this cannot be changed from Router and Bridge Manager definition windows. To get to the MLM Threshold and Collection table double-click the line on this option in the Systems Monitor window. This will open a panel as shown in Figure 121. On the top of this panel there is a list of threshold names. All thresholds beginning with NCMP belong to Router and Bridge Manager.

Selecting one of these thresholds and clicking on **Start Query** or **Modify** will fill out the mask in the middle of the panel with the actually defined threshold values.

The Threshold Name is a symbolic name automatically defined by Router and Bridge Manager. These names are referenced to an IP address. The reference can be shown in the MLM Alias table. To display this table, double-click on the MLM Alias table line within the Systems Monitor window. This symbolic name may refer to more than one IP address.

This shows the current polled MIB value for the given MIB variable after selecting the **Start Query** button. This allows you to compare the threshold settings against the actually polled values. Since this version of Router and Bridge Manager does not have the Interface at a Glance function, this table can be used to balance the settings.

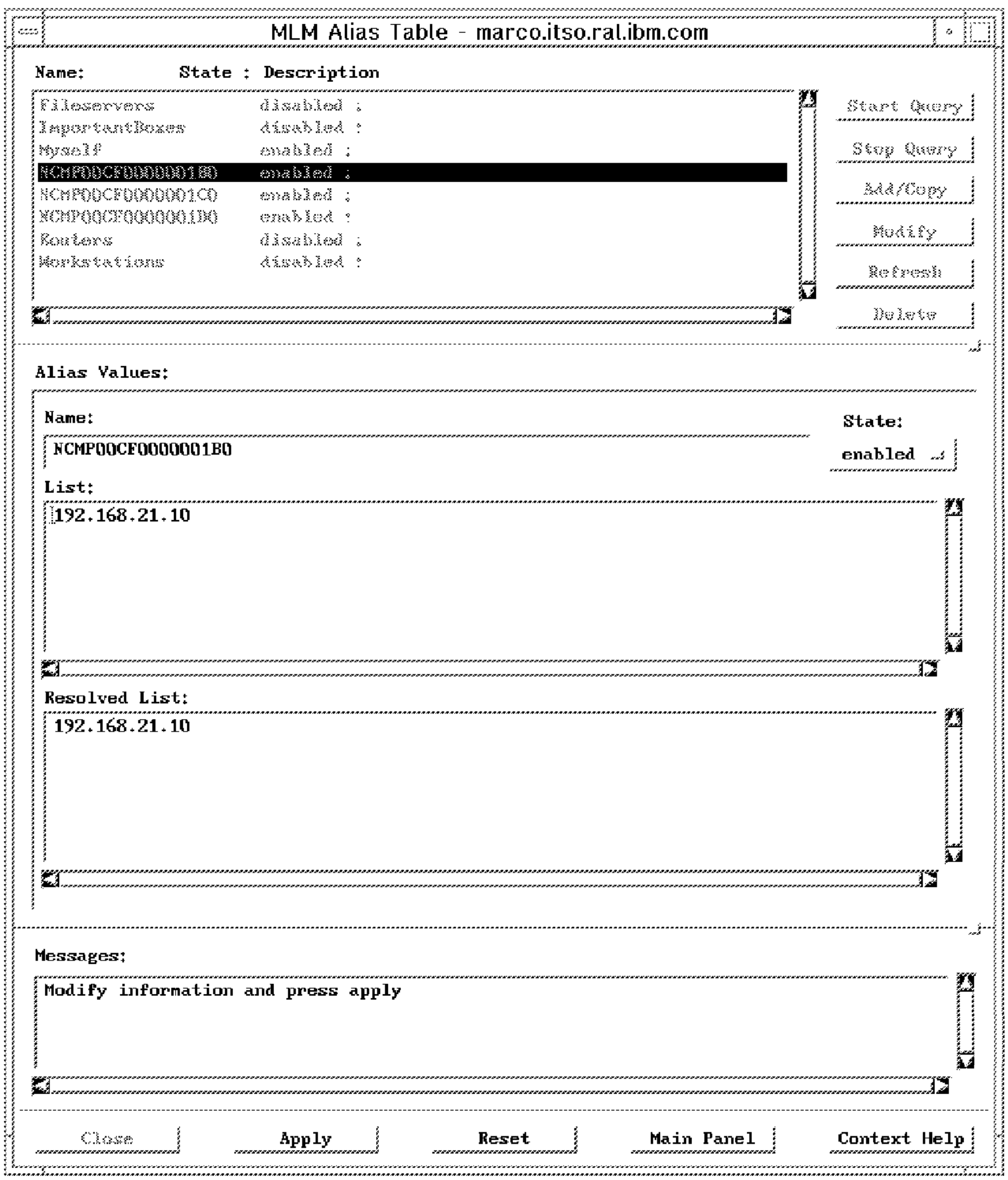

Figure 122. System Monitor Alias Table

Figure 122 shows the alias definition created by RABM.

7.6 The Poller Debug Tool

The Poller is a debug tool for trace and debug purposes only. It can be used to retrieve internal information for problem tracking.

Note: This tool is an unsupported function.

To start the Poller issue the command:

```
/usr/rabmv2/bin/poller &
```

You will see a window similar to Figure 124 on page 178. Click on the highlighted **Connect** button and a window like Figure 123 will appear.

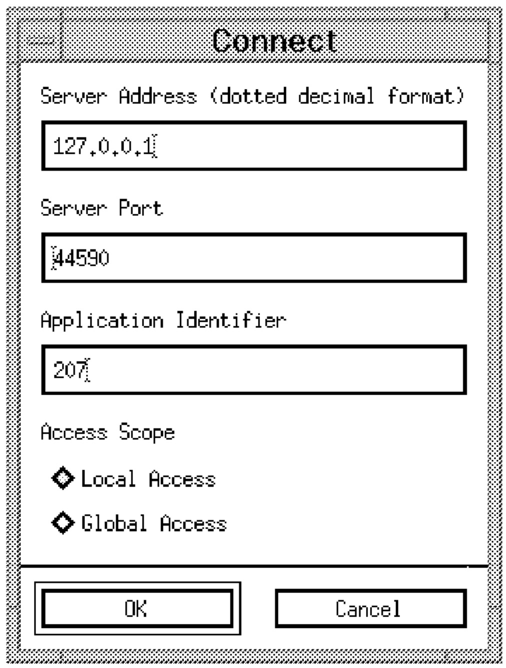

Figure 123. Router and Bridge Manager Poller Connection Window

At this panel type in the address of the machine were the Router and Bridge Manager you are looking for is located. The server port number is 44590. In the Application Identifier field, type 207. Access Scope Local Access should be used, because Global Access is for future use. Clicking on **OK** at this point gets you the next picture.

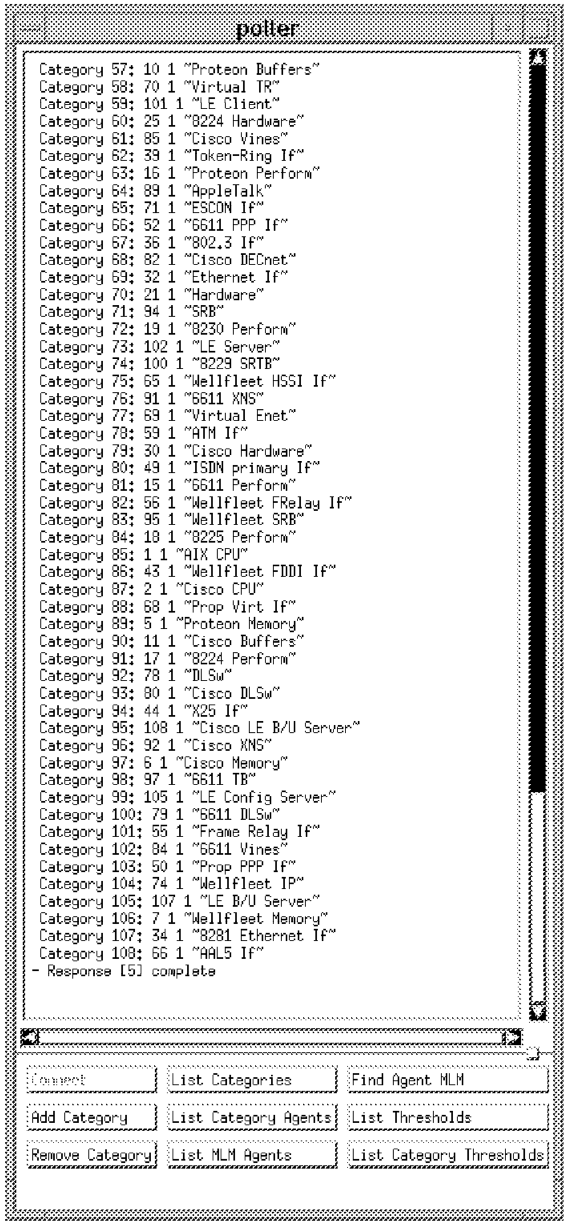

Figure 124. Router and Bridge Manager Poller Window

The Poller program is able to retrieve date from the Object Store database. When some of the Poller windows require an application ID, the value is 207.

Here are a few functions that can be performed using this tool:

List Categories Categories in this case is a synonym for resources. That means clicking on the List Categories button shows a list of all currently defined resources in the Poller window.

List Category Agents This lists all agents other than the local machine dealing with this category. List MLM Agents lists all agents explicitly defined to a given MLM. This can also be done using the SMIT menu.

Find Agent MLM This is used to find the related MLM for a given agent, by typing the agent address into a window popping up when this button is being selected.

List Thresholds This lists all defined thresholds within the Poller window such as the listed categories. This is important to get a threshold ID for further investigations on a certain threshold.

Query Threshold This displays all collected values for a given threshold by typing in the threshold ID after the window has popped up. This function displays information similar to the List Category Thresholds.

Add/Update and Remove Threshold This edits the thresholds regarding all values you can define to a threshold as you can also do from the Threshold Definition window or from the Threshold and Collection table within MLM.

We used this tool to verify our Router and Bridge Manager configuration and to view the total amount of thresholds that we had defined.

Chapter 8. LAN Emulation Performance

This chapter shows what performance information we can see using Nways Campus Manager LAN application using examples. Here we are primarily concerned with the LAN Emulation components.

Existing monitoring of ATM resources is extended to gather information on the amount of resources dedicated to LAN Emulation to help distribute the load between hardware devices and to anticipate the need for additional resources.

LAN Emulation traffic is monitored to assist in deciding how to distribute and define the ELAN entities and to anticipate the need for network re-design.

Note: The statistical information is retrieved directly from the devices using the LAN Emulation MIBs.

8.1 ATM Connections and Traffic

A good place to start with performance is to look at the overall ATM traffic. This will give you an idea of the ATM devices performing.

To start the ATM monitor application do the following from the cluster submap:

1. Click on the device using the right-hand mouse button. (In our case we chose the CPSW module.)
2. Select **CMA->Monitor** from the pull-down menu shown in Figure 125 on page 182.

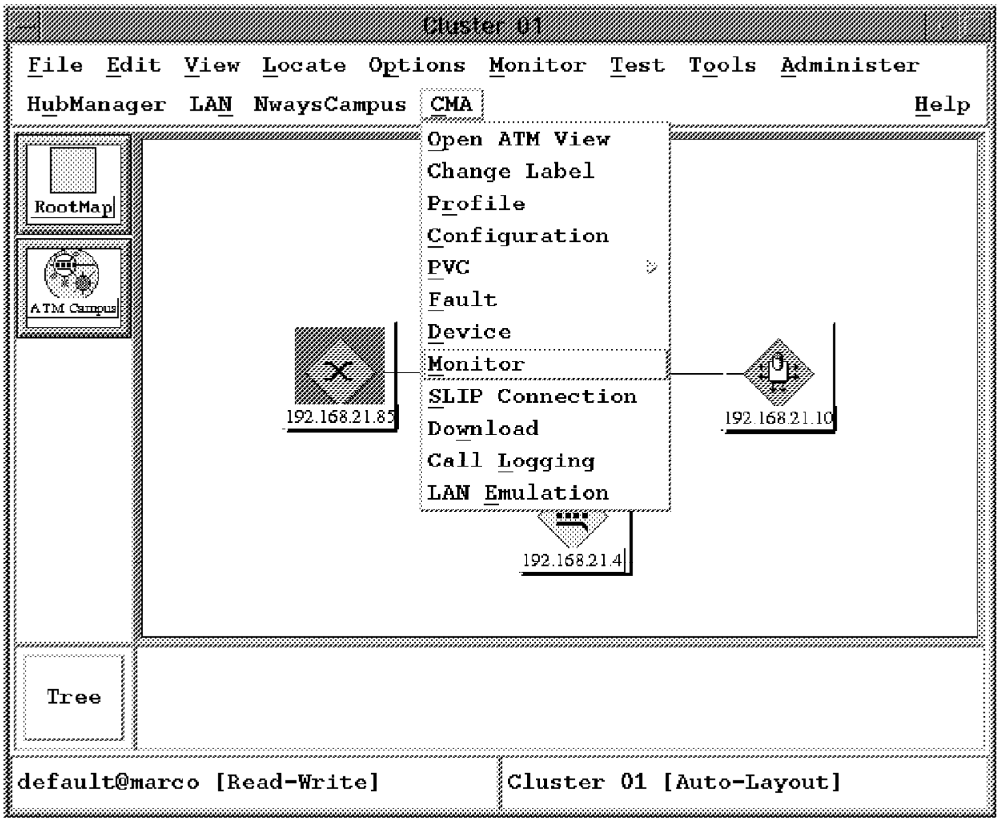

Figure 125. Starting the Monitor Application

Figure 126 on page 183 will appear showing the top five ports for the switch, displaying traffic information, such as kbps.

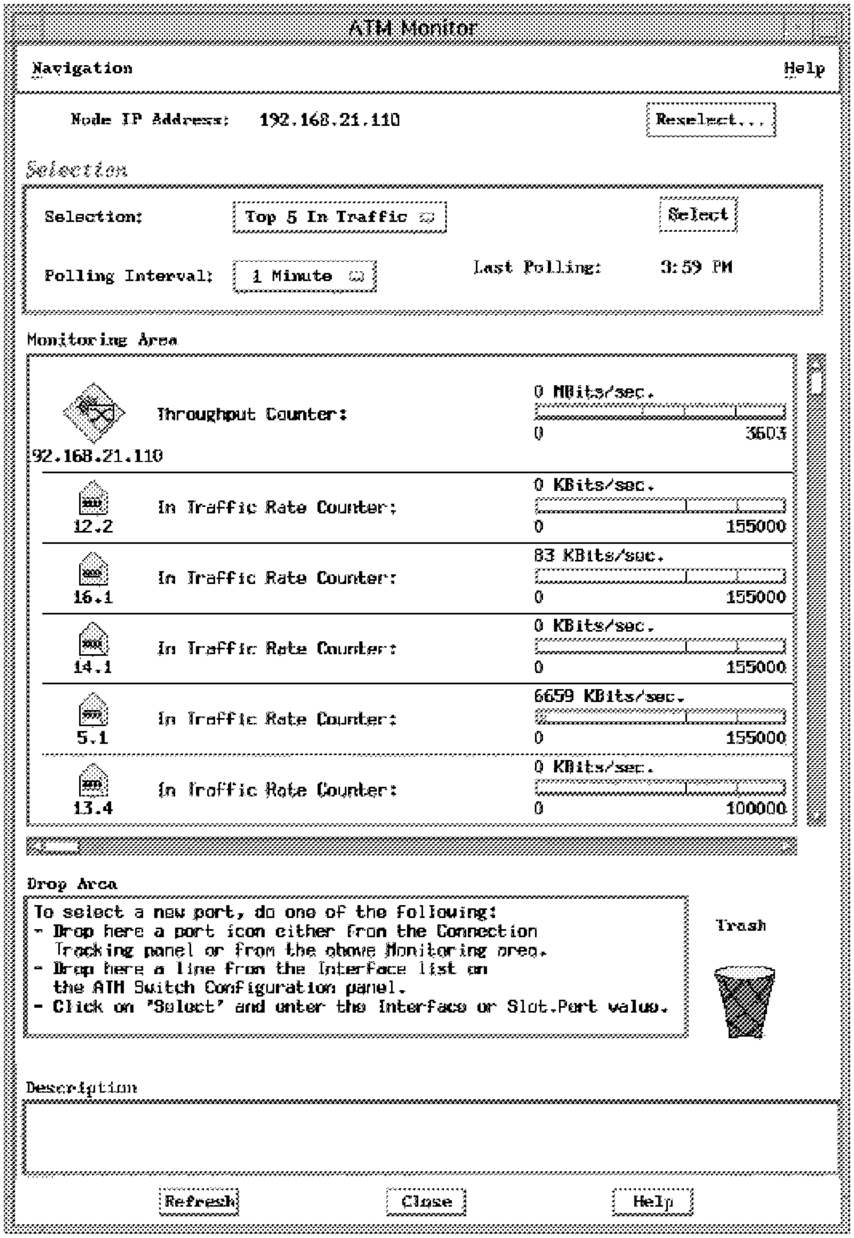

Figure 126. ATM Monitoring

The ATM ports are listed on the left of the screen. These actual port connections can be resolved by starting the ATM view. Here you can correlate the port to the specific device. For instance the the port 16.1 can be seen in Figure 127 on page 184 as 1601. This is the connection from the CPSW to the IBM 8210.

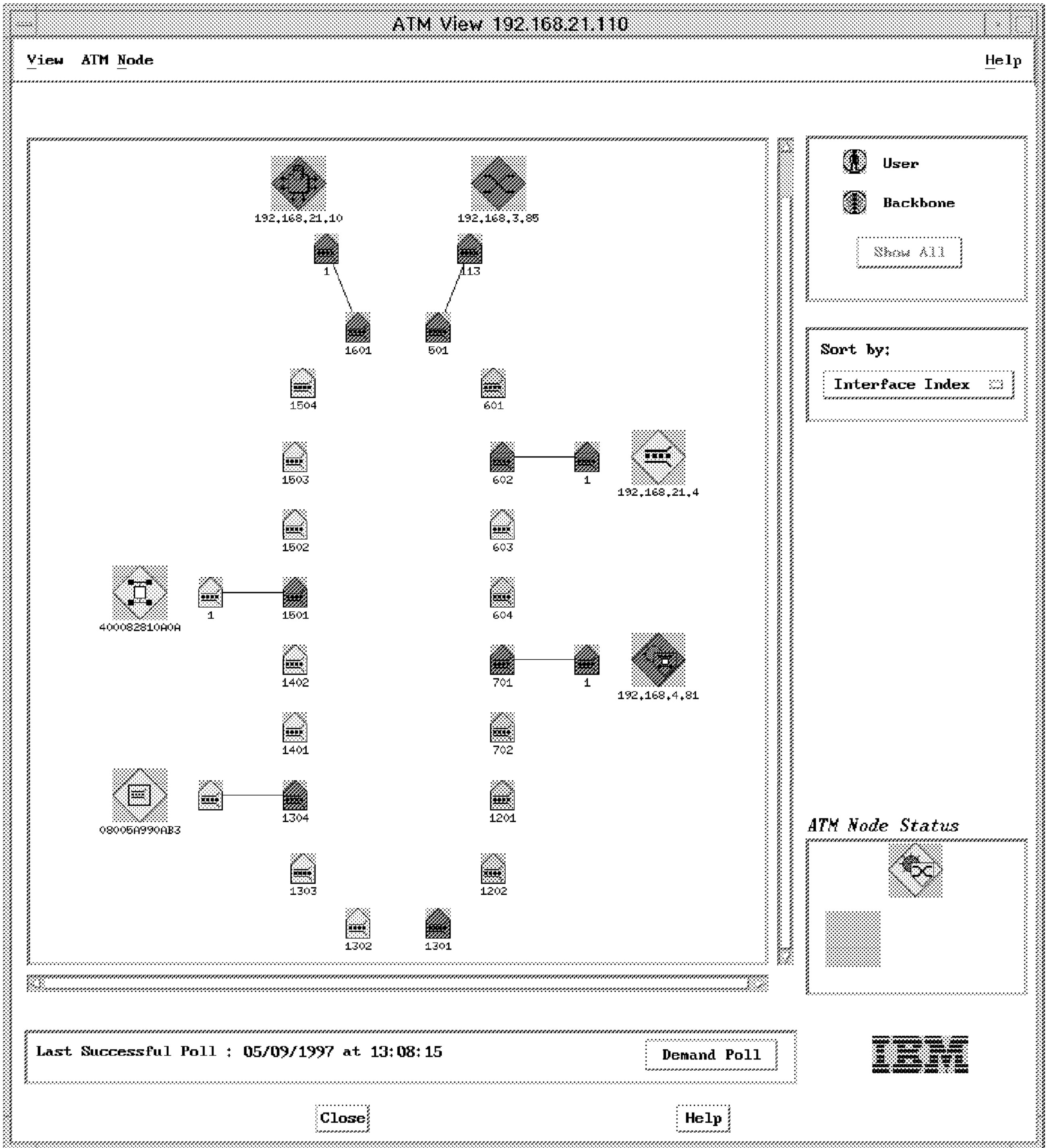

Figure 127. Locating the Specific ATM Ports

Figure 20 on page 42 is where you can view the specific network connection. We can see that port 16.1 is depicted as 1601 here.

We could not show any real performance-related problems due to the size of our ATM network.

The next section takes a look at the what performance statistics can be retrieved for our LAN emulation entities.

8.2 LAN Emulation Performance

The LAN Emulation statistics are shown by the performance application dynamically retrieving the data using the LAN Emulation MIBs. Here we show a few examples of what information can be shown, stored or graphed.

The types of performance-related data we can monitor are:

- Performance of the traffic load
- Performance of the MAC layer, where we can view an emulated LAN as providing a connectionless packet delivery service
- Performance of LUNI traffic, for example, LE_ARPs frames
- Performance of individual circuits within an emulated LAN
- Performance management of the ATM switched network over which an emulated LAN runs

The LECs provide an interface to higher level protocols such as IP, IPX and NetBIOS. The first category of performance management is the most important one as it focuses mainly on the total traffic load it services to higher protocol layers.

LAN Emulation performance management retrieves statistics from both LAN Emulation servers and LAN Emulation clients. LAN Emulation performance management detects abnormal conditions and performance deterioration in order to provide information to assist in fault-finding and loss in quality of service for the following:

- Traffic and network load generated
- Errors detected
- Main contributors (Top-N contributors)
- Monitoring resources

8.3 The Performance Application

The statistics application is started from the LAN emulation screen. Next you must select the required LANE entity. Here we chose the LES for the ELAN TR_ELAN_8210_2.

Using the right-hand mouse button select **Statistics** from the context menu (see Figure 129 on page 187).

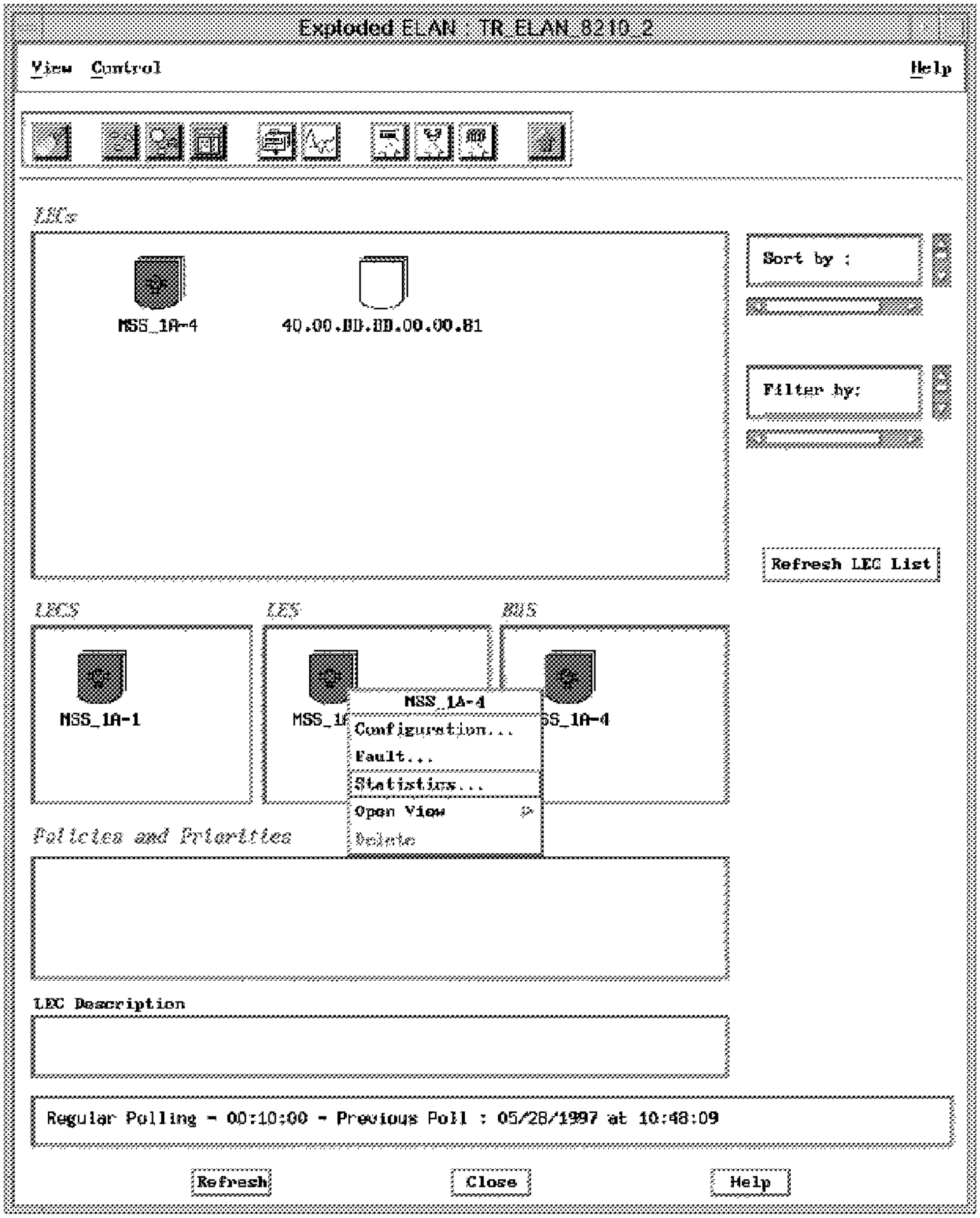

Figure 128. Starting the Statistics Application

We selected **LES Device Configuration Errors** from the category menu, then clicked on **OK** to display Figure 130 on page 187.

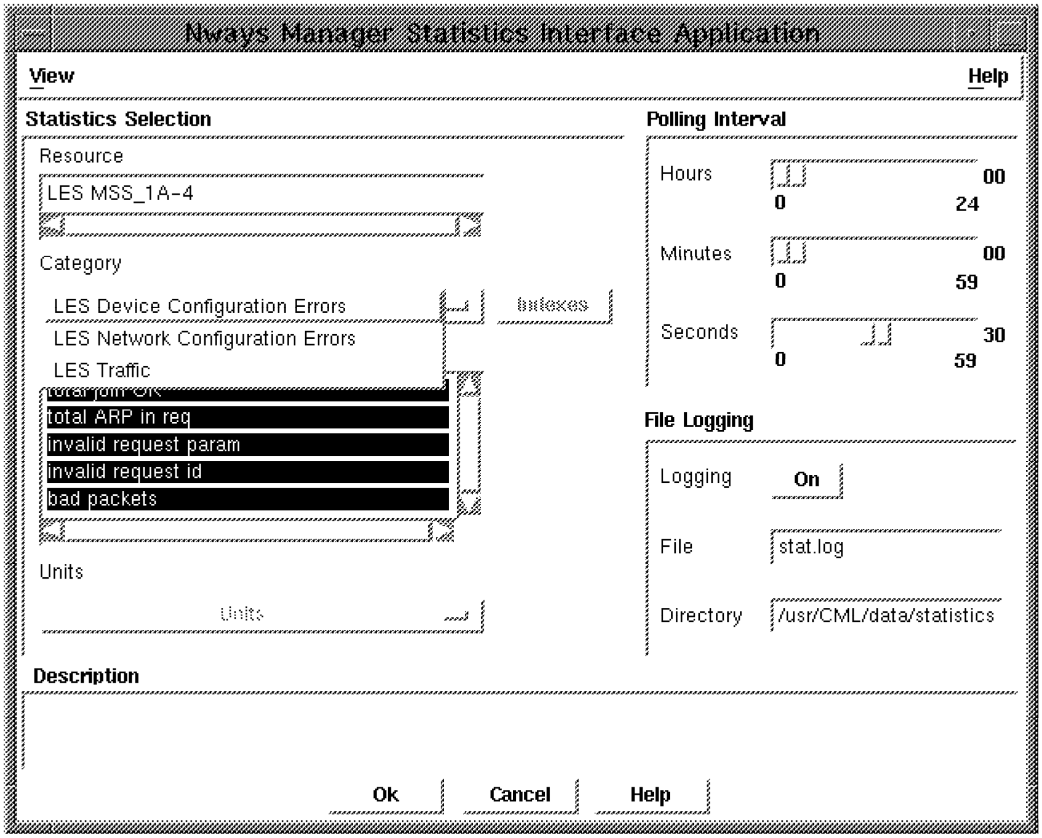

Figure 129. LES Performance Data

The data can be collected into a file by entering the file name in the File Logging field.

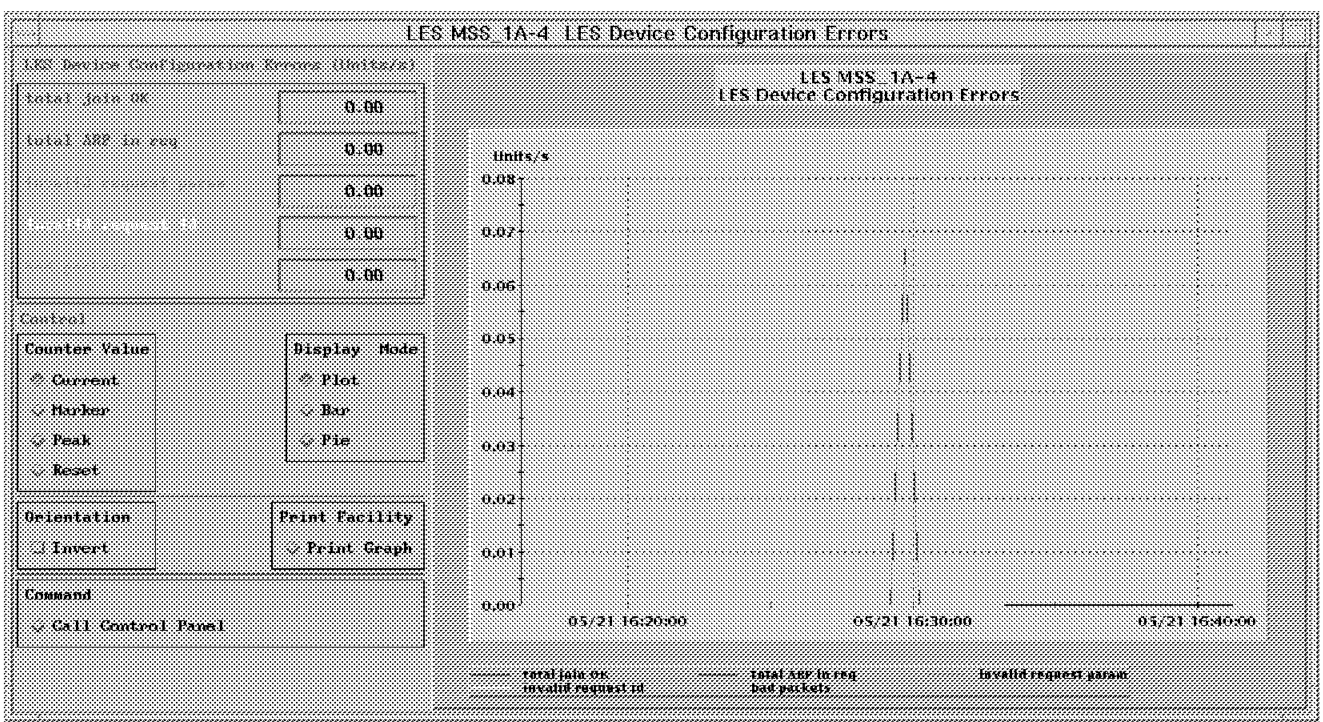

Figure 130. The LES Device Configuration Errors

The values shown in Figure 130 are:

- The total number of join OK. This is the number of LE_JOIN responses sent out by the LES instance.
- The total ARP in-req. This is the total number of LE_ARP_REQUEST frames the LES instance has accepted since its last initialization.
- The total number of ARP-forward requests. This the total number of LE_ARP_REQUESTs that the LES instance has forwarded onto the LECs (either via the control distribute VCC or individually over each control direct VCC) rather than answering directly. This may be due to forward all requests or because the resolution to the request did not reside in the LES′s ARP cache.
- The total number of LE_ARP_REQUESTs rejected due to a lack of resources on the LES devices.
- The number of access denieds for security reasons.

8.3.1 BUS Network and Traffic Load

To view the BUS traffic select the BUS from the Figure 128 on page 186. This time you will see different selection criteria specific for the BUS.

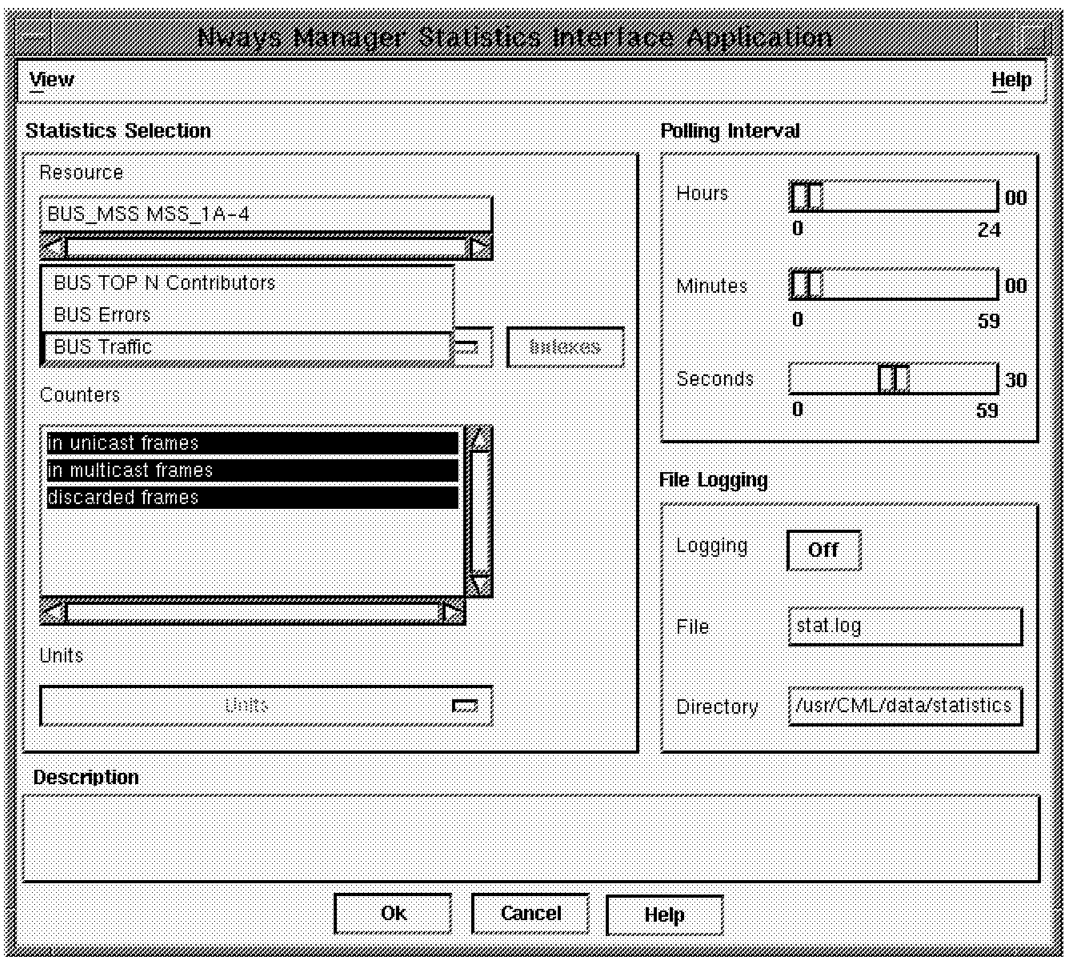

Figure 131. BUS Traffic

Click on **Ok** to start the data retrieval. This will show Figure 132 on page 189.

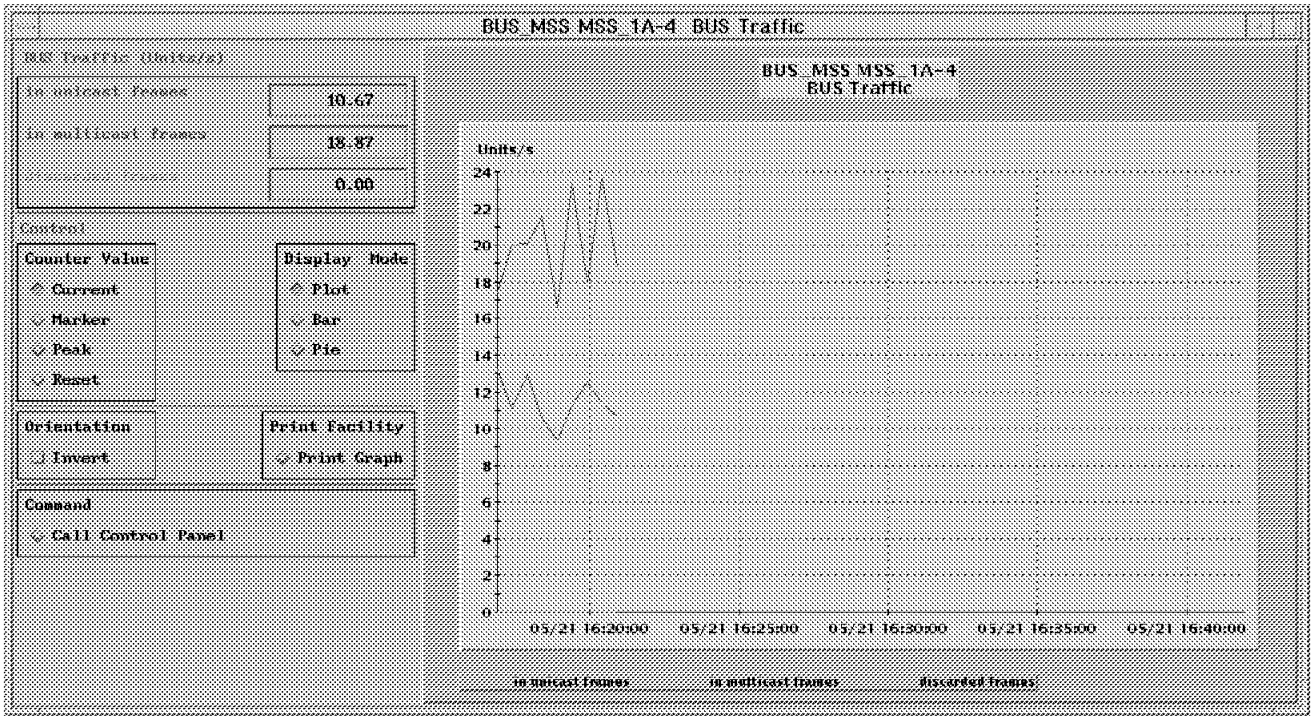

Figure 132. BUS Traffic Statistics

Three counters are available for traffic and network loads. These are:

1. The total number in unicast frames. This is the number of frames that the BUS has received that were unicast data frames (destination MAC address not set to FFFFFFFFFFFF or to any functional MAC address) and all control frames (LE_FLUSH_REQUESTs).
2. The total number of multicast frames. This is the number of frames the BUS has received that were multicast frames (either set to FFFFFFFFFFFF for IP_ARP or functional MAC addresses such as 802.1d spanning tree).
3. The total number of discarded frames. It's the number of frames discarded due to a resource error.

8.3.2 BCM Network and Traffic Load

BCM traffic information:

1. The total number of frames received. This is the number of frames received by BCM for all protocols (IP, IPX, NetBIOS).
2. The total number of frames returned. This is the total number of frames, for all protocols not managed by BCM and returned to BUS for transmission.
3. The total number of frames discarded. This is the total number of frames discarded (filtered) by BCM for all protocols (IP, IPX, NetBIOS).
4. The total number of frames transmitted. This is the total number of frames transmitted by BCM for all protocols.

8.3.3 LEC Network and Traffic Load

The information we can retrieve for the LEC network and traffic is as follows. As the LEC instance is presented in MIB-II as an interface, it makes sense to retrieve statistics for a given LEC instance, from the MIB-II branch of its SNMP agent. MIB-II interface statistics deal with data traffic sent from/to MAC layer (here LAN Emulation) and higher layers (IP, IPX, NetBIOS). The traffic selection screen is shown in Figure 133.

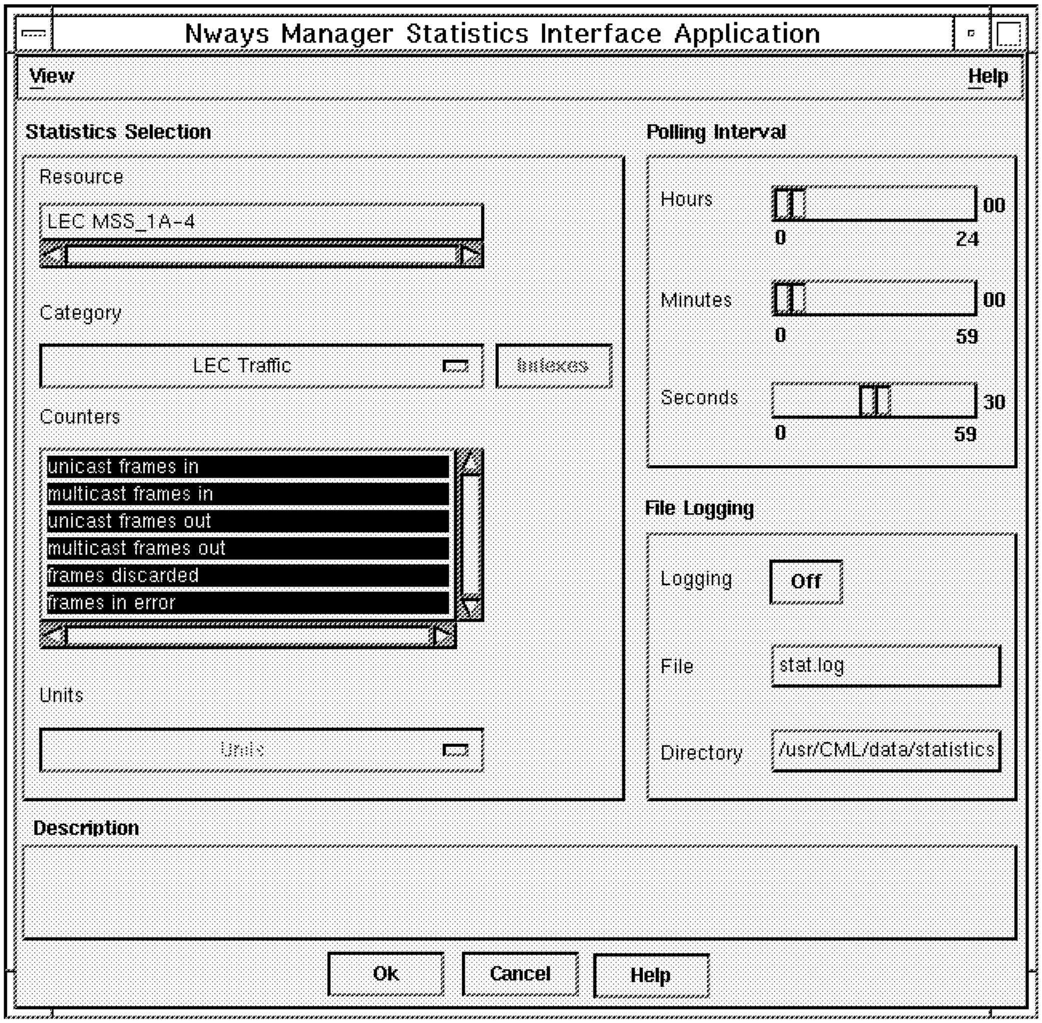

Figure 133. LEC Traffic Information

1. The total number of unicast frames in. This is the number of data packets delivered by this LEC instance to a higher (sub)layer that were not addressed to a multicast or broadcast LAN destination.

2. The total number of multicast frames in. This is the number of packets delivered by the LAN Emulation layer to a higher (sub)layer, which were addressed to a multicast or broadcast address at the LAN Emulation layer.

3. The total number of unicast frames out. This is the number of data packets that higher level protocols requested to be transmitted, which were not addressed to a multicast or broadcast address at the LAN Emulation layer, including those that were discarded

4. The total number of multicast frames out. This is the number of packets, that higher level protocols (IP, IPX, NetBIOS) requested to be transmitted, and which were addressed to a multicast or broadcast address at the LAN Emulation layer, including those that were discarded or not sent.
5. The total number of frames discarded. This is the total number of inbound and outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted from higher layers of protocols or their being deliverable to higher layers of protocols. One possible reason for discarding such a packet could be to free up buffer space.

8.3.4 Error Monitoring

LAN Emulation errors are monitored to identify and analyze faults due to hardware resources, configuration or user actions. Error monitoring provides a graphical display similar to the traffic and network load monitoring.

8.3.5 LECS Errors Monitoring

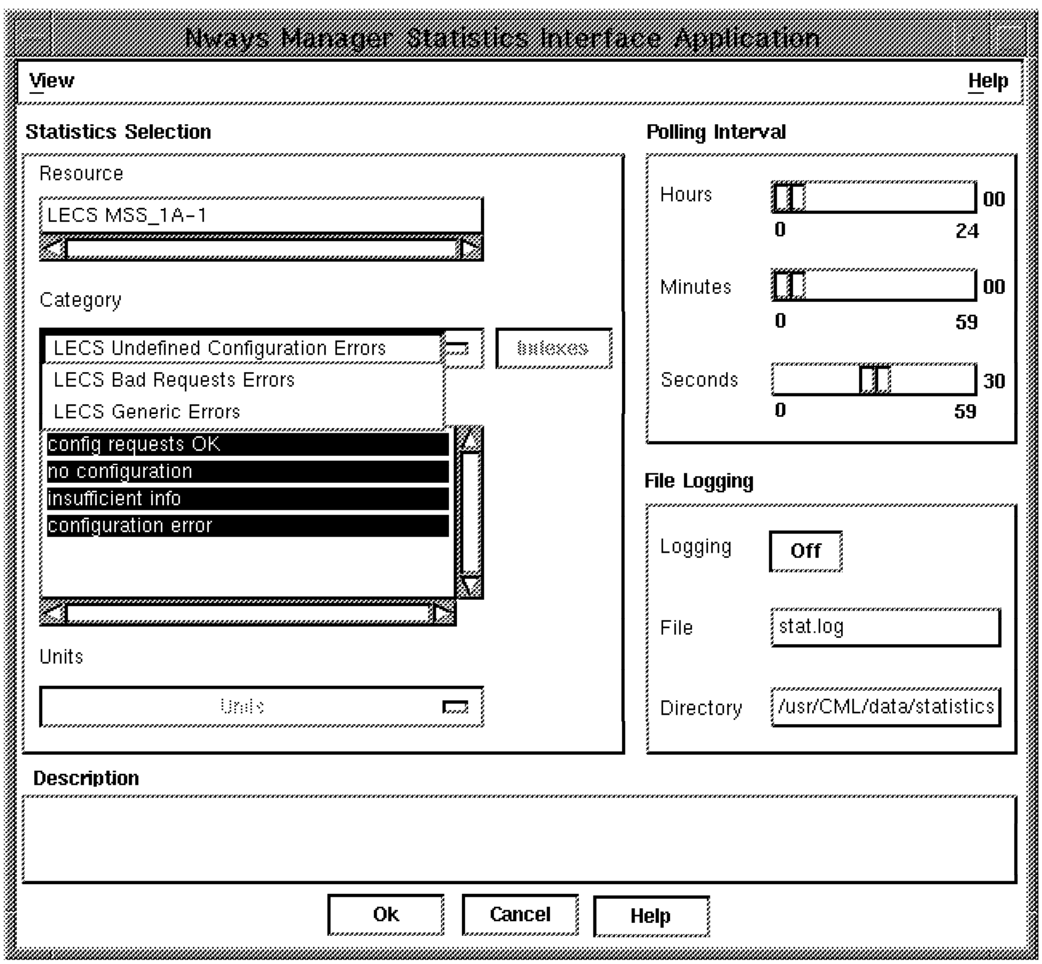

Figure 134. LECS Error Monitoring

The values for LECS error monitoring are:

- The Undefined Configuration category:

1. The total number of LE_CONFIGURE_REQUESTs successfully granted since the LECS agent was last initialized.
2. The total number of LE_CONFIGURE_REQUESTs rejected due to the LEC not recognized error.
3. The total number of LE_CONFIGURE_REQUESTs rejected due to the Insufficient information error.
4. The total number of LE_CONFIGURE_REQUESTs rejected due to the LE_CONFIGURE_ error.

- The Bad Requests category:

1. The total number of LE_CONFIGURE_REQUESTs successfully granted since the LECS agent was last initialized.
2. The total number of malformed LE_CONFIGURE_REQUESTs dropped by the LECS instance.
3. The total number of LE_CONFIGURE_REQUESTs rejected due to invalid parameters.
4. The total number of LE_CONFIGURE_REQUESTs rejected due to invalid requester LECID.
5. The total number of LE_CONFIGURE_REQUESTs rejected due to an invalid destination error.
6. The total number of LE_CONFIGURE_REQUESTs rejected due to an invalid ATM address.

- The Generic Errors category:

1. The total number of LE_CONFIGURE_REQUESTs successfully granted since the LECS agent was last initialized.
2. The total number of LE_CONFIGURE_REQUESTs rejected due to insufficient resources to grant.
3. The total number of LE_CONFIGURE_REQUESTs rejected due to a denied access.

8.3.6 LES Errors Monitoring

These counters are:

- The Network Configuration errors category refers to problems occurring due to a bad configuration of LECs LAN Emulation network parameters (ATM address, MAC address). To assess the relative importance of network configuration errors, some traffic and network load counters are applicable in this error category. The following counters can be found:

1. The total number of successful LE_JOIN_RESPONSESs sent out by the LES.
2. The total number of LE_ARP_REQUESTs the LES has accepted since its last initialization.
3. The total number of duplicate LAN destination errors experienced by this LES instance since initialization. A LAN destination may be either a MAC address or a route descriptor.
4. The total number of duplicate ATM address errors experienced by this LES instance since initialization.

- The Device Configuration category refers to errors experienced due to bad configuration of the device implementing the LEC. Once more for comparison purposes with regular traffic, two traffic and network load counters can be found here.
  1. The total number of successful LE_JOIN_RESPONSESs sent out by the LES.
  2. The total number of LE_ARP_REQUESTs the LES has accepted since its last initialization.
  3. The total number of errors due to invalid request parameters.
  4. The total number of errors due to invalid request identifier.
  5. The total number of errors due to malformed LE_ARP_REQUESTs received by this LES instance.
  6. The total number of registration failure sent back by this LES instance.

8.3.7 BUS Errors Monitoring

The BUS errors reported are:

- The total number of frames that the BUS instance has received that were unicast data frames and all control frames (LE_FLUSH_REQUESTs). The unicast frames refer to LAN Emulation frames with a Destination field containing the MAC address of a physically well-located station. Unicast refers to MAC address type.
- The total number of frames that the BUS instance has received that were multicast frames.

  Note: The multicast frames are LAN Emulation frames whose LAN Destination field contains either the broadcast MAC address (FFFFFFFFFFFF) or any functional MAC address.
- The total number of timeout frames dropped by the BUS due to timeout.
- The total number of multicast send VCC connection setup attempts to the BUS instance that were refused.
- The total number of multicast forward VCC connections setup attempts from the BUS instance that were unsuccessful.

8.3.8 BCM Errors Monitoring

The BCM counters:

- The total number of frames received by BCM for all protocols (IP, IPX, NetBIOS.
- The total number of frames discarded (filtered) by BCM for all protocols.
- The total number of frames for all protocols that BCM could not sent due to an error.
- The total number of multicast forward VCC connection setup attempts from the BUS instance but on behalf of the BCM instance which were unsuccessful.

  Note: BCM transforms broadcast frames into unicast frames but sends this unicast frame over the BUS multicast direct VCC. Whenever this transmission is impossible, then BCM increments this counter.

8.3.9 Top-N Contributors

This RMON-like (rfc1271 RMON Host TopN group) allows you to locate end users that may be over-utilizing the BUS. This function provides a list of the Top-N MAC addresses with the following information:

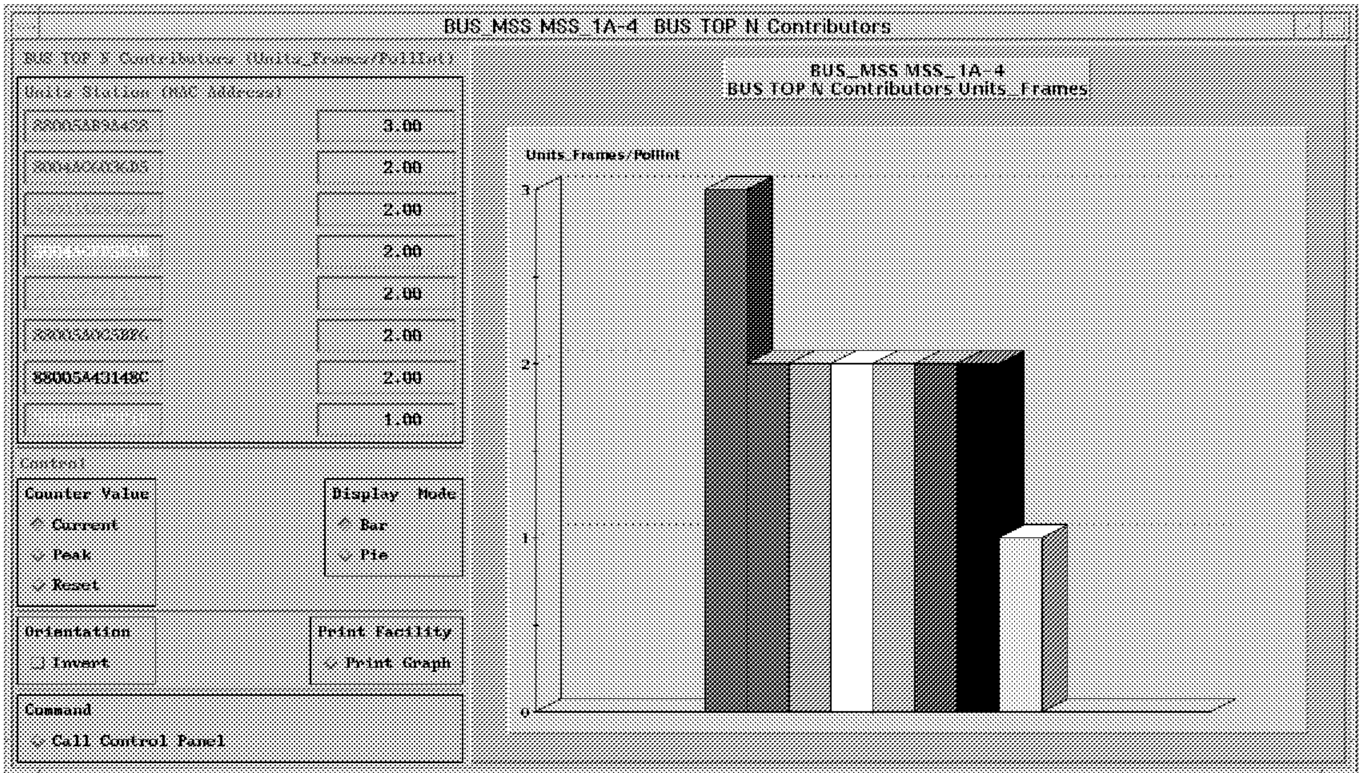

Figure 135. BUS Top 10

- For each sample:
  - The duration of the last sample
  - The number of frames actually sampled during the last complete sample interval
  - The number of frames received during the last complete sampled interval
  - The number of top hosts MAC actually recorded during the last complete sample interval

    Note: This number may be lower than the configured Top-N number of host MAC addresses.
  - The frame sampling rate given as N where the rate is 1 out of every N frames has been sampled.

    Notes:

    This is a read-only indicator that refers to the previously configured desired sampling rate that allows you to specify the rate at which the BUS Monitor will sample frames sent to the BUS during a sample interval.

For the frame sampling rate, a value of 1 indicates that every frame sent to the BUS is sampled. A value of 100 indicates that 1 out of 100 frames sent to the BUS is sampled.

- For each MAC address identified in the Top-N group with N being the highest consumers of BUS resources:

  1. The rank for the indicated host (MAC address) given as N, where 1 is the host originating the most frames
  2. The source MAC address for this host
  3. The associated LEC ATM address
  4. The number of frames sampled from this host during last complete sample interval

8.3.10 Controlling the Number of Sessions

The Statistics Control panel allows you to control all current tasks when the initial panel is started.

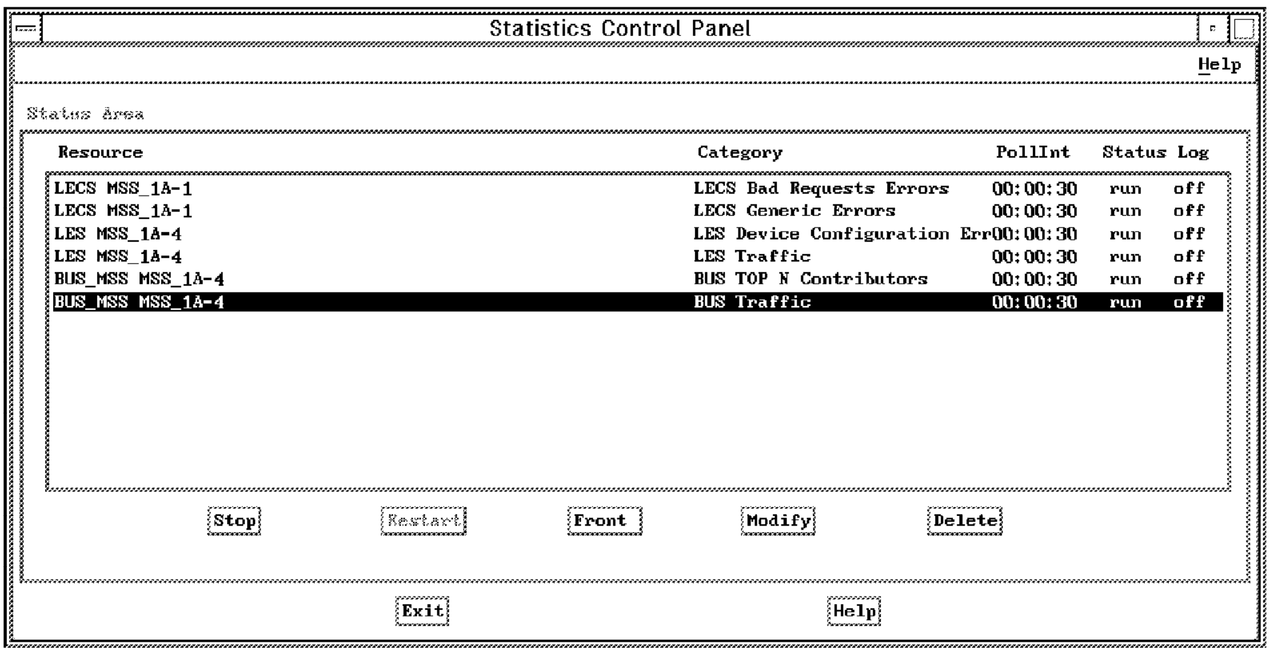

Figure 136. Performance Statistic Sessions

Chapter 9. LAN Emulation Fault

Fault management is concerned with the detection of problems encountered in the Emulated LAN environment. TME 10 NetView will display the majority of SNMP traps generated in our network. In addition we can also use the fault function contained in the Router and Bridge Manager application and the Nways Campus Manager fault function for the LAN emulation elements.

9.1.1 ATM Devices Traps

We configured each ATM device to send SNMP traps to our network management station marco using the PSM configuration modules. For the IBM 8210 we used a telnet session.

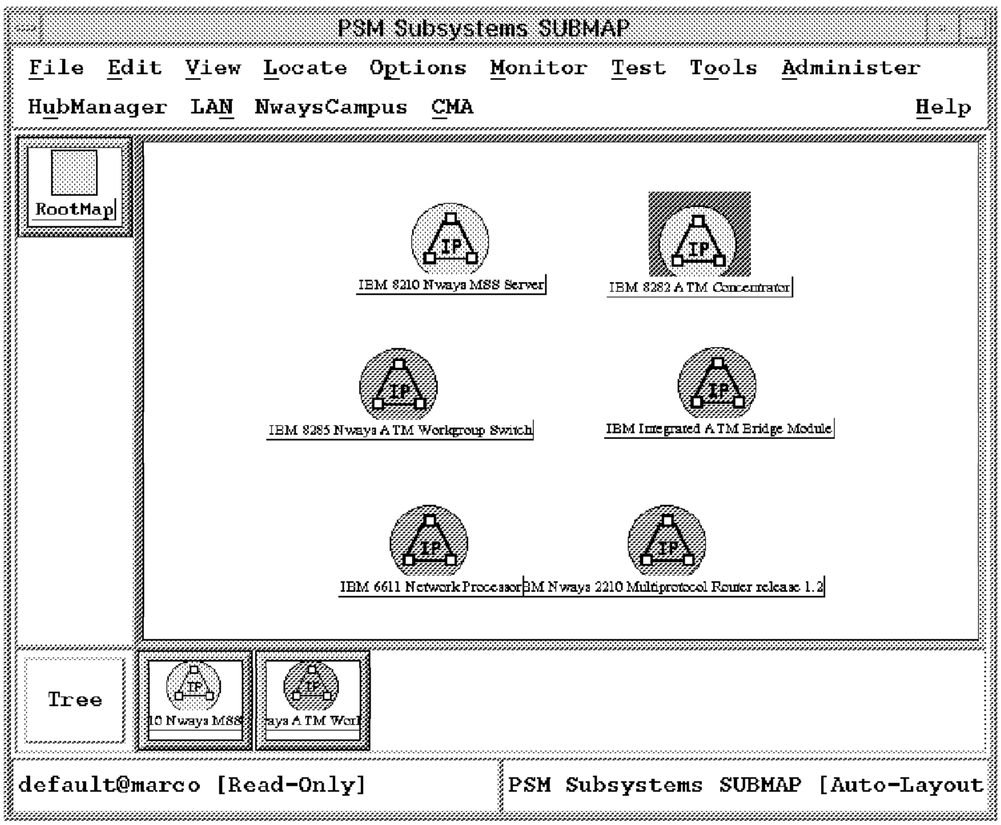

Figure 137. The PSM Submap

For the remaining devices the required trap destination can be configured using the relevant PSM module.

Using the PSM for the 8285 we show how the traps are activated for this device.

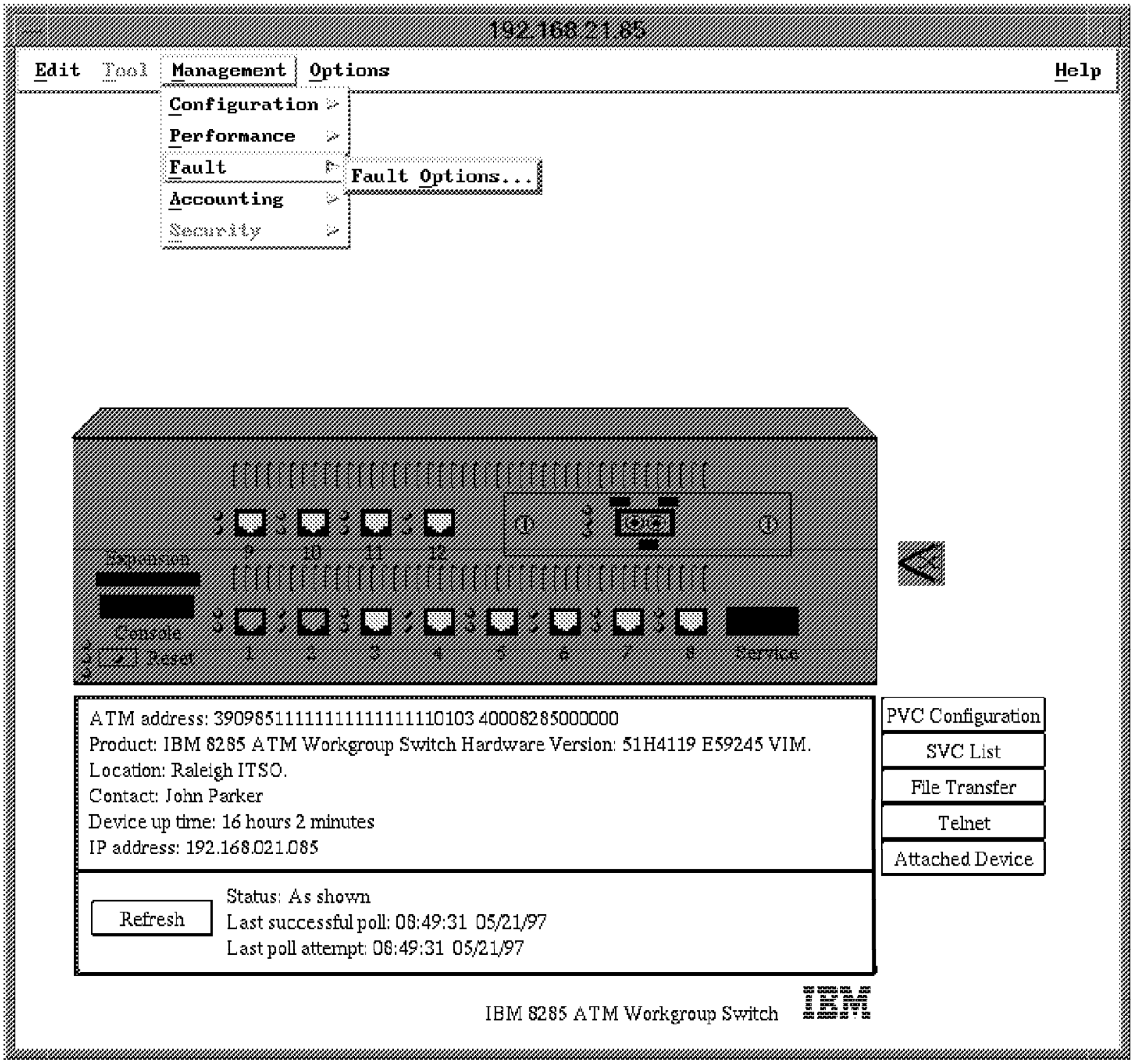

Figure 138. PSM Fault Options

Double-click on the **8285 PSM** icon and select **Management->Fault->Fault-Options**. Figure 139 on page 199 will appear.

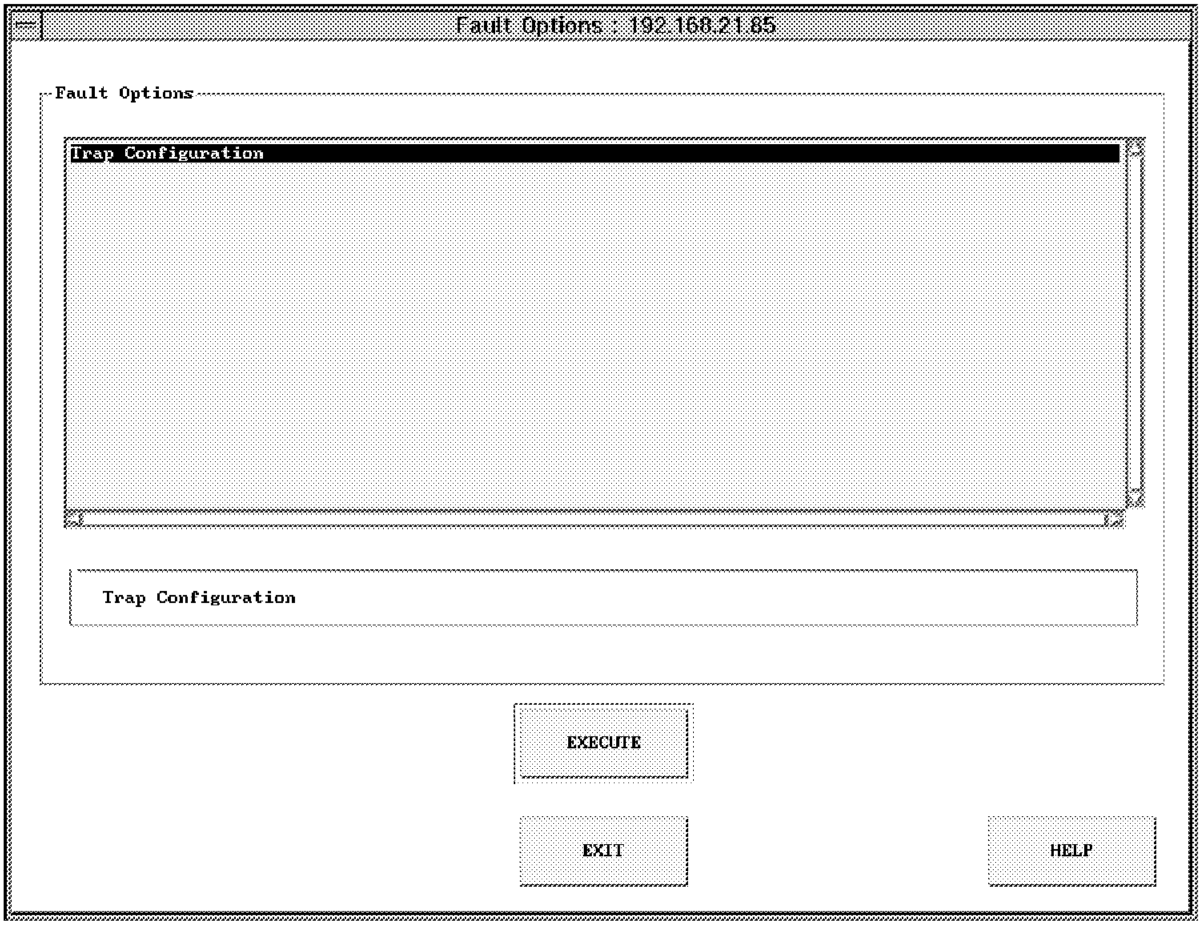

Figure 139. 8285 Trap Configuration

By clicking on **Execute** Figure 140 on page 200 allows the customization for the traps defined for the 8285. Each trap can be enabled and have a specific alarm level associated with it. Figure 140 on page 200 shows how we enabled the Max LE Clients Reached and assigned an alarm level of 3.

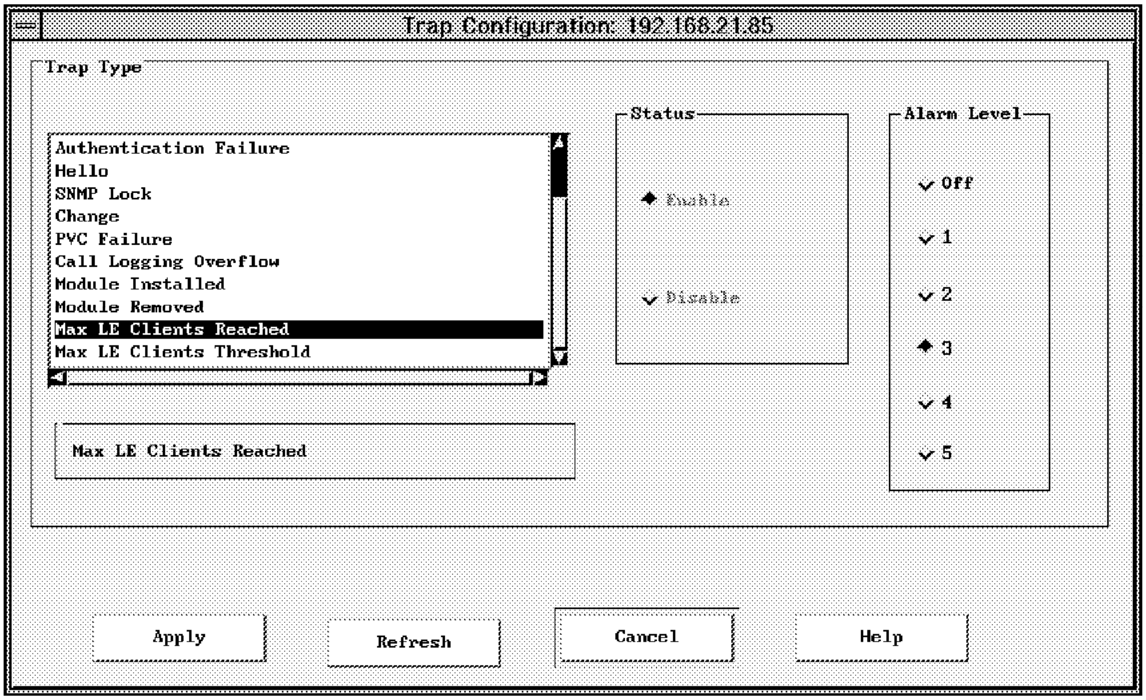

Figure 140. 8285 Trap Customization

For the 8282 and 8281 devices the trap destination can be added by opening the trap receiver option from the configuration screen and entering the IP address or host name of the Network Management Station.

For the 8285 Switch the trap destination must be added manually. Now with the following command you must telnet to the device to set the trap destination so that the network management station can receive these defined traps:

```
telnet 192.168.21.85
```

To define the trap destination:

```
 8285> show community
Index Community_Name  IP_Address           Accesses
--------------------------------------------------------------------------
   1  public          192.168.20.6      Read -  Write - Trap
   2  public          9.24.104.249      Read -  Write - Trap
```

Our network management station was not included in the list so we added it as follows:

```
8285> set community public 192.168.21.12 all
8285> save all
```

When configuring the traps on each of the devices there is a field called Alarm Level. This field refers to the trap severity when shown in the NetView events window. These traps are defined as ibm_win_nv 1.3.6.1.4.1.2.6.87 and have five traps defined. These traps are the associated trap definitions for the five trap levels defined for the devices.

To modify these settings select the enterprise ID shown in Figure 141 on page 201.

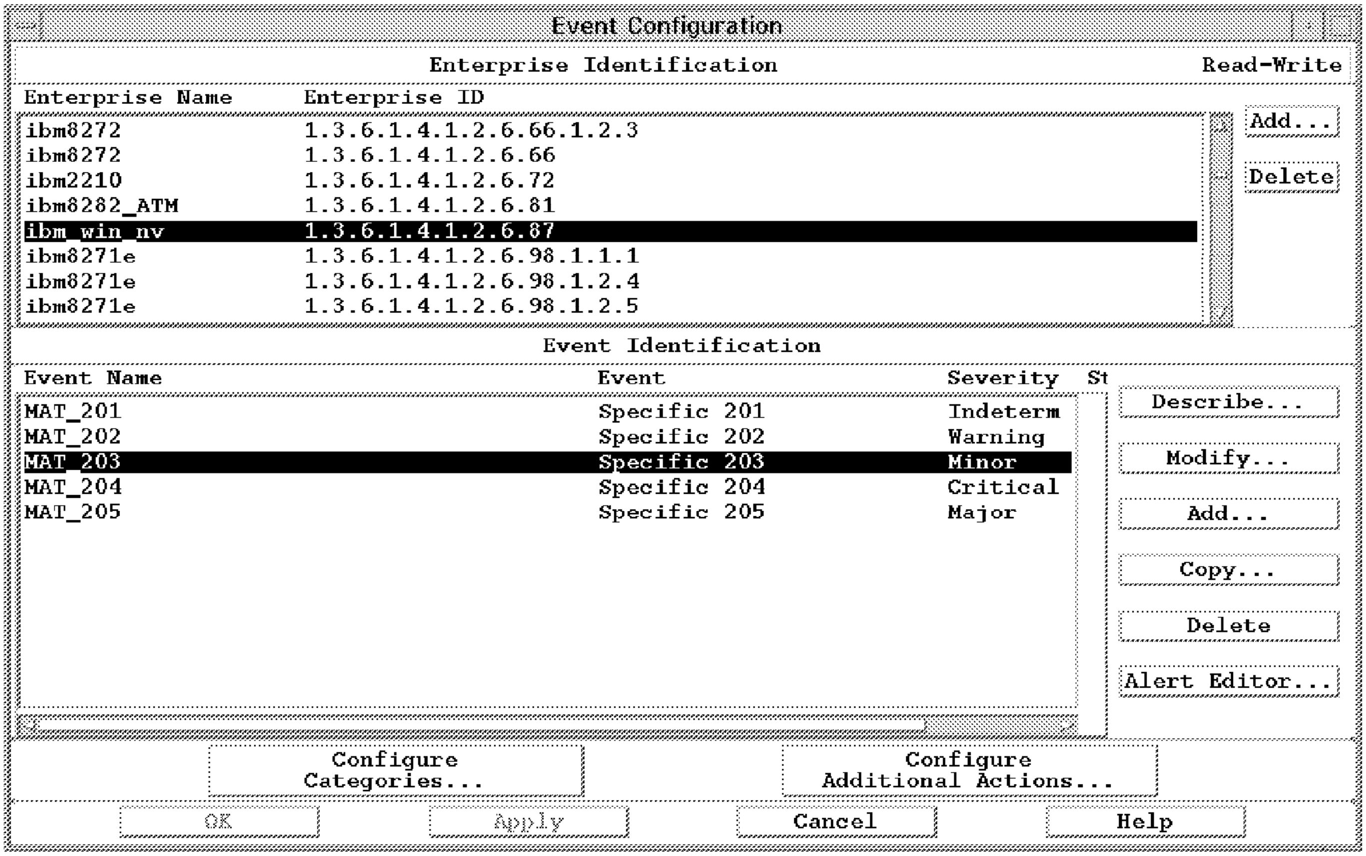

Figure 141. PSM Trap Definitions

For the 8210 we initiated a telnet session and performed the tasks below to define where these traps will be sent.

```
MSS_A *t 6

MSS_A Config>protocol snmp
SNMP user configuration

MSS_A SNMP Config>add address public 192.168.21.12 255.255.255.0
MSS_A SNMP Config>list all

SNMP is enabled
Trap UDP port: 162
SRAM write is enabled

          Community Name                 Access
--------------------------------  -------------------
public                            Read, Write, Trap



         Community Name             IP Address        IP Mask
--------------------------------  ---------------  ---------------
public                            192.168.21.12    255.255.255.0


         Community Name                  Enabled Traps
--------------------------------  --------------------------------
public                            Cold Restart, Warm Restart,
                                  Link Down, Link Up,
                                  Authentication Failure,
                                  EGP Neighbor Loss, Enterprise Specific


          Community Name                       View
--------------------------------  --------------------------------
public                            All0 can also send a trap for each
```

All the managed ATM devices will now send traps to our Network Management Station. The next section deals with the ELAN errors reported that can be reported to the fault component of the Nways Campus Manager ATM.

9.1.2 The LECS Fault Management

The fault management for the LECS instance consists of isolating a problem between the LECS instance, the LECS device and the LEC using the LECS instance.

To get to the LECS Fault Management panel select **Fault** from the context menu shown in Figure 125 on page 182. This will reveal Figure 142 on page 203.

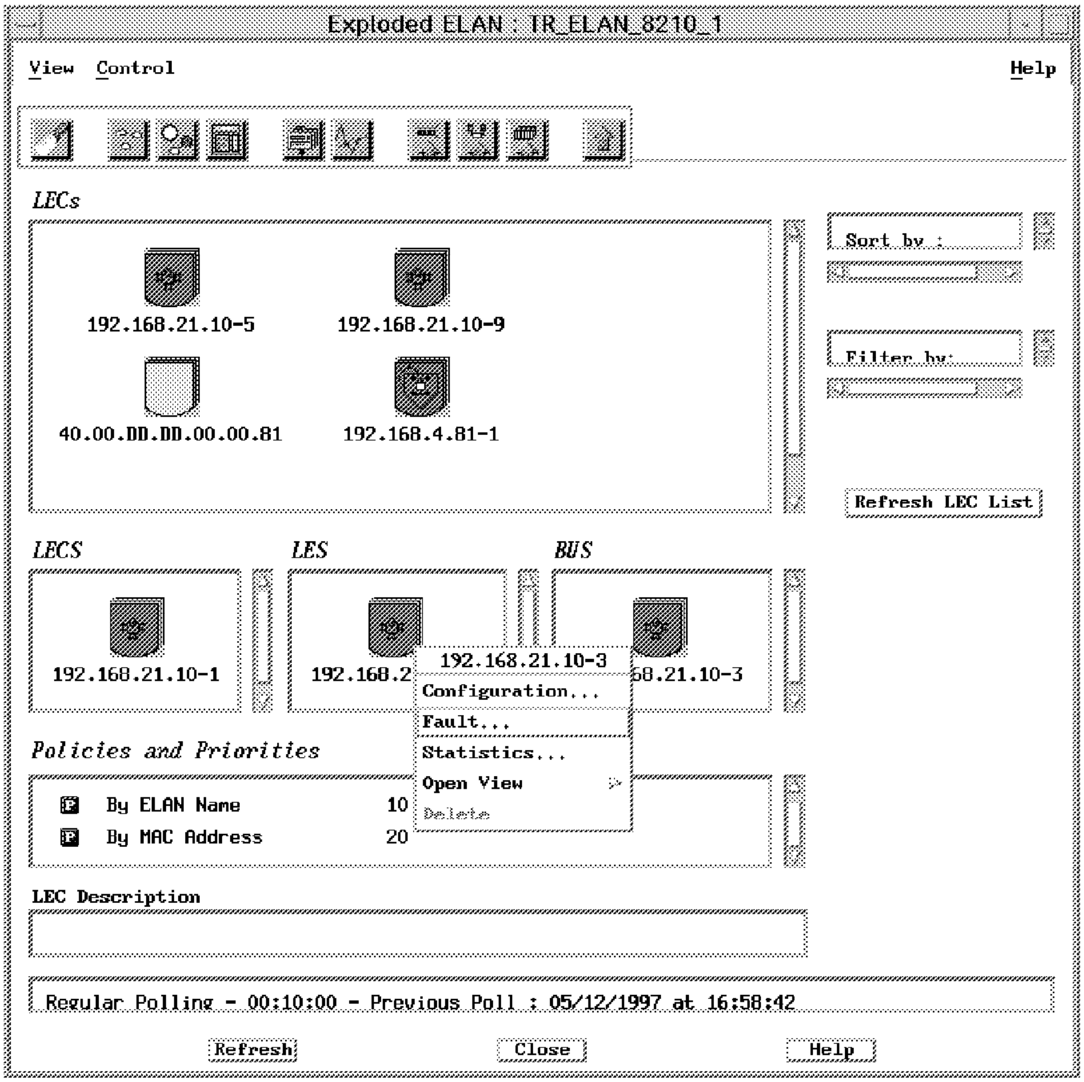

Figure 142. The LES Fault Management Panel

The panel is divided into two parts. The Error Log Control area allows you to set up the error logging capability and the Error Log List displays all the logged error messages. From the Error Log Control area, you can trigger logging by setting the Administrative State to enable. The Operational State should turn to active. Clear the error log associated with this LECS instance by setting the Clear Log button to clear. The maximum number of error log entries is a read-only field and depends on the ATM device implementing the LECS instance. The Last Entry field points to the index of the last entry in the error log table associated with this LECS instance.

The Error Log List area displays logged errors entries. Each entry represents an LEC that was rejected due to a violation against the policies or an error. It contains three fields:

1. The Error Code, which indicates the cause of the error triggered by the LE_CONFIGURE_REQUEST sent by the LEC instance.
2. The Log Time, which indicates the sysUpTime when this entry was logged by the LECS.

3. The ATM address of the LEC that sent the LE_CONFIGURE_REQUEST to the LECS and caused the error to occur.

9.1.3 The LES Fault Management

For the LES instance, the fault management consists of:

- Isolating a problem between the LES instance, the LES device and the LECs serviced by this LES instance
- Analyzing the cause of the problem
- Recovering from the problem

To see the LES Fault Management panel, click on an LES icon in the LAN Emulation ELAN view. Select, from the context-sensitive menu, **Fault**. The LES Fault Management panel is shown. It′s quite similar to the LECS panel.

We configured an OS/2 ATM workstation with the ATM address of:

39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.FF.FF.00.00.81

with the LES ATM address to avoid LECS control. As security is enabled and the policy value table doesn′t contain any value (ATM address) matching this station ATM address, the LE_JOIN_REQUEST should be rejected.

There are a number of LE_JOIN_REQUESTs tried by the LEC. The error code (accessDenied) specifies that the LE_JOIN_REQUEST was rejected by the LES, at the time when the LEC tried to join the ELAN. The primary ATM address of the LEC having tried to join the ELAN can be found in the last column (see Figure 143 on page 205).

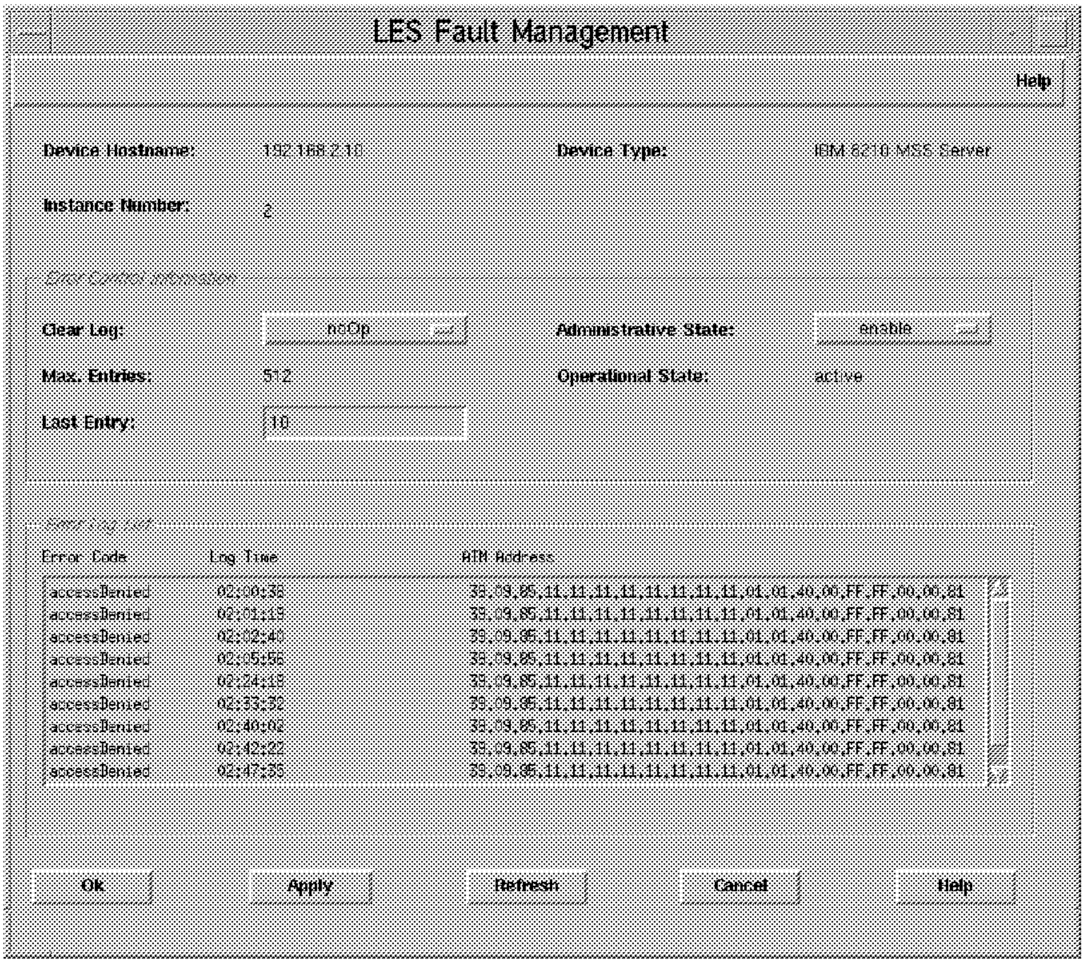

Figure 143. Errors Logged by the LES

The Error Log List, entry represents an LE_JOIN_REQUEST or an LE_REGISTER_REQUEST that was rejected due to an error. The LEC requester, the ATM address, which sent the join or register request and caused the error to occur, can also be found.

9.1.4 The BUS Fault Management

The fault management for a BUS instance consists of:

- Isolating a problem between the BUS instance, the BUS ATM device and the LECs serviced by this NUS instance
- Analyzing the cause of the problem
- Recovering from the problem

The BUS Fault Management application is started from the the LAN Emulation ELAN view. Select the **Fault...** option. The BUS Fault Management panel is displayed. This panel looks like the previous fault management panels for the LECS and LES instances.

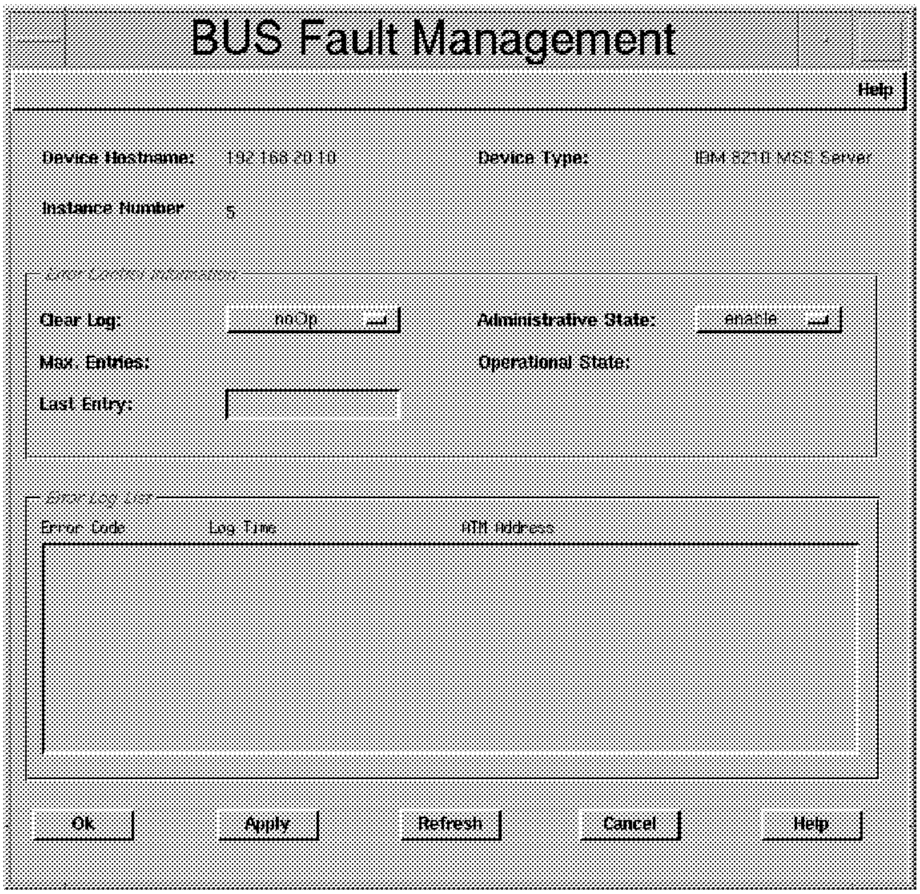

Figure 144. The BUS Fault Management Panel

The Error Log List displays a list of entries referring to LEC instances. The ATM address refers directly to the LEC instance on which the multicast send VCC the error occurred. The following error codes apply to this list:

- Out of resource error
- Malformed control frame for FLUSH_REQUEST frames
- Malformed data frames when the frame received by the BUS is either too big or too small

9.1.5 What Error Messages Are Reported

The following messages will be displayed from the fault screens. This information is contained in the publication.

Table 3 (Page 1 of 2). LAN Emulation Fault Messages

Name	Description
Invalid request parameters	The parameters given are incompatible with the ELAN.
Duplicate LAN destination registration	SOURCE-LAN-DESTINATION duplicates a previously registered LAN destination.
Duplicate ATM address	SOURCE-ATM-ADDRESS duplicates a previously registered ATM address.

Table 3 (Page 2 of 2). LAN Emulation Fault Messages

Name	**Description**
Insufficient resources to grant request	Responder is unable to grant request for reasons such as insufficient table space or ability to establish VCCs.
Access Denied	Request denied for security reasons.
Invalid Requestor-ID	LECID field is not zero (Configure or Join) or is not LE clients LECID (others).
Invalid LAN Destination	LAN destination is a multicast address or, on an Ethernet/802.3 ELAN, a route descriptor.
Invalid ATM Address	Source or target ATM address not in a recognizable format.
No Configuration	LE client is not recognized.
LE_CONFIGURE Error	Parameters supplied give conflicting answers. May also be used to refuse service without giving a specific reason.
Insufficient Information	LE client has not provided sufficient information to allow the LECS to assign it to a specific ELAN.

9.2 Using the IBM 8210 Event Logging System to Generate Traps

The IBM 8210 has a comprehensive event logging system (ELS) that reports on the 8210 warnings and errors. These messages can be converted into SNMP traps and sent to the NetView interface. This process is described below.

The ELS can be defined using the Web browser, configuration tool or using the command interface. We have documented the Web browser and the command prompt options.

To configure using the Web browser select the following from the initial Web screen: **Operator Console->Event Logging**.

From here you can define what messages will be displayed on the 8210 console and what traps are generated based on the ELS messages. These options can also be de-activated from this screen.

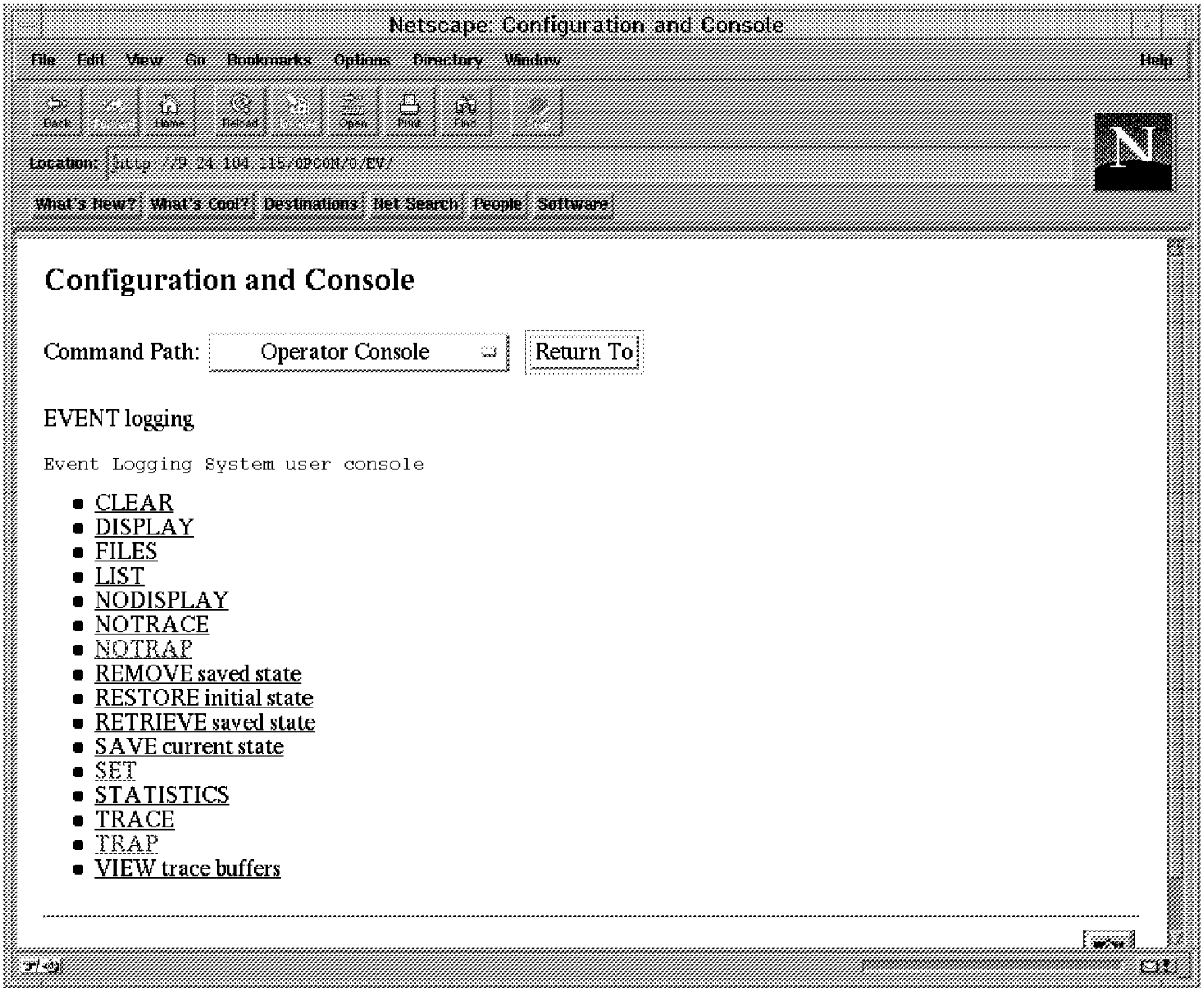

Figure 145. Event Logging Options

The ELS groups the messages into the categories shown in Figure 146 on page 209.

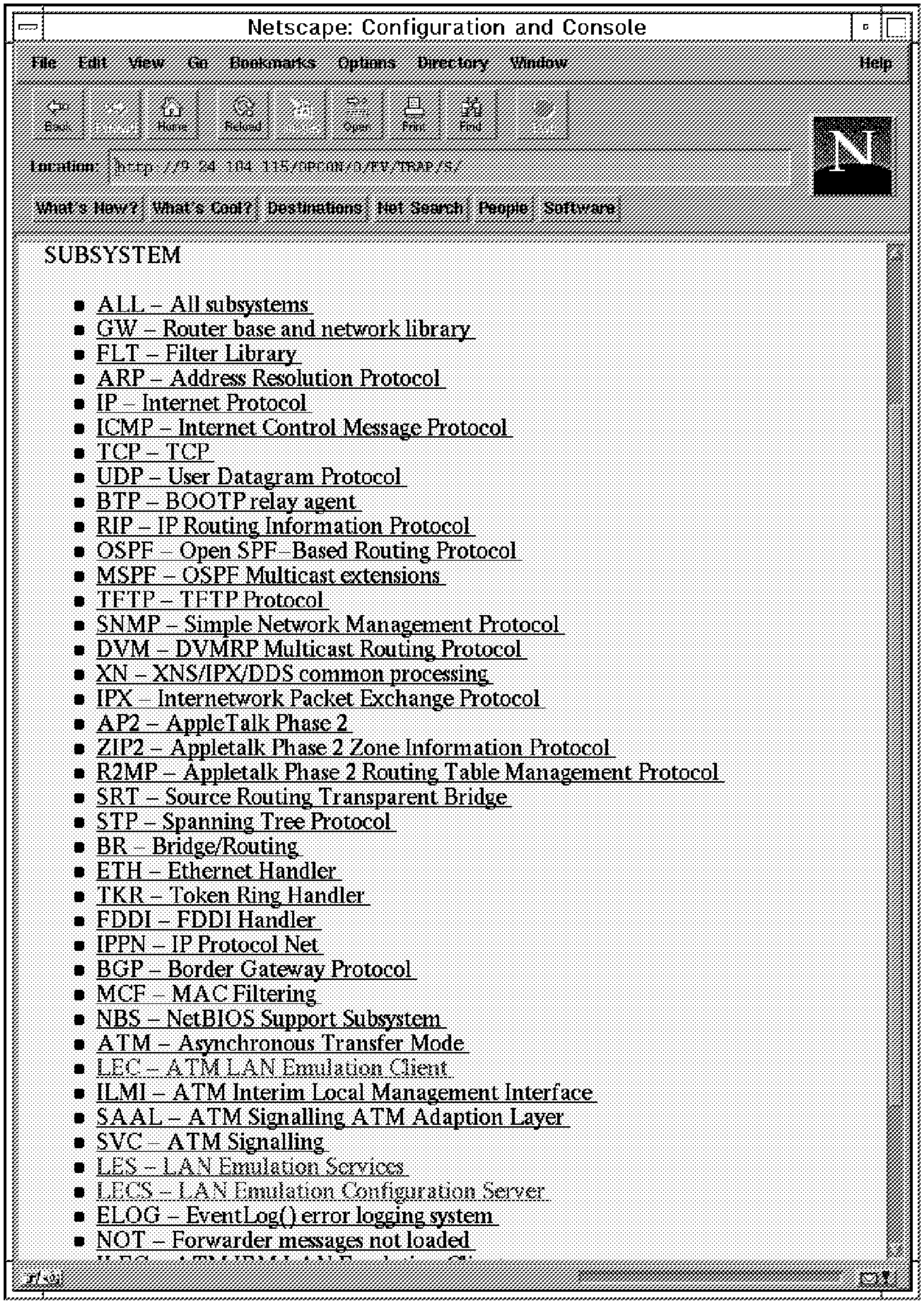

Figure 146. ELS Subsystems

There was one configuration step to be performed on the NetView event customization. Initially when the ELS traps were displayed in the events window they appeared as the PSM type 3 trap detailed earlier in this section. This trap did not display the text message associated with the specific ELS message, therefore this was not useful. However, we did find that there is a trap defined in NetView that is set by default to log only. We amended this to be a status trap and found that the correct message information was being displayed (see Figure 147 on page 210).

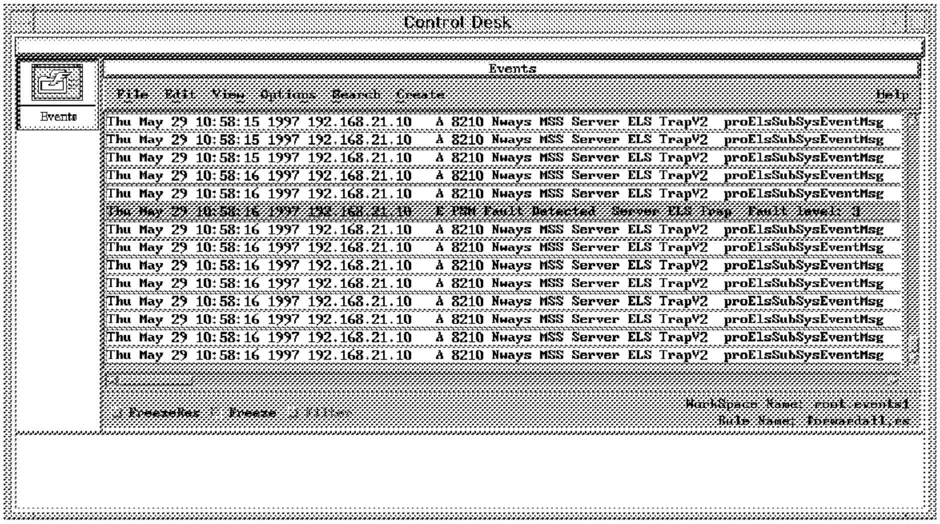

Figure 147. How the Traps Will Appear in NetView

The trap description contained in the example trap is shown in Figure 148.

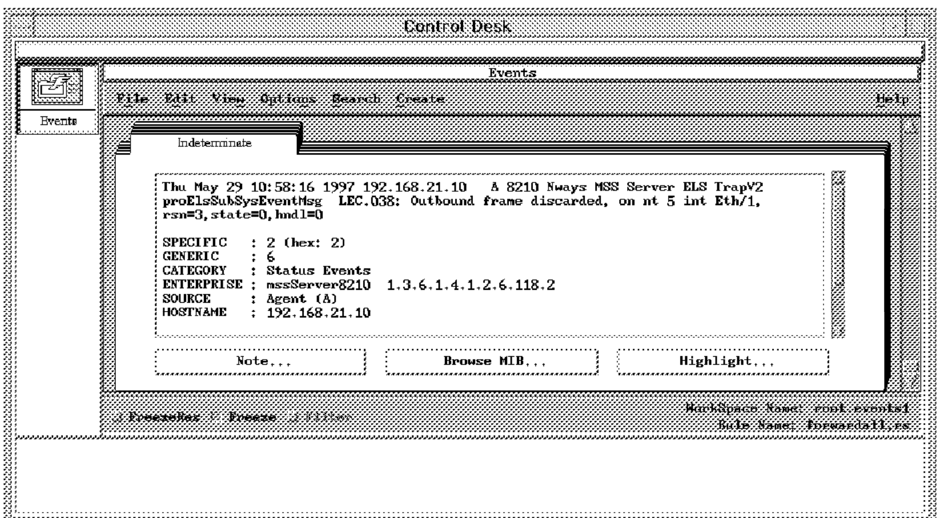

Figure 148. Trap Detail

It is advisable to view the messages using the talk 2 console on the IBM 8210 prior to activating the traps due to the volume of messages that can potentially be generated. Using the display screen the messages can be evaluated and only the required traps can be generated. You can define a different set of messages to be displayed and trapped.

All the ELS messages will appear in the trap definition shown in Figure 148.

To de-activate this using the Web interface issue the following:

```
notrap->subsystem->LAN emulation Client->Error
```

The process below shows how we first evaluated the messages before defining the traps.

Telnet to the 8210.

```
talk 5
```

Initially we activated the logging system to display the traps using talk 2. This enabled us to view the maximum number of traps that we could send to the Network Management Station display subsystem LEC

To view the displayed traps either enter the WEB browser or use talk 2 from the 8210 command prompt.

To view what messages can potentially be generated from the 8210 for a particular subsystem issue the command shown below:

```
ITSO Lab MSS ELS>list subsystem LES

LES.333    UI-ERROR   LES/BUS:'%S':Rstrt fld:%S VCC PCR (%lu Kbps) excds ATM dev
     lnspeed (%lu Kbps)
LES.334    U-INFO     LECS Intf:dev %lu:ATM dev lnspeed -  Config Dir VCC PCR (%
    lu Kbps) mismatch:PCR chngd to lnspeed (%lu Kbps)
LES.335    C-INFO     LECS Intf:dev %lu:ATM dev lnspeed is  %lu Kbps, Config Dir
     VCC PCR = %lu Kbps
LES.336    C-INFO     LECS Intf:dev %lu:ATM dev lnspeed is  %lu Kbps, Config Dir
     VCC PCR = %lu Kbps, SCR = %lu Kbps
LES.337    UI-ERROR   LECS Intf:dev %lu:Create fld:Config Dir VCC PCR (%lu Kbps)
     excds ATM dev lnspeed (%lu Kbps)
LES.338    UI-ERROR   LECS Intf:dev %lu:Rstrt fld:Config Dir VCC PCR (%lu Kbps)
    excds ATM dev lnspeed (%lu Kbps)
LES.339    C-INFO     LES/BUS:'%S':updtd cnfgrtn for fld '%S'
LES.340    UI-ERROR   LES/BUS:'%S':join fld, TLV mem alloc err
LES.341    UI-ERROR   LES/BUS:'%S':rfsd Mcast Send VCC splice to Mcast Fwrd VCC,
LES.343    UI-ERROR   LES/BUS:'%S':Incompatible hardware for VCC-splice operatio
LES.344    U-INFO     SUPER ELAN:Super ELAN spans multiple ATM interfaces, ID=%l
LES.348    U-INFO     BCM:'%S'&colon.Warning: MAC addr x%S
```

This will provide an idea of what messages are categorized, for example ERRORS or WARNINGS.

To list what the active messages are for the LECS subsystem issue see the screen below:

To activate subsystem to send traps to the Network Management Station issue the command:

```
ITSO Lab MSS ELS>trap subsystem lec error
```

To display the messages on the MSS console issue the command:

```
ITSO Lab MSS ELS>display subsystem lec all
```

To view what messages and traps are defined issue the command:

```
ITSO Lab MSS ELS>list active subsystem LEC

Event      Active  Count

LEC.002            13
LEC.008    DT      0
LEC.009    DT      0
LEC.010    DT      0
LEC.011            16439
LEC.012            2400
LEC.015    DT      18
LEC.016    DT      0
LEC.017    DT      39
LEC.018    DT      0
LEC.020    DT      0
LEC.021    DT      0
LEC.022    DT      17
LEC.023    DT      0
LEC.024    DT      0
LEC.025    DT      0
LEC.026    DT      0
LEC.027    DT      0
LEC.028            89
LEC.029    DT      0
LEC.030    DT      0
LEC.031    DT      0
LEC.032    DT      0
LEC.033    DT      0
LEC.034    DT      0
LEC.035    DT      0
LEC.036    DT      0
LEC.037    DT      0
LEC.038    DT      0
LEC.039    DT      0
LEC.040    DT      0
LEC.041    DT      0
LEC.042    DT      0
LEC.043    DT      0
LEC.044            2309
LEC.046    DT      0
LEC.047    DT      0
LEC.048    DT      0
LEC.049    DT      0
LEC.050    DT      0
LEC.051    DT      1
LEC.052    DT      0
LEC.053    DT      0
LEC.054    DT      0
```

D is display and T is a trap.

Finally you can see the volume of messages using the command:

```
ITSO Lab MSS ELS>stat

Subsys  Vector  Exist   String  Active    Heap

  GW     100      99      3345     3        36
 FLT      20       7       184     0         0
 ARP     150     138      6755     0         0
  IP     100     100      2401     0         0
ICMP      30      21       529     0         0
 TCP      60      57      2420     0         0
 UDP      10       6       179     0         0
 BTP      40      13       695     0         0
 RIP      30      19       395     0         0
OSPF      80      73      2590     0         0
MSPF      40      15       514     0         0
TFTP      35      29       819     0         0
SNMP      30      28       821     0         0
 DVM      30      21       589     0         0
  XN      35      21       780     0         0
 IPX     110     107      4545     0         0
 AP2      80      70      1755     0         0
ZIP2      60      51      1859     0         0
R2MP      50      38      1185     0         0
 SRT     120      91      4852     0         0
 STP      60      32      1590     0         0
  BR      50      30      1616     0         0
 ETH      60      47      1098     0         0
 TKR      60      45      2031     0         0
FDDI      30      27      1155     0         0
IPPN      20       4       132     0         0
 BGP      80      74      2477     0         0
 MCF      15       9       244     0         0
 NBS     100      50      3029     0         0
 ATM     200     176      8647     0         0
 LEC     200      56      2251     0         0
ILMI     150      23       482     0         0
SAAL      30      26       621     0         0
 SVC      30      26       435     0         0
 LES     350     348     21517     0         0
LECS     150     137      5342     0         0
ELOG       1       1       105     0         0
 NOT      25      15       508     0         0
ILEC     100      46      1748     0         0
NHRP     250     201      7786     0         0
BBCM      20      14       466     0         0

Total   3191    2391    100492     3        36
```

Once the messages have been activated you can view them on the MSS using talk 2.

```
ITSO Lab MSS *t 2
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Misc LEC_DROP_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
 LEC.015: nt 1 Debug LEC_PROCESS_INBOUND_MCAST_FRAME
```

Appendix A. ATM Forum-Compliant LAN Emulation

The reason for this chapter is to familiarize the reader with the basic concept of the ATM Forum-Compliant (FC) LAN emulation.

A.1 Why LAN Emulation?

Most data traffic in existing customer premise networks (CPNs) is sent over local area networks (LANs) such as Ethernet or token-ring networks. This data traffic is generated by applications that interface to LAN adapter device drivers via standard interfaces such as NDIS or ODI. As ATM APIs (application programming interfaces) are not yet ready to allow application-to-interface directly with ATM and the AAL layer, and to go on using the vast base of existing LAN applications, a new service has been defined. This service is called LAN Emulation.

The main objectives of this LAN Emulation service is to offer existing applications that have access to ATM networks via protocol stacks such as APP, NetBIOS, IPX, and AppleTalk as if they were running over traditional legacy LANs (Ethernet or token-ring). The LAN Emulation service offers the same MAC driver service primitives (NDIS and ODI) to the upper protocol layers. At this price, the upper protocol layers will stay unchanged.

A.2 Forum-Compliant LAN Emulation

Today′s networking applications are running primarily on Ethernet and token-ring networks that interface to LAN adapters via standard interfaces such as ODI and NDIS. ATM Application Programming Interfaces (APIs) are under development which will allow applications to interface directly with the ATM layer and take advantage of all of ATM′s advanced features (such as Quality of Service). In the meantime, a service is required that will allow existing applications running on Ethernet and token-ring networks to take advantage of, at least some of ATM′s benefits today, such as high-speed switched connections and scalability. This service is called LAN Emulation.

LAN Emulation allows ATM-attached stations, as well as token-ring and Ethernet stations to communicate over an ATM network without any changes to existing applications. For directly attached ATM stations (via 25, 100 or 155 Mbps), a driver is installed at the data link layer which presents a standard token-ring or Ethernet interface to the upper layers, while at the same time, converting LAN frames to ATM cells to present to the ATM network. Endstations that do not have an ATM interface, but are on token-ring or Ethernet segments, can access the ATM network by means of a bridge or switch which has an ATM uplink. This type of device is known as a proxy as it does the frame-to-cell conversion and connection management, on behalf of its LAN-attached endstations.

A.3 Emulated LANs (ELANs)

There is much confusion in the industry over what is meant by the terms ELAN and VLAN, as these terms are often used interchangeably. To avoid further confusion, we define these terms as they apply in this publication.

VLAN: A Virtual LAN (VLAN) is a logical grouping of hosts, independent of physical location in the network, which defines what stations can communicate to each other. A VLAN can be based, for instance, on layer 2 MAC addresses, in which case all members of the VLAN belong to the same broadcast domain. VLANs can also be assigned based on LAN switch ports.

ELAN: The term Emulated LAN (ELAN) is a specific implementation of a Virtual LAN, as it relates to LAN Emulation in ATM networks. An ELAN consists of one or more LAN Emulation clients (LEC) which share the same LAN Emulation Server and Broadcast and Unknown Server (LES/BUS). Broadcasts by any member of the ELAN are contained within the boundaries of that ELAN, and ELAN membership can be assigned based on configurable policies.

The device that provides the LAN Emulation functions is the IBM 8210. This device supports the creation of multiple ELANs, each with their own instance of LES/BUS. In addition, it also supports a single instance of LAN Emulation Configuration Server (LECS). The LES, BUS and LECS are collectively known as the LE Service components. The LE clients may obtain the address of their LES/BUS from a LAN Emulation Configuration Server (LECS), or alternatively, may be pre-configured with their LES/BUS address. It is preferable to allow the LECS to assign the LES/BUS address to the LE client, as the LECS can act as the central administration point for the creation of ELANs based on policies. For instance, an ELAN based on an ELAN_NAME policy, could assign all LE clients with the name ACCOUNTS to one ELAN, and all the LE clients with the name ENGINEERING to another ELAN. For ATM-attached endstations, this would allow the physical re-location of the endstation without requiring reconfiguration of that endstation, that is, an engineering workstation would still belong to the ENGINEERING ELAN, regardless of where it is located.

Note: For token-ring or Ethernet-attached endstations, care must be taken when relocating endstations to ensure that the switch or bridge to which they are being moved has an LE client on the same ELAN.

Figure 149 on page 217 shows a physical and logical view of a simple LAN Emulation network consisting of two ELANs.

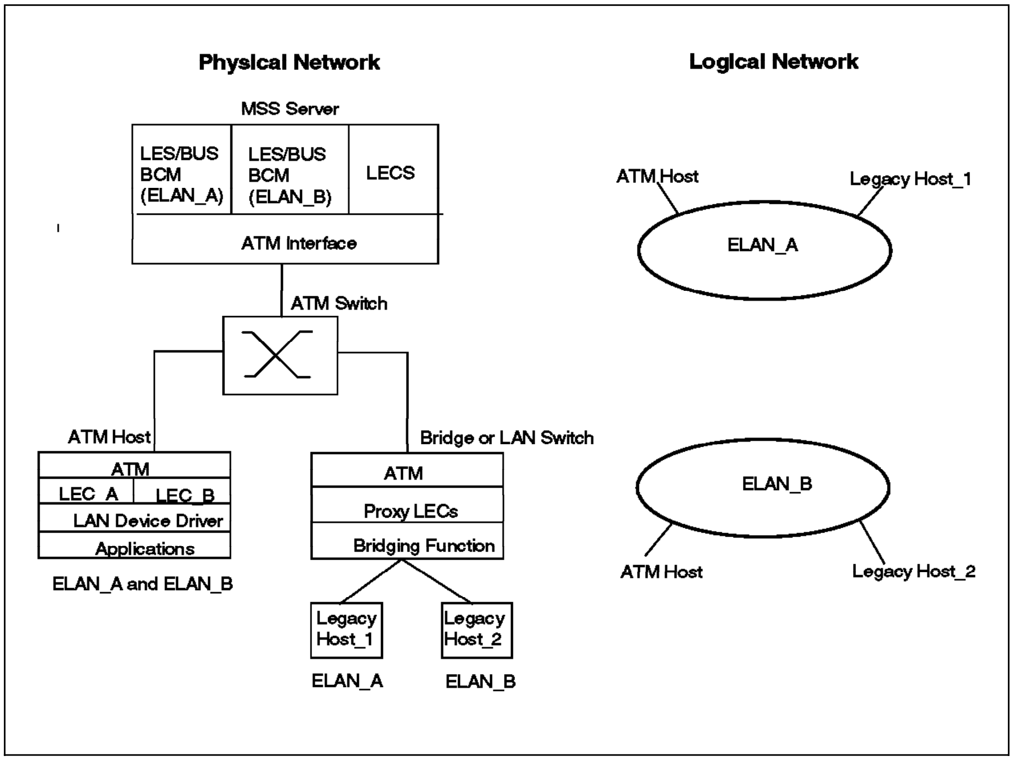

Figure 149. Physical and Logical Views of a Simple LAN Emulation Network

The LAN Emulation 1.0 specification does not specify how ELANs should be interconnected. To enable ELANs to be interconnected, the MSS server has extensive bridging and routing functions. These bridging and routing functions are accessed by creating internal LE clients (LECs), which are assigned to the ELANs to be bridged or routed. These internal LECs convert the ATM cells to token-ring or Ethernet frames which are then processed by the MSS′s internal bridge or router, before being converted back to ATM cells to be forwarded to the destination ELAN. All members of an ELAN must be of the same type, that is, Ethernet or token-ring. However, ELANs of different types can be bridged or routed by the MSS server.

Note: It is worth noting that the Nways Campus Manager ATM application *does not* provide the function to define the routing and bridging capabilities for the IBM 8210. This is performed using either the IBM 8210 configuration application or the Web browser.

An LE client can only belong to a single ELAN, however, an endstation that has more than one ATM adapter (or an adapter that supports more than one LE client), can have LE clients belonging to different ELANs.

Before going into LAN Emulation in more detail, we review the basics of ATM addressing and the functions of ILMI, as they relate to LAN Emulation.

A.4 ATM Addresses

ATM uses 20-byte hierarchical addressing. The first 13 bytes of an ATM address are called the network prefix, and end systems obtain the network prefix component of their addresses from their adjacent switch. The next six bytes of the address are called the end system identifier (ESI), and the final byte is called the selector. End systems form their addresses by appending an ESI and selector to the network prefix provided by the switch. The selector is only significant within the end system; it is not used to route calls within the ATM network, but is used within end systems to uniquely identify called/calling parties.

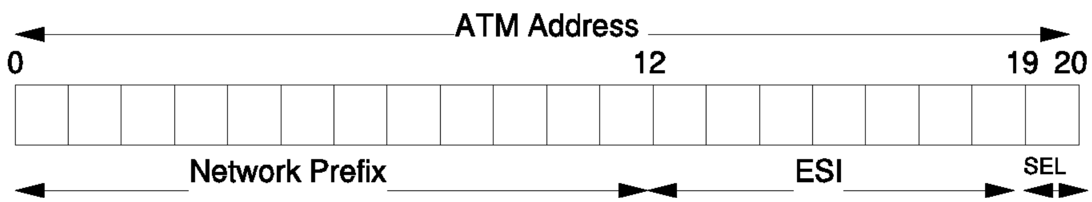

Figure 150. ATM Addresses

The network prefix and ESI components of ATM addresses must be registered with ATM switches before calls can be placed or received. If the address is not unique (that is, if it duplicates an address already registered with the switch), the switch will reject the registration. One way to guarantee a unique ATM address is to use the burned-in (universally administered) IEEE MAC address as the ESI. Each ATM interface on the MSS contains a burned-in MAC address that may be used in this manner. The MSS also allows users to configure locally administered ESIs on each ATM interface.

A.4.1 ATM Addresses of LAN Emulation Components

In general, ATM addresses must be unique among LAN Emulation components. The only exception is that an LES and BUS serving the same ELAN, may share an ATM address. (This is the case on the MSS server.) LAN Emulation components are configured for a particular ATM interface, and the user may decide to use the burned-in MAC address as the ESI portion of the component′s ATM address, or select one of the locally administered ESIs defined for the ATM interface. Multiple LE components may share the same ESI if they have unique selectors. By default, the configuration interface assigns each LE component a unique selector value for the configured ESI; however, the user may override this assignment and explicitly configure a particular selector value.

An ATM interface parameter determines the number of selectors per ESI reserved for explicit assignment. (The remainder are available for dynamic assignment by the ATM interface at run time.) LE components only use the selectors reserved for explicit assignment; by default, 200 of the 256 possible selectors per ESI are reserved for explicit assignment. Run-time selector assignment is beneficial when the user does not need to control the assigned selector. (Classical IP Clients are an example.)

While ATM addresses must be unique among LE components, LE components may use the same ATM addresses as non-LE components such as Classical IP clients/servers.

A.5 Overview of ILMI Functions

The Interim Local Management Interface (ILMI) defines a set of SNMP-based procedures used to manage the user-to-network interface (UNI) between an ATM end system and an ATM switch. The following three ILMI functions are particularly relevant to LAN Emulation:

1. ATM address registration
2. Dynamic determination of UNI version being run on the switch
3. Acquisition of the LECS ATM address(es)

By default, the ATM interfaces of an MSS server use ILMI procedures to query the switch MIB in an attempt to determine the signalling version (UNI 3.0 or 3.1) being run at the switch. If the query succeeds and both ends of the ATM link have defined the same UNI version, the MSS server configures accordingly, if both ends have defined different UNI versions, connection establishment fails. In addition to explicit definition, either or both ends can specify auto-detection of the other end′s UNI version as well.

ILMI is also the method of choice for locating the LECS. The ILMI MIB at the ATM switch included a list of LECS ATM addresses that may be retrieved by the LECs. This is useful because the LECS ATM address(es) has to be configured at the ATM switches only, not at LECs, and there are fewer switches than LECs.

A.6 Classical IP

Classical IP is included because we use this connection method for our Network Management Station. The ATM host connection using Classical IP will connect to other hosts by being part of a logical IP subnet (LIS). This LIS will contain an ATM Address Resolution Protocol (ATMARP) server and a number of ATMARP clients. The ATMARP server is responsible for maintaining a table of ATM addresses and their corresponding IP address.

The Classical IP connected devices will be routed to other IP subnets in order to communicate with the LECs. The Classical IP components are as follows:

- ATMARP Server
- Clients
- ARP VCCs

A.6.1 LAN Emulation Components

We now take a closer look at the individual components that make up an ELAN. An emulated LAN comprises the following components:

- One LAN Emulation Server (LES)
- One LAN Emulation Configuration Server (LECS)
- One Broadcast and Unknown Server (BUS)
- LAN Emulation Clients (LECs), such as user workstations, bridges, routers, etc.

Users connect to the ELAN via LE clients, which request services through the LAN Emulation User-to-Network Interface (LUNI). The three components (LE server, LECS, and BUS) may be distributed over different physical systems or may be grouped together in one system, but logically they are distinct functions.

The LAN emulation services may be implemented in ATM intermediate systems (for example, switches such as the 8260 and 8285) as part of the ATM network, or in one or several ATM end systems, such as the MSS.

As illustrated in Figure 151 on page 221, each LEC has to support a variety of VCCs across the LUNI for transport of control and data traffic.

A.6.1.1 LAN Emulation Server (LES)

The basic function of the LE server is to provide directory and address resolution services to the LECs of the emulated LAN. Each emulated LAN must have an LE server. An LE client registers the LAN address(es) it represents with the LE server. When an LE client wants to establish a direct connection with a destination LEC, it gets the destination′s MAC address from the higher layer protocols and has to ask the LE server for the destination′s ATM address. The LE server will either respond directly (if the destination client has registered that address) or forward the request to other clients to find the destination.

An emulated token-ring LAN cannot have members that are emulating an Ethernet LAN (and vice versa). Thus, an instance of an LE server is dedicated to a single type of LAN emulation. The problems of translational bridging between different LAN types is not addressed in the ATM Forum′s LAN emulation. However, the MSS will do translational bridging between Ethernet and token-ring for NetBIOS and SNA protocols.

The LE server may be physically internal to the ATM network or provided in an external device, but logically it is always an external function that simply uses the services provided by ATM to do its job.

Note: For a discussion of the value-adds that the MSS server introduces in addition to the basic LES functions, see Chapter 4, “Configuring LAN Emulation Elements” on page 87.

A.6.1.2 LE Configuration Server (LECS)

The LECS assigns the individual LE clients to the different virtual LANs that can exist in the ATM network. During initialization, an LE client requests the ATM address of the LE server for the ELAN to which it should be connected. An LE client is not required to request this information from the LECS; an LE server′s ATM address may be configured (system-defined) in the LE client.

Using an LECS to assign clients to the different ELANs allows for central configuration and administration of multiple ELANs in an ATM network. The LECS could make its decision to assign an LE server, for example, based on a client′s ATM or MAC address according to a defined policy, or simply based on a system-defined database.

Note: For a discussion of the value-adds that the MSS server introduces in addition to the basic LECS functions, see Chapter 4, “Configuring LAN Emulation Elements” on page 87.

A.6.1.3 LECS Recommendations

To take advantage of MSS Server′s flexibility in creating policy-based ELANs, it is recommended that LECs be configured to use the LECS to obtain the ATM address of their LES, where possible.

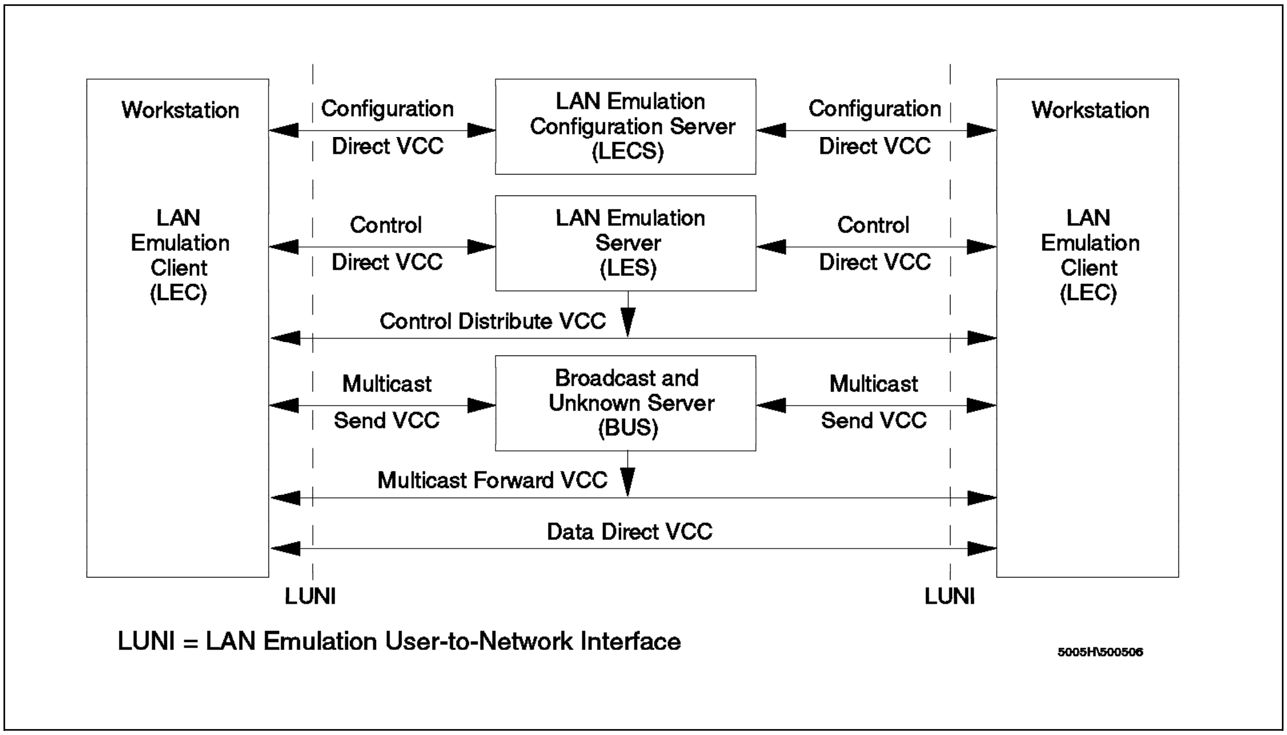

Figure 151. LAN Emulation Components

A.6.1.4 Broadcast and Unknown Server (BUS)

The BUS has two main functions: to distribute multicast and broadcast frames to all LECs in the ELAN, and forward unicast frames to the appropriate destination. An LEC sends unicast frames to the BUS if it does not have a direct connection to the LEC representing the destination. To avoid creating a bottleneck at the BUS, the rate at which an LEC can send unicast frames to the BUS is limited.

Note: For a discussion of the value-adds that the MSS server introduces in addition to the basic BUS functions, see Chapter 4, "Configuring LAN Emulation Elements" on page 87.

A.6.1.5 LAN Emulation Client (LEC)

Each workstation connecting to the ELAN has to implement the LE layer (also called LE entity), which performs data forwarding and control functions such as address resolution, establishment of the various VCCs, etc. The LE layer functions could be implemented completely in software, in hardware on a specialized LAN emulation ATM adapter, or in a combination of both. The layered structure of the LEC is shown in Figure 152 on page 222.

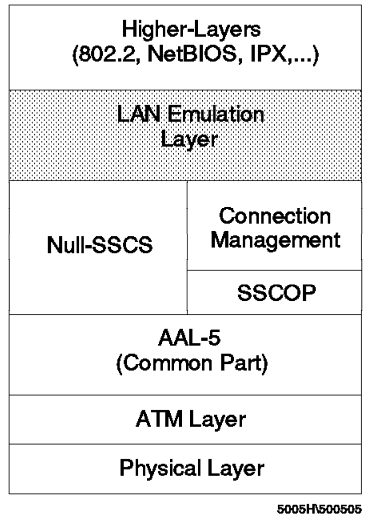

Figure 152. LAN Emulation Client Functional Layers

The LE layer provides the interface to existing higher layer protocol support (such as IPX, IEEE 802.2 LLC, NetBIOS, etc.) and emulates the MAC level interface of a real shared media LAN (802.3/Ethernet or token-ring). This means that no changes are needed to existing LAN application software to use ATM services. The LE layer implements the LUNI interface when communicating with other entities in the emulated LAN.

The primary function of the LE layer is to transfer LAN frames (arriving from higher layers) to their destination either directly or through the BUS.

A separate instance of the LE layer is needed in each workstation for each different LAN or type of LAN to be supported. For example, if both token-ring and Ethernet LAN types are to be emulated within a single station, then you need two LE layers. In fact, they will probably just be different threads within the same copy of the same code but they are logically separate LE layers. Separate LE layers would also be used if one workstation needed to be part of two different emulated LANs both emulating the same LAN type (for example, token-ring). Each separate LE layer needs to have a different MAC address and must be attached to its own LE server, but it can share the same physical ATM connection (adapter).

A.6.2 LAN Emulation VC Connections

Data transfer in the LE system (consisting of control messages and encapsulated LAN frames) uses a number of different ATM VCCs.

A.6.2.1 Configuration and Control Connections

Control VCCs connect an LE client to the LE configuration server and the LE server, but they are never used for user data traffic. These connections may be permanent or switched and are established when an LE client connects to the ELAN.

Configuration Direct VCC

A bidirectional, point-to-point configuration direct VCC may be established between an LE client and the LECS to obtain configuration information (for example, the LE server′s ATM address).

Control Direct VCC

A bidirectional, point-to-point control direct VCC must be established (and kept active) between each LE client and the LE server. This is used for the exchange of control traffic (for example, address resolution) between the LE client and the LE server.

Control Distribute VCC

The LE server may optionally establish a unidirectional control distribute VCC to distribute control information (for example, query for an unregistered MAC address) to all LE clients connected to the ELAN. This can be a point-to-point VCC to each LE client. If the ATM supports point-to-multipoint connections, then the LE server might instead establish one point-to-multipoint VCC to all LECs (of course, the clients will be added or deleted as leaves on this point-to-multipoint tree as they enter or leave the ELAN).

A.6.2.2 Data Connections

Data connections are direct VCCs from an LE client to other LE clients and to the BUS. They are used to carry user data traffic and never carry control traffic (except for a flush message for cleanup).

Data Direct VCC

For unicast data transfer between end systems, data direct VCCs are set up through ATM signaling as bidirectional, point-to-point connections once the LE client has received the destination′s ATM address from the LE server.

As long as a data direct VCC has not been established (the protocol flows with the LE server may take some time), an LE client may send initial data frames through the BUS, but as soon as a data direct VCC is established, it has to be used and no data must be sent through the BUS. Since the LAN frames can be exchanged between two LE clients through either the BUS or using the direct VCC (that is, there are two possible paths between the clients to exchange LAN frames), careful control is needed to ensure that when the direct VCC becomes available, frames are not delivered out of sequence to the destination.

Data direct VCCs stay in place until one of the partner LECs decides to end the connection based on installation options defining relevant timeouts, etc.

Multicast Send VCC

During initialization, an LEC has to establish a bidirectional, point-to-point multicast send VCC to the Broadcast and Unknown Server (the BUS′s ATM address is provided to the LEC by the LE server) and must keep this VCC established while being connected to the ELAN. This VCC is used by the LEC to send broadcast and multicast data frames. It is also used by the LE clients for sending unicast frames until a data direct VCC is established between the LE client and its partner. The BUS may use this VCC to send data (including multicast) to the LEC.

Multicast Forward VCC

When an LE client establishes its multicast send VCC to the BUS, the BUS learns about the new member of the ELAN. The BUS then will initiate signaling for the unidirectional multicast forward VCC to the LEC, which is used to forward data frames from the BUS to the LECs. This VCC can be either point-to-point or point-to-multipoint. (Of course, a point-to-multipoint VCC is more effective for multicast operations.)

Every LEC must be able to receive data frames from the BUS (both over the multicast send VCC or the multicast forward VCC) but will not receive duplicates as the ATM Forum LAN emulation specification prevents the BUS from sending duplicates frames on these VCCs.

Note: When using the MSS server′s intelligent BUS function two separate multicast forward VCCs will be established; one to the proxy LE clients and one to the non-proxy LE clients.

A.6.3 LE Service Operation

In operation, the LAN emulation service performs the following functions:

Initialization

During initialization, the LE client discovers its own ATM address from the ATM switch, which is needed if the client is to later set up direct VCCs. It obtains the LE server′s ATM address from the LECS and establishes the control VCCs with the LE server and the BUS. The BUS address is provided to the LE client by the LE server.

For more details of this function, refer to A.6.3.1, "Initialization" on page 225.

Address Registration

Clients use this function to provide address information to the LE server. A client must either register all LAN destinations for which it is responsible, or join as a proxy. The LAN destinations may also be unregistered as the state of the client changes. An LE server may respond to address resolution requests if LE clients register their LAN destinations (MAC addresses, or for source routing IEEE 802.5 LANs only, route descriptors) with the LE server.

For more details on address registration, see A.6.3.2, "Address Registration" on page 230.

Address Resolution

This is the method used by an ATM client to associate a LAN destination with the ATM address of another client or the BUS. Address resolution allows clients to set up data direct VCCs to carry frames. This function includes mechanisms for learning the ATM address of a target station, mapping the MAC address to an ATM address, storing the mapping in a table, and managing the table.

For the server, this function provides the means for supporting the use of direct VCCs by endstations. This includes a mechanism for mapping the MAC address of an end system to its ATM address, storing the information, and providing it to a requesting endstation.

For more details on this function, refer to A.6.3.3, "Address Resolution" on page 231.

Connection Management

In SVC environments the LAN emulation client, the LAN emulation server, and BUS set up connections between each other using UNI signaling. This function is beyond the scope of this book.

Data Transfer

To transmit a frame, the sending LE layer must do the following:

- Decide on which of its VCCs (to destination LE client or BUS) a frame is to be transmitted.
- Encapsulate the frame. (AAL-5 is used).

It must also decide when to establish and release data direct VCCs. To do this it may need to access the LE server for address resolution purposes.

For more details of this function, refer to A.6.3.4, "Data Transfer" on page 232.

Frame Ordering

A sending LAN emulation client and a receiving client may have two paths between them for unicast frames, one via the BUS and one via a data direct VCC between them. A client is expected to use only one path at a time for a specific LAN destination, but the choice of paths may change over time. Switching between those paths introduces the potential for frames to be delivered out of order to the receiving client. The out-of-order delivery of frames between two LAN end systems is uncharacteristic of LANs, and undesirable in an ATM emulated LAN. The Flush protocol is therefore provided to ensure the correct delivery of unicast data frames.

For more details of this function, see A.6.3.5, "Frame Ordering" on page 233.

A.6.3.1 Initialization

The initialization of a LAN emulation client comprises the definition of the initial state and the following five operational phases:

1. LAN Emulation Configuration Server Connect Phase
2. Configuration Phase
3. Join Phase
4. Initial Registration Phase
5. Broadcast and Unknown Server Connect Phase

These phases must be completed in the specified order; and if a LAN emulation client (LE client) is to achieve full interoperability, all of these phases must be completed successfully.

Initial State: The initial state of a client is an implementation issue, but certain parameters are the subject of range constraints. Parameters have a minimum and maximum value and also a default value. If any parameter falls outside of its range, the result may be a poorly functioning or possibly a non-functioning emulated LAN.

If the initialization phase terminates abnormally, the LAN emulation client must return to the initial state and inform layer management.

LAN Emulation Configuration Server (LECS) Connect Phase: In the LECS connect phase, the LE client establishes its session with the LAN emulation configuration server. Although connecting to the LECS is optional, its use is recommended. Use of the LECS enables you to centrally control which LE clients connect to which ELANs, and to set LE configuration parameters. Another reason to use LECS functions to learn the LES ATM address is because the MSS server′s LES/BUS redundancy relies on the use of LE clients connecting to an LECS first.

Some LE client drivers, however, do not support use of the LECS, in which case, the LES address needs to be manually configured in the LE client and LECS functions are bypassed.

The LEC may obtain the ATM address of the LECS from its adjacent switch in one of several ways. The correct order to obtain the ATM address of the LAN Emulation Configuration Server is as follows:

1. Get LECS address via ILMI

   The LE client should issue an ILMI Get or GetNext to obtain the ATM address of the LECS for that user-to-network interface (UNI). The LE client then attempts to establish a configuration direct VCC to the ATM address it has received from the ILMI process. If the connection establishment fails the LE client issues an ILMI Get or GetNext request to determine if an additional LECS ATM address is available and connects to it.

   Note: See "IBM 8260 and 8285 LECS Address Support:" on page 227 for how to configure the 8260/8285 to enable adjacent LE clients to learn the LECS via ILMI.

2. Use the well-known LECS address (WKA)

   If the LECS address cannot be obtained from ILMI, or if the LEC is unable to connect to any of the addresses found in the ILMI table, the LEC will attempt to connect to the following well-known address (WKA):

   x′47007900000000000000000000000A03E00000100′

   Note that the adjacent switch must be configured to map the WKA to the real address of the LECS.

   Note: See "IBM 8260 and 8285 LECS Address Support:" on page 227 for how to configure the 8260/8285 to enable adjacent LE clients to use the well-known LECS address.

3. Use the LECS PVC

   If the LEC cannot establish a connection to the well-known address, then the well-known PVC of VPI=0, VCI=17 (decimal) must be used to connect to the LECS.

It is recommended you use the ILMI procedure, unless an ATM switch or the LAN emulation device driver of an ATM adapter does not support this.

After the LEC has obtained the ATM address of the LECS it will set up a configuration direct VCC to the LECS. The LEC then enters the configuration phase. Note that the LEC can drop this VCC whenever it wants to.

IBM 8260 and 8285 LECS Address Support: Both IBM 8260 and 8285 support the previously outlined methods of obtaining the LECS address. To put one or more addresses in the ILMI MIB of the 8260 or 8285, the following command has to be issued from the command prompt:

```
>set lan_emul configuration server inactive_wka
>Enter ATM address :
```

Multiple LECS addresses can be entered in this way. The client will attempt to connect to each address entry, in turn, until it makes a successful connection.

To address the rerouting of the well-known address to a real address the following command must be issued from the 8285/8260 command prompt:

```
>set lan_emul configuration server active_wka
>Enter ATM address :
```

Configuration Phase: In the configuration phase, the LE client obtains the ATM address of the LE server and optionally other configuration parameters necessary to prepare the LE client to enter the join phase (see "Join Phase" on page 228).

There are the following two types of control frames used in the configuration phase:

- LE_CONFIGURE_REQUEST

  This is issued by the LE client to the LECS along the configuration direct VCC to obtain configuration information. The request contains the following information:
  - C1 The primary ATM address
  - C2 The LAN type
  - C3 The maximum data frame size
  - C4 Whether the LE client is acting as a proxy for other unicast MAC address(es)
  - C5 The name of the emulated LAN
  - C6 The local unicast MAC
  - C8 The route-descriptors (SRB bridges only)

  The local unicast MAC address is optional. ELAN name, type and maximum data frame size may be unspecified.
- LE_CONFIGURE_RESPONSE

  This is issued by the LECS in response to the LE_CONFIGURE_REQUEST. The response contains the following information:
  - C2 The LAN type
  - C3 The maximum data frame size
  - C5 The name of the emulated LAN
  - C9 The target ATM address - the address of the LE server

The configuration phase can be performed by using static parameters configured into the LE client or by using the LE configuration protocol that retrieves the parameters from the LECS. By using the LE configuration protocol, the LE client can be assigned to different emulated LANs and will learn the operating parameters of those LANs. The LECS will forward these operating parameters as well as the ATM address of the LE server to the LE client using the LE_CONFIGURE_RESPONSE.

If the LE client does not receive an LE_CONFIGURE_RESPONSE within the specified time period (configurable) it can retry until the configured number of retries is exhausted, at which time the configuration phase fails. The client will then return to the beginning of the initialization phase.

Join Phase: In the join phase, the LE client establishes its connection with the LE server. It will determine the operating parameters of the emulated LAN and is permitted, though not required, to register one MAC address/ATM address with the LE server.

The join protocol uses the following two type of frames:

- LE_JOIN_REQUEST

  This is sent by the LE client to the LE server as a request to be permitted to join an emulated LAN. It contains the following information:
  - C1 The primary ATM address
  - C2 The LAN type
  - C3 The maximum data frame size
  - C4 Whether the LE client is acting as a proxy for other unicast MAC address(es)
  - C5 The name of the emulated LAN
  - C6 The local unicast MAC
  - C8 The route descriptors (SRB bridges only)

  The local unicast MAC address is optional. ELAN name, type and maximum data frame size may be unspecified.
- LE_JOIN_REPONSE

  This is sent by the LE server to the LE client in response to the LE_JOIN_REQUEST. It contains the following information:
  - C2 The LAN type
  - C3 The maximum data frame size
  - C5 The name of the emulated LAN
  - C14 The LE client identifier (LECID)

The LE client will set up a control direct VCC with the LE server or use a predefined control direct PVC if the LE client has been unable, or fails, to set up an SVC connection. The control direct VCC is point-to-point bidirectional connection. If the LE client is unable to establish either of these virtual circuits it terminates the join phase. Once the control direct VCC is established, the LE client sends an LE_JOIN_REQUEST containing the information discussed above. Having sent the LE_JOIN_REQUEST, and if no LE_JOIN_RESPONSE has been received, the LE client will accept any request by the LE server to establish a control distribute VCC. However, if a response has been received, the LE client will assume no control distribute VCC is required and has the option to refuse an attempt by the LE server to make this connection. Further, if the LE client receives no response within the configured time allowed (the default is 120 seconds), it can retry until the configured number of retries is exhausted, at which time the join phase fails.

If the LE server does not receive the LE_JOIN_REQUEST on a new control direct VCC within a set time (the default is 120 seconds), it has the option of terminating the LE client′s membership of the emulated LAN.

When an LE_JOIN_REQUEST is received, the LE server validates the request, in which case it has the option of setting up a control distribute VCC to the LE client. For the request to be successful it must contain either an exact match with the LE server′s LAN type or unspecified in the LAN type (LE client variable C2). The maximum frame size (LE client variable C3) must be either unspecified or greater than or equal to the LE server′s maximum frame size.

The LE server will check for duplicate MAC addresses and/or duplicate ATM addresses already registered. If this occurs, the join request will fail and no LE client identifier will be assigned. Once the conditions are met for a successful join, the LE server will issue an LE_JOIN_RESPONSE to the LE client and the join phase of initialization is completed.

Initial Registration Phase: When the LE client sends an LE_JOIN_REQUEST, it has the option of including one MAC address in LE client variable C6. If this occurs, the LE server will register this MAC address with the ATM address mapping as part of the join phase. The LE server will check for duplicate MAC addresses and duplicate ATM addresses already registered. If either are found, the registration request will fail.

Following a successful join phase, the LE client has the option of registering more LAN destinations using the LE registration phase and the LE client variables C6 (or route descriptor fields using variable C8 if the LE client is a source-route bridge).

Important

The registration phase is optional, however, if the registration is performed the LE client must register all of its local unicast MAC addresses and if the LE client is a token-ring emulated client, it must also register all its route descriptors. All registrations must be complete before the LE client reaches an operational state. Once in operational state, the LE client must not have in its variable C6 or C8 any LAN destination that has not successfully been registered with the LE server. Therefore, an LE client with only one unicast MAC address need not use the registration protocol, since it may implicitly register one MAC address during the join phase. This is because a join with a MAC address is functionally equivalent to a join without a MAC address, followed by a register with a MAC address.

Also note that an LE client must either register all LAN destinations for which it is responsible or join as a proxy.

Broadcast and Unknown Server Connect Phase: In the Broadcast and Unknown Server (BUS) connect phase, the LE client establishes its connection with the BUS. In order to determine the ATM address of the BUS, the LE client issues an LE_ARP_REQUEST to the LE server to resolve all the broadcast MAC addresses. The LE server will respond with the LE_ARP_RESPONSE containing the ATM address of the BUS.

The LE client uses this address to establish a bidirectional multicast send VCC. This VCC is used by the LE client to send all broadcast and multicast destination packets to the BUS. When the multicast send VCC is established, the BUS automatically establishes the multicast forward VCC. This VCC is unidirectional and can be either point-to-point or point-to-multipoint. It is used by the BUS to send multicast frames to LE clients. If the multicast send VCC cannot be established, the LE client may be removed from the emulated LAN.

If either party detects the release of the multicast send VCC, it will automatically release the multicast forward VCC. The LE client has the option of attempting to reestablish the connection for a configurable number of attempts. If these attempts fail, the LE client will terminate its membership of the emulated LAN.

If the LE client detects the intentional release of the multicast forward VCC, it will terminate its membership of the emulated LAN without any attempt at recovery. If it detects that this release was accidental, it may attempt to recover the connection for a configurable number of attempts after which it will terminate its membership of the emulated LAN.

In the case of the BUS detecting that the multicast forward VCC has been released, it will release that LE client′s multicast send VCC and will make no attempt to reestablish the multicast forward VCC.

A.6.3.2 Address Registration

The address registration protocol is used by an LE client wishing to register additional LAN destination and ATM address pairs not registered during the join phase.

The registration procedure can occur at any time after successfully joining an emulated LAN and is optional. The following are the four types of registration protocol frames:

- LE_REGISTER_REQUEST

  This frame is sent by the LE client to the LE server. It contains a request to register one LAN destination ATM address pair.
- LE_REGISTER_RESPONSE

  This frame is sent by the LE server in response to the LE_REGISTER_REQUEST. It contains confirmation of a successful registration.
- LE_UNREGISTER_REQUEST

  This frame is sent by the LE client to the LE server. It contains a request to remove the registration of one LAN destination ATM address pair.
- LE_UNREGISTER_RESPONSE

  This frame is sent by the LE server in response to the LE_UNREGISTER_REQUEST. It contains confirmation of a successful removal of the registration.

If an LE client has only one unicast MAC address, it need not use the registration protocol because every LE client can implicitly register one MAC address during the join phase. It should also be noted that a join with a MAC address is functionally equivalent to a join without a MAC address followed by a register with a MAC address.

All (un)register requests are issued over the control direct VCC. The LE server will respond to (un)registration requests over either the control distribute VCC or the control direct VCC. The LE server checks for duplicate MAC addresses and duplicate ATM addresses already registered. The rules governing registrations are as follows:

- An ATM address can only be associated with one LECID.

- An LECID can only be associated with one ATM address.
- An ATM address/LECID mapping can have multiple MAC addresses associated with it.
- A MAC address cannot be registered by more than one ATM address.
- An ATM address/LECID mapping cannot register a MAC address already associated with another ATM address/LECID mapping.

If a registration request does not fully comply with these rules, then it will fail.

If an LE client requests the unregistration of a mapping it did not register, the LE server will send a successful response but will not actually unregister a mapping registered by another LE client.

A.6.3.3 Address Resolution

The address resolution protocol is used by the LE client to associate a MAC destination address with the ATM address of another LE client. Address resolution makes the establishment of data direct VCCs possible so that data can be transferred directly between ATM end systems.

The following are four types of address resolution frames:

- LE_ARP_REQUEST

  This frame is sent by an LE client to determine the ATM address of a given MAC address or route descriptor.
- LE_ARP_RESPONSE

  This frame is sent by the LE server in response to the LE_ARP_REQUEST to provide the information requested.
- LE_NARP_REQUEST

  This frame is sent by the LE client to advertise changes in remote address bindings.
- LE_TOPOLOGY_REQUEST

  This frame is sent by either the LE server or the LE client to indicate that network topology changes are in progress.

LE_ARP Procedure: When the LE client has a frame to transmit to an unknown MAC destination address, it issues an LE_ARP_REQUEST on its control direct VCC to the LE server.

When the LE server receives the LE_ARP_REQUEST, it can take the following actions:

1. If the MAC destination address is known to the LE server, it can issue an LE_ARP_RESPONSE. This response will contain the ATM address of the LE client responsible for the LAN destination. If the LE_ARP_REQUEST contains the broadcast MAC address, the LE server responds with the ATM address of the BUS.

2. If the LAN destination is unknown to the LE server, it will do the following:

   a. Forward the LE_ARP_REQUEST to all LE clients using either the control direct VCC or the control distribute VCC.

   b. Forward the LE_ARP_REQUEST to those LE clients that registered as proxy agents using either the control direct VCC or the control distribute VCC.

If the LE server has forwarded the LE_ARP_REQUEST and then receives an LE_ARP_RESPONSE from an LE client, it adds the new mapping to its LE ARP cache and forwards the response to the LE client that originated the request. The LE client adds the new mapping to its LE ARP cache.

LE_NARP Procedure: When an LE client believes that the mapping between a target LAN destination and target ATM address is no longer valid, it has the option of issuing an LE_NARP_REQUEST. This only applies to remote LAN-ATM address mappings and usually occurs because the LE client is now representing the target LAN destination at its source ATM address.

LE_TOPOLOGY Procedure: When the topology of the network changes, either the LE client or the LE server will issue the LE_TOPOLOGY_REQUEST frame to inform the other members of the emulated LAN that these changes are underway. When an LE client receives an LE_TOPOLOGY_REQUEST, it will not use any entries for non-local LAN destinations from its LE ARP cache. If the LE server receives an LE_TOPOLOGY request, it will forward this to all LE clients.

If the LE client is an IEEE 802.1D transparent bridge, it issues an LE_TOPOLOGY_REQUEST for every configuration BPDU that it issued to the BUS. These LE clients also have the option of basing the LAN emulation topology change state on the spanning tree configuration BPDU instead of those received in the LE_TOPOLOGY_REQUEST.

A.6.3.4 Data Transfer

Once the LE client has established the ATM location of the other party, it will establish a data direct VCC with that client. The calling client may already be sending unicast data frames to the BUS to forward to the client. If this is the case, the LE client will issue an LE_FLUSH_REGISTER (see A.6.3.5, “Frame Ordering” on page 233). The LE client will examine all frames received on any data direct VCC and if it finds any frames with its own LECID, it will discard them. All frames will be filtered by LECID to allow only those frames required by the higher layer to be forwarded.

If the LE client receives a connection request from a client to which it already has a connection, it will accept the request, but will send frames only on the VCC that was initiated by the numerically lower ATM address. This may cause the duplicate VCC to be aged out. If the LE client detects that the control direct VCC or the control distribute VCC is released at any time other than the join phase, then the LE client must terminate its membership of the emulated LAN.

If the BUS receives a valid data frame from an LE client over a multicast send VCC, it will forward it using either the multicast forward VCC or the multicast send VCC.

Delivery of Token-Ring Frames: When the LE client has a frame to send, it examines both the frame′s destination MAC address and the routing information field to determine where to send the frame and if it is required to issue an LE_ARP_REQUEST. An LE client emulating token-ring must support address resolution of route descriptors. If the location of the target LAN destination is unknown, it must send an LE_ARP_REQUEST to the LE server. It may also send the frame to the BUS.

A.6.3.5 Frame Ordering

The LE client is able to send unicast frames to the same MAC address using the BUS and using a data direct VCC at different times. A mechanism is required to ensure that there is no possibility of delivering frames out of order by having two paths. That mechanism is known as the Flush protocol.

The flush message is a special frame identifiable as a non-data frame by having a reserved value X′FF00′ in the LAN emulation data frame header in place of the LECID of the sender.

The Flush protocol uses the following two frame types:

- LE_FLUSH_REQUEST

  This frame is sent by the LE client to either the BUS using the multicast send VCC, or another LE client using the data direct VCC. It is used to ensure that all data frames in transit on the path have reached their destination LE client.

- LE_FLUSH_RESPONSE

  This frame is sent in direct response to the LE_FLUSH_REQUEST by the called LE client. The frame is sent to the LE server using the control direct VCC or the control distribute VCC for forwarding to the LE client who initiated the flush.

Flush protocol is comprised of mandatory rules that must be applied to any component of the emulated LAN, whether they implement Flush protocol or not, and optional rules that must be applied if an LE client implements flush. The mandatory rules are discussed below.

The LE client sends LE_FLUSH_REQUEST over either the data direct VCC or the multicast send VCC. The client that receives the LE_FLUSH_REQUEST will always send the LE_FLUSH_RESPONSE to the LE server using the control direct VCC. The LE server will then forward this response to the LE client that originated the request. If the BUS receives an LE_FLUSH_REQUEST for another LE client, it will forward the request to that client using either the multicast send VCC or multicast forward VCC.

If an LE client chooses to implement flush, there are certain mandatory rules. These are discussed below.

The LE client sends an LE_FLUSH_REQUEST on either the data direct VCC or the multicast send VCC. This request must contain a transaction identifier, the source ATM address and the ATM address of the target LE client. The sending LE client cannot reuse the data direct VCC for the same LE client until it has received the LE_FLUSH_RESPONSE with matching transaction identifier. During this period, the sending LE client can either hold or discard data frames destined for a LAN destination. If the LE client does not receive a response within the required time, it will either discard any frames it is holding for that target or will send them down the old path. It can then issue another LE_FLUSH_REQUEST containing a new transaction identifier. Once the reply is received, it will send all held data frames on the new path before sending any additional frames.

A.6.3.6 Termination Phase

In the preceding section where it is indicated that the LE client will terminate the phase and all the SVCs associated with the client (including all control VCCs, data direct VCCs, and all VCCs to and from the BUS) must be released, the LE server and BUS will not attempt to reestablish the VCC for any reason.

A.6.3.7 Operation in Real Systems

In many practical LAN networks this system is going to work very well indeed. While LANs allow any-to-any data transport, typical LAN users connect to very few servers (such as communication servers, file servers, and print servers) at one time.

In this situation, the LE architecture described above can be extremely effective. After a short time, workstations will have established VCCs with all of the servers that they usually communicate with. Data transfer is then direct and very efficient. Timeouts can be set so that the switched VCCs are maintained during normal session usage.

Further details and an explanation of ATM Forum LAN emulation over ATM is available in the ATM Forum Technical Committee′s *LAN Emulation Over ATM* technical specification.

A.6.4 LAN Emulation Summary

LAN Emulation provides a relatively efficient means of transporting existing LAN-based applications across an ATM network, providing them with the benefits of high-speed switched connections and scalability. A LAN Emulation system consists of the following basic components:

1. LAN Emulation Clients which reside on endstations or proxy-bridges/ switches. These provide the interface between traditional LAN traffic based on frames, and the ATM cell-based network.
2. A LAN Emulation Server (LES) which provides ATM to MAC address resolution.
3. A Broadcast and Unknown Server (BUS) which forwards all broadcast traffic (and some unicast traffic) to the LE clients.
4. A LAN Emulation Configuration Server, which assigns LES/BUS addresses to attaching LE clients. This feature is optional, but if available, provides a central administration point for the assignment of policy based ELANs.

Appendix B. Appendix B MIB Definitions

The Nways Campus management applications require SNMP MIBS in order to manager the components. The sections below explain what MIBs are used.

The following MIB definition files can be found in the directory /usr/OV/snmp_mibs. They can be loaded using the command /usr/OV/bin/xnmloadmib.

The MIBS we loaded are listed below:

```
af-FORUM-TC.mib
af0044-LEC.mib
af1129-BUS.mib
af1129-ELANLECS.mib
af1129-LES.mib
```

The MIBS are described in the sections below.

B.1 MIB II Definitions

The section below lists the MIB II definitions concerned with LAN Emulation:

ifIndex The index identifying the interface.

ifType The type of the interface:

1. aflane8023(59) for 802.3 LAN Emulation client
2. aflane8025(60) for 802.5 LAN Emulation client

ifPhysAddress The interface address at the protocol layer immediately below the network layer in the protocol stack. For an active LAN Emulation client the MAC address it has registered to a LAN Emulation Server (LES). As LUNI lets clients register MAC addresses dynamically, this value may change over time when the client either joins the emulated LAN or unregisters its current MAC address.

ifAdminStatus The desired state of the interface used when an inactive client joins an emulated LAN. The MIB-II ifOperStatus and the LAN Emulation client MIB lecInterfaceState will mirror the progress and success of the attempt. This MIB variable doesn′t mirror the success or failure of a join attempt and won′t be set to down because an attempt ended in a failure.

ifOperStatus The current operational state of the interface. It refers to the state of the MAC interface between the LAN Emulation client and the higher layer.

ifInOctets/ifOutOctets The total number of octets received or transmitted on the interface. For LAN Emulation it refers to the total number of octets received on all the VCCs associated with the emulated LAN interface. It includes octets from circuits that have been torn down since the LAN Emulation client joined the emulated LAN.

ifInUcastPkts The number of packets delivered by the LAN Emulation client to higher layers and not addressed to a multicast or broadcast LAN destination.

ifInErrors The number of inbound packets that contained errors preventing them from being deliverable to higher a layer.

ifInUnknownProtos The number of LAN Emulation PDU packets this client received via the LUNI which were discarded because of an unknown or unsupported LAN Emulation protocol control, IEEE 802.3, Ethernet, or IEEE 802.5 protocol.

ifOutUcastPkts The total number of data packets that higher protocols asked this LAN Emulation client to transmit, and which were not addressed to a multicast or broadcast LAN destination.

ifOutNUcastPkts The total number of data packets that higher protocols asked this LAN Emulation client to transmit, and which were addressed to a non-unicast address.

ifOutDiscards The total number of outbound LAN Emulation PDU packets that were chosen to be discarded even though no errors had been detected to prevent them from being transmitted.

ifOutErrors The total number of outbound LAN Emulation PDU packets that couldn′t be transmitted because of errors. This count includes all types of LAN Emulation PDUs (Ethernet, 802.3, 802.5 and control).

ifInBroadcastPkts The number of data packets delivered by this LAN Emulation client to a higher layer, which were addressed to the broadcast MAC address.

ifOuMulticastPkts The number of data packets that higher protocols asked this LAN Emulation client to transmit and which were addressed to a multicast LAN destination and which were addressed to the broadcast MAC address should be generated for this interface. Default is disabled.

To illustrate the implementation of MIB-II for an IBM 8210 we used the TME 10 NetView MIB browser. The IBM 8210 had only one ATM physical interface and seven internal LAN Emulation clients defined. The MIB data was retrieved for the MSS interfaces and description of its MIB-II interface table (ifDescr of ifTable) (see Figure 153 on page 237).

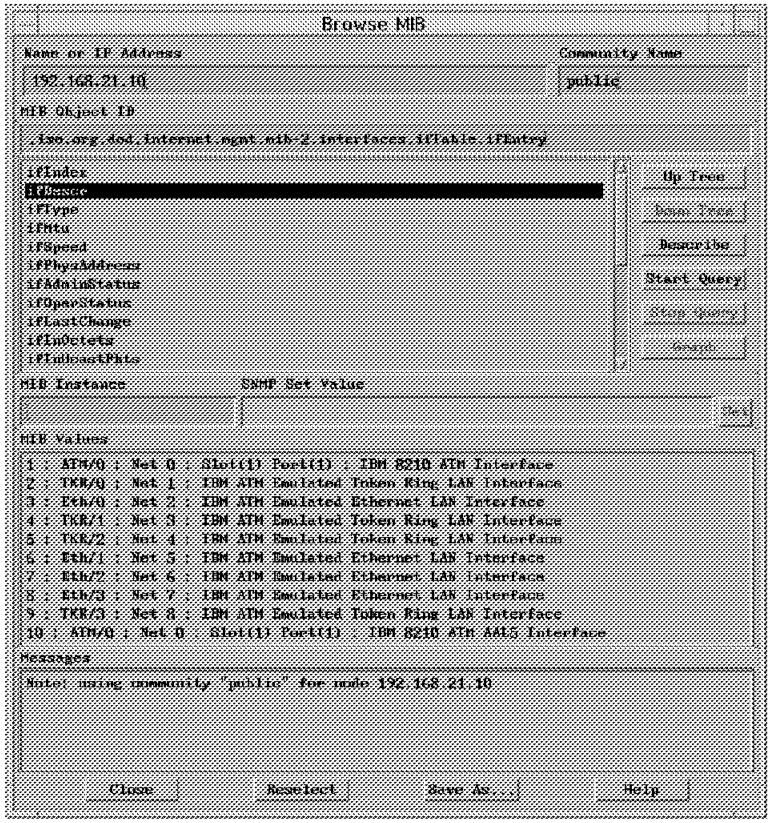

Figure 153. MIB-II Interfaces Description

The information contained in the MIB Values window describes the interface characteristics. the first line shows the physical ATM interface referring to network 0. The subsequent lines refer to each ELAN defined for this ATM device (that is, the logical interfaces). The last line shows the AAL-5 interface information. This AAL-5 interface relates to all interfaces between any LEC and the AAL-5 layer.

These measurements can be found in the LAN Emulation client individual interface with the higher layers. If we look for the same MSS device its physical addresses list ifPhysAddress, we find the list of all the LAN Emulation clients′ MAC addresses (see Figure 154 on page 238).

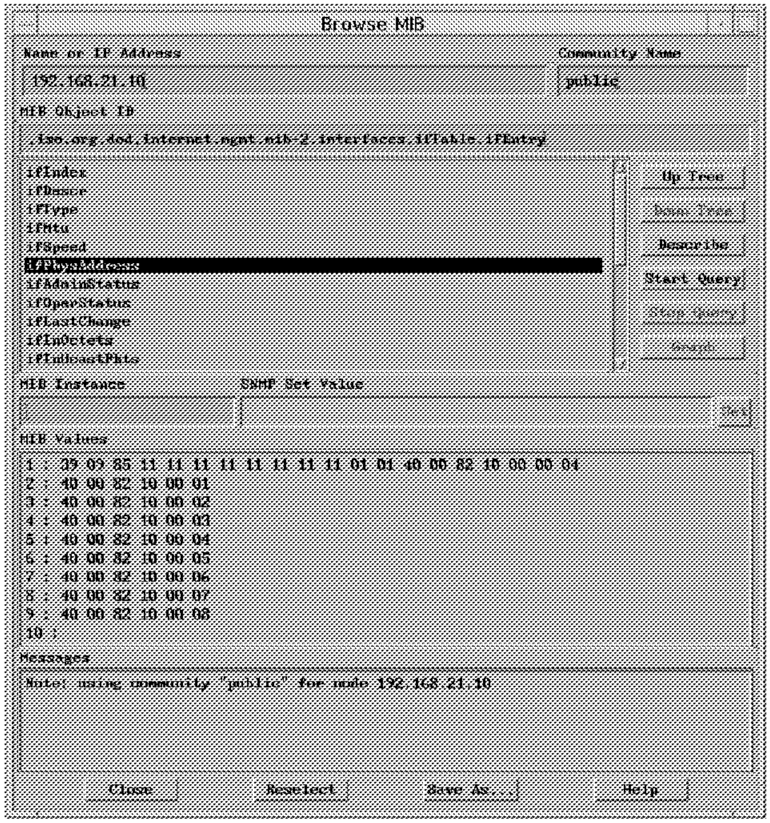

Figure 154. MIB-II LAN Emulation Clients MAC Addresses

This is how we can associate between these two MIB variable instances. The first entry references the physical ATM interface and displays the ATM address of the ATM adapter. Entries 2 though 8 point to instantiated LAN Emulation clients and are their MAC addresses. Higher layer applications utilize this MAC address for networking.

The last entry doesn′t contain any value. That is due to the AAL-5 layer having no sublayer protocol addresses defined.

Note: In most simple LAN Emulation ATM workstations the MAC address is numerically equal to the ESI part of the corresponding ATM address. The LAN Emulation client ATM addresses are not displayed in MIB-II but in the LEC MIB.

B.2 The LAN Emulation Client MIB

The LEC MIB allows the network management application to define and delete LAN Emulation clients. In addition this MIB is used for monitoring the LAN Emulation traffic and SVC failures.

The LAN Emulation Client MIB is organized into the following groups:

The Configuration Group

This group consists of a table containing settable creation, deletion and configuration parameters with one row per LAN Emulation client. Unlike hardware ports, LAN Emulation clients can be created or deleted. The MIB-II (or RFC 1573) interface table doesn′t support row (LEC) creation or deletion.

LAN Emulation creation and deletion tasks are performed through this configuration group. As soon as an LEC instance is created in this table, it′s immediately mirrored in the MIB-II (or RFC 1573) interface table. The following MIB definitions contain descriptions for each of the MIB definitions.

The Statistics Group

This group contains traffic statistics for all the LAN Emulation clients implemented by a given host. There is one row per LAN Emulation client.

The Server Connections Group

This group consists of control and multicast VCC identifiers with one row per client instance.

The ATM Addresses Group

This group lists all the ATM addresses for each of the host′s LAN Emulation client. It consists of a table indexed by the client index and the ATM address.

The Registered MAC Addresses Group

This group lists all the local unicast MAC addresses registered by this host′s LAN Emulation clients. It consists of a table indexed by the client and MAC address.

Let′s have a look at this table for an IBM 8281 ATM bridge (Ethernet) (see Figure 155).

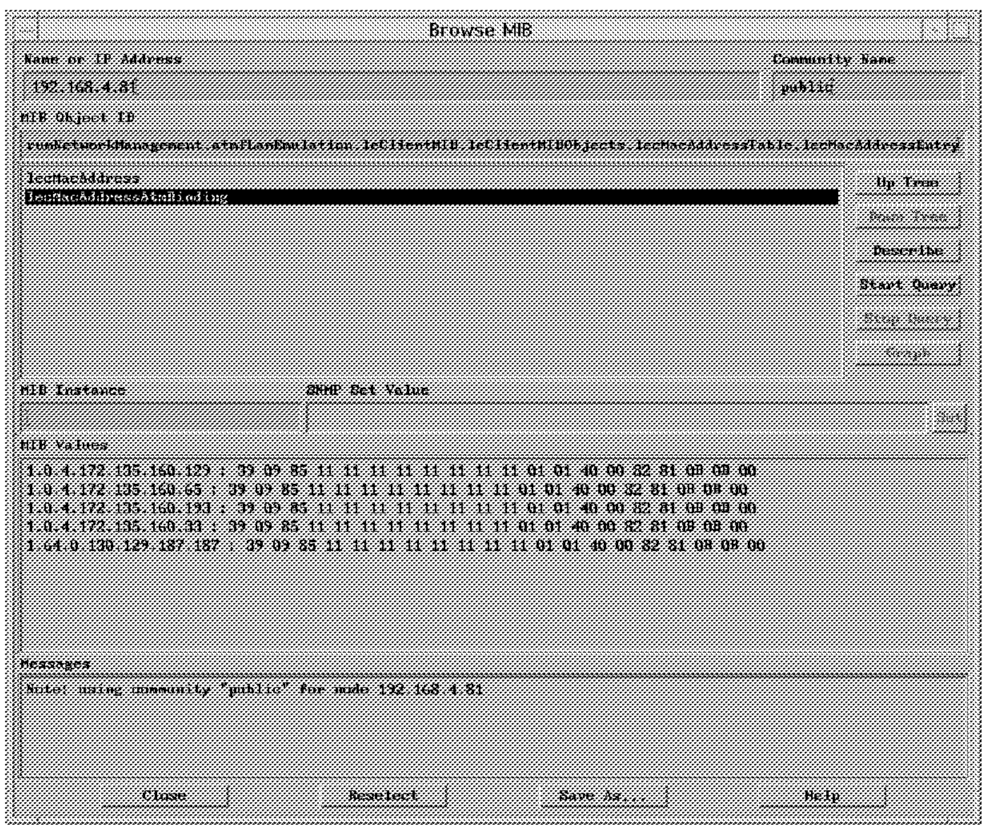

Figure 155. The Local Unicast MAC Addresses of an IBM 8281 ATM Bridge

The bridge has registered all its MAC addresses referring to its legacy LAN ports and the MAC address of its emulated LAN port. All these MAC addresses map the same ATM address. This ATM address is the ATM address of its ATM port.

The Registered Route Descriptors Group

This group lists all the route descriptors registered for this host′s LAN Emulation clients.

The LE_ARP Cache Group - MAC Addresses

This group provides access to a LAN Emulation client′s MAC-to-ATM ARP cache.

The LE_ARP Cache Group - Route Descriptors

This group provides access to an IEEE 802.5 LAN Emulation client′s route descriptor-to-ATM ARP cache.

The Index Mapping Group

This group describes the mapping of the ifIndex values of aflane8023 and aflane8025 interfaces to the lecIndex values of the corresponding LAN Emulation clients. It′s used to correlate information of the LEC MIB with MIB-II interface table information. It consists of a table with one row for each client.

B.3 The LAN Emulation Server MIBs

The ATM interface is specified via the MIB modules for VCCs that are in use by defined servers and also in every server configuration table where the server′s ATM addresses are defined. This enables network management to determine which ATM switch the servers derived their ATM addresses from.

If LAN Emulation servers utilize VCCs to communicate with clients; information about these VCCs can be found in the AToM MIB. LAN Emulation servers provide the indexing for these VCCs so network managers can obtain the attributes of a server VCC from the AToM MIB.

An LECS will use policy rules and policy values recorded in the ELAN MIB to assign LECs to ELANs. As information recorded in the ELAN MIB is used by a LECS, most of the time the ELAN information will be recorded in the host implementing the LECS instance. The ELAN MIB reflects this last point as the ELAN MIB hosts both LECS active component information plus ELAN administrative information. LES and BUS MIBs are likely to be collocated on the same host. Nevertheless the ATM Forum has separated their MIBs to allow independent implementation. Three MIBs will be used when creating a controlled ELAN:

1. The ELAN MIB to configure LECS instance and ELAN
2. The LES MIB to configure the LES instance
3. The BUS MIB to configure the BUS instance

Note: When an ELAN is not controlled by an LECS, all its potential LAN Emulation clients are configured automatically and only the two last steps are used. We discuss these three MIBs in the following sections.

B.4 The ELAN MIB

The ELAN MIB contains a repository of static information used by an active LECS component. In addition the ELAN MIB contains MIB objects allowing a network manager to control and monitor this same LECS.

The static information repository is used by the LECS to assign LAN Emulation clients to a given ELAN on the basis of its LE_CONFIGURE_REQUEST and to append the LE_CONFIGURE_RESPONSE sent back to the clients. It is possible for an ELAN to exist without an LECS; by a client obtaining this information by some other means. If all known implementations rely on LECS instances, the LAN Emulation ATM Forum allows the ELAN MIB to exist without requiring an LECS. For this reason the LECS part of the ELAN MIB is contained in a separate group.

Note: The ELAN MIB provides a means to control ELAN topology by assigning LECs to ELANs, but it doesn′t reflect the current topology of an ELAN. To determine the current topology of an ELAN (which clients have joined which LES), the LES MIB and the BUS MIB must be used.

The ELAN MIB is also divided into groups and tables. The structure is as follows:

The ELAN Administration Group Provides a registry for the LEC assignment policy types.

The ELAN Configuration Group Provides configuration information for emulated LANs.

The LECS Configuration Group Enables network managers to control, configure and monitor the LECS. It′s divided into several tables.

The LECS Statistics Group Contains one table, which is the LECS Statistics table.

The ELAN Configuration Group The ELAN group provides configuration information for ELANs.

ELAN Configuration Table Its MIB identifier is elanConfTable. This table contains all emulated LANs this agent manages. An ELAN is defined by an ELAN name, a set of TLVs, a LAN type and a maximum frame size. This table information is used by the LECS in its LE_CONFIGURE_RESPONSEs to LAN Emulation clients.

ELAN LES Table Its MIB identifier is elanLesTable. This table lists all LESs associated with each ELAN specified in the elanConfTable. This table contains the ATM address of the LESs and is indexed by both the ELAN index (elanConfIndex) and the LES index within this ELAN (elanLesIndex). To illustrate this we interogated the MIB for an IBM 8210 device (see Figure 156 on page 242).

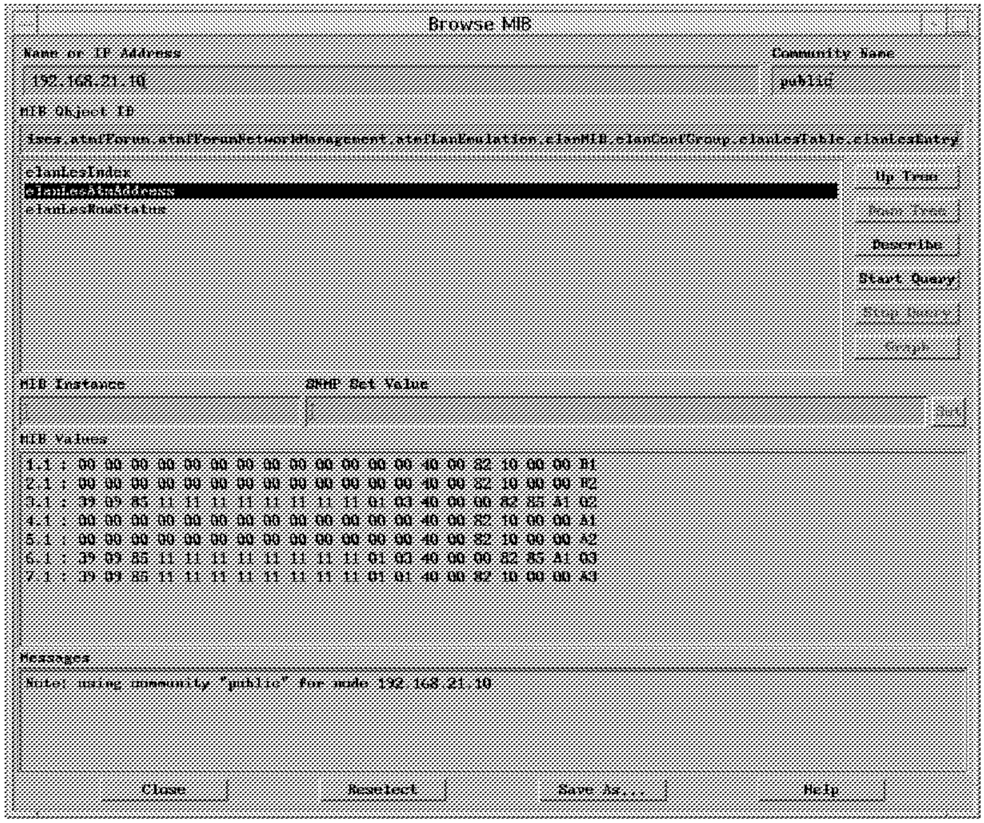

Figure 156. The ELAN LES Table

The ELAN Policy Table Its MIB identifier is elanPolicyTable. This table describes policies currently in use for assigning LAN Emulation clients to an ELAN but not policy values. The policy table contains policy rules and policy priorities that are used as a general hierarchical scheme of evaluation.

This selector enables different LECSs to operate different sets of policies if these two LECSs are to use the same ELAN administrative information.

The LEC Assignment Table by ATM Address Its MIB identifier is elanLecAtmAddrTable. This table is used to assign an LEC to an ELAN by ATM address specified by the LEC ATM address or portion of an ATM address. The ATM address (or portion) is used by the LECS to determine the ELAN membership (see Figure 156).

Using the MIB browser we found that five entries are prefixed by 9.1, each describing the LEC ATM address that the LECS will assign to the LES instance referred by 9.1 (see Figure 157 on page 243). 9.1 corresponds to the elanLesTable LES ATM address (elanLesAtmAddr) 39.09.85.11.11.11.11.11.11.11.11.01.01.40.00.82.10.00.00.A1.

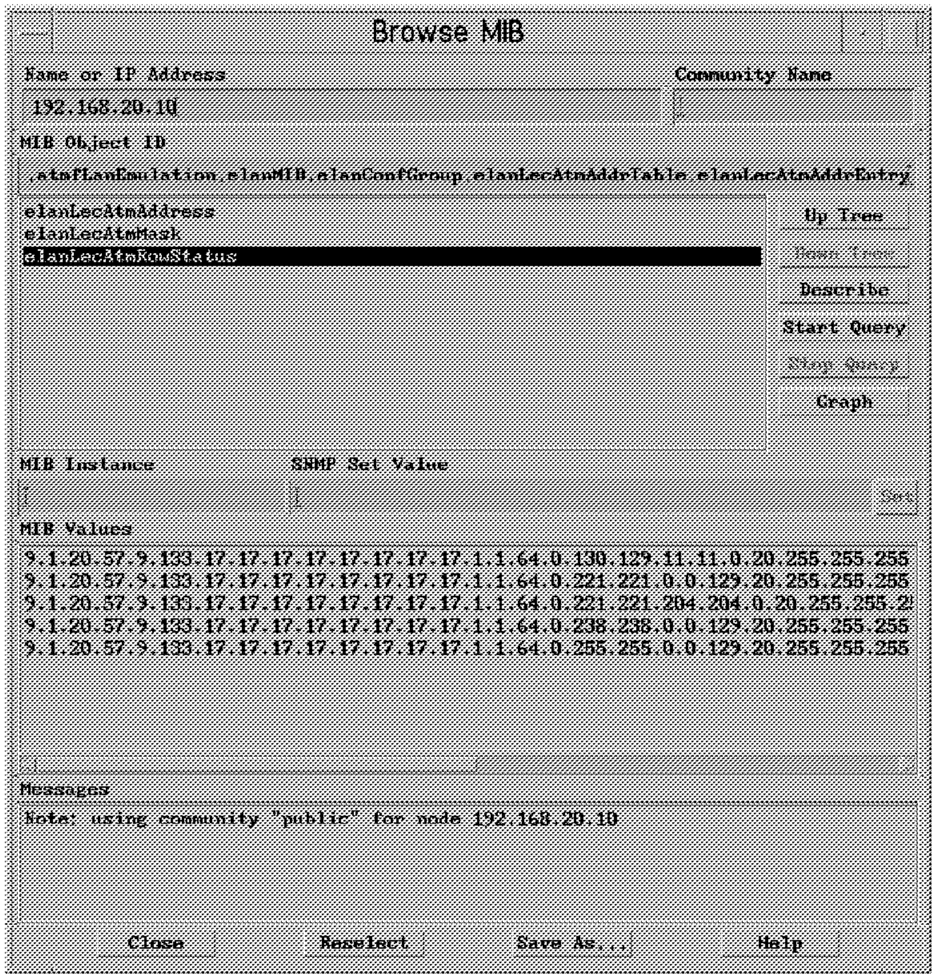

Figure 157. The LEC Assignment Table by ATM Address

LECS Configuration Group This group enables the network managers to create, delete, configure, and monitor LECSs. It also provides configuration information on TLVs (type, length, value) entries to be used in LE_CONFIG_RESPONSEs. This group includes four tables.

LECS Configuration Table MIB identifier: lecsConfTable. This table contains the configuration and status information for all the LECSs managed by this agent.

This table can also be used to create, delete or configure an LECS. The object lecsAtmIfIndex provides the number of the ATM interface on which the LECS is listening for LE_CONFIGURE_REQUESTs.

LECS ELAN Table MIB indentifier: lecsElanTable. This table contains the mapping between ELANs and LECSs. When an LECS is deleted from the lecsConfTable all entries associated with this entry will also be deleted. This table lists which ELANs are managed by which LECS.

LECS Configuration Group This group contains only one table (lecsStatsTable). This table is made of counters providing information about the LE_CONFIGURE_REQUESTs. One counter displays the number of successful LE_CONFIGURE_REQUESTs; all others the number of failed LE_CONFIGURE_REQUESTs based on a per category of failure.

LECS Fault Group This group provides fault information for LECSs. The network manager can enable or disable the error logging capability of an LECS. The enabled LECS will log the error events until the maximum number of error log entries are reached. The logged events are saved in the LECS ErrorLog table.

LECS Error Log Control Table MIB identifier: lecsErrCtlTable. This table is an extension of the lecsConfTable and is used to control error logging capability on an LECS. The network manager can enable or disable error logging for a particular managed LECS. It can also reset the error log.

LECS Error Log Table MIB identifier: lecsErrLogTable. This table contains all the error logs of the LECS instances enabled in the lecsErrCtlTable. Each entry describes when the error occurred, the nature of the error, and the ATM address of the client whose LE_CONFIGURE_REQUEST resulted in the error. The lecsErrLogIndex ranges from 2 to 32 minus 1 down 1. It is assigned consecutively in the descending order. The network manager can easily retrieve the most recent N entries by using the get-next on the value of this object. The entries after 1 are discarded.

B.5 LES MIB

This MIB may be used to determine the distribution of the LECs among LESs and to create, configure and monitor LESs. The LES MIB is divided into the following groups:

- The LES Configuration Group provides configuration and topology information through six tables.
- The LES Statistics Group provides various counters for each LES and contained in the LES statistics table. It contains only one table.
- The LES Fault Management Group provides and logs LES error information.

The LES Configuration Table This table contains all the managed LAN Emulation Servers and is used to create, delete, and configure LES instances, unlike the ELAN MIB elanLesTable where only the LES ATM address was entered (see Figure 156 on page 242). This table describes the active LES component. The object lesAtmAddrSpec specifies an ATM address that, with the ATM address mask, determines a portion of the ATM address that the LES on the designated ATM interface will use to derive the actual ATM address from the network or ILMI.

The ATM address is specified in the object lesAtmAddrActual, which is used to receive ATM ARP requests. The object lesElanName gives the name of the Emulated LAN for which this LES is providing service. This object may be used to identify the ELAN the LES is in.

Note: These LES ATM addresses are the ATM addresses of the active LESs implemented on this agent.

The LES VCC Table This table lists all the control distribute VCCs used by the LES to distribute control traffic to the participating LECs. The control distribute VCC can be either point-to-point or point-to-multipoint.

The LES BUS Table This table contains the BUSs paired with the LESs found in the lesConfTable. The BUS handles data sent by the LEC to the broadcast MAC address (FFFFFFFFFFFF), all multicast traffic, and initial unicast MAC frames that are sent by an LEC before the data direct target ATM address has been resolved. This table is indexed by the lesIndex (see Figure 158 on page 245). This BUS ATM address will be sent back to LECs after they have sent an LE_ARP_REQUEST to the LES for the broadcast MAC address.

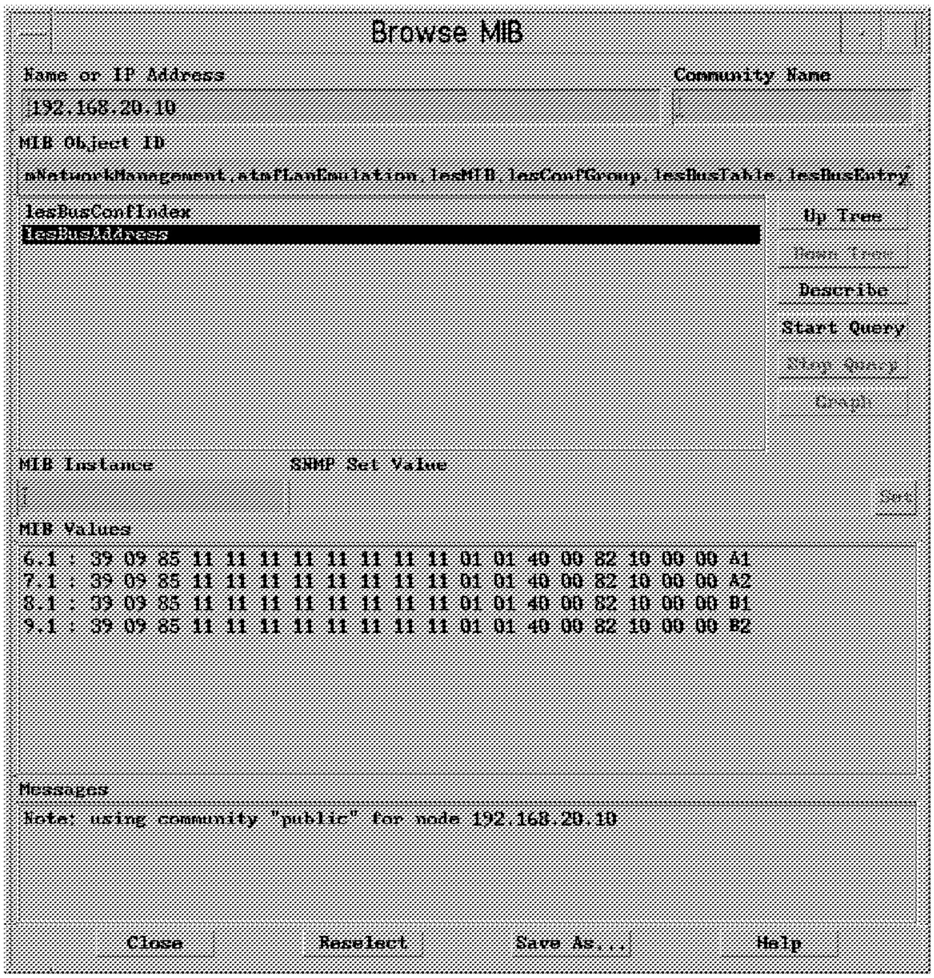

Figure 158. The BUS ATM Addresses

LES ARP Table by MAC Address The MIB indentifier is lesLeArpMacTable. This table provides access to the LES MAC-to-ATM address table. It contains entries for unicast MAC addresses and for the broadcast MAC address (FFFFFFFFFFFF). An entry for the broadcast MAC address will have the ATM address of a BUS. When the entry is for a unicast MAC address the corresponding ATM address will be for an LEC. A network manager can write entries in this table although most of the time this table is filled up through LE_(JOIN,REGISTER)_REQUESTs.

The LES-LEC Topology Table MIB identifier: lesLecTable. This table lists all LAN Emulation clients serviced by LESs specified in the lesConfTable. This table can be used to retrieve the topology of an ELAN. An entry in this table is created by the agent when an LEC registers successfully with the LES. The lesLecCtlDirectVpi and lesLecCtlDirectVci objects can be modified by the network manager if

PVC is used. Let's use the MIB browser again to list the LES-LEC topology table LECs ATM addresses (see Figure 159 on page 246).

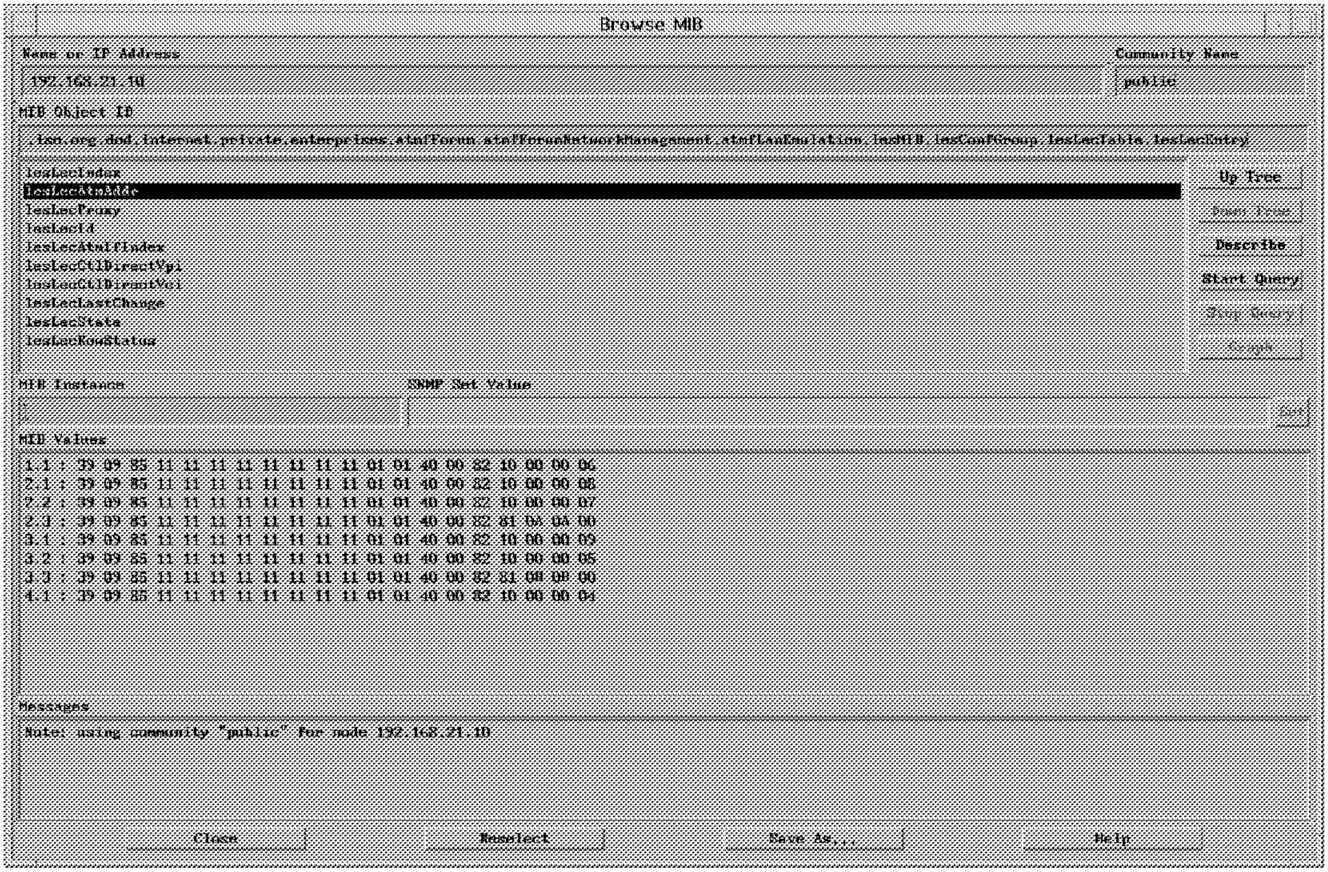

Figure 159. The LES-LEC Topology Table

LESs 6, 7, 8 and 9 currently service LECs. LESs 9 and 7 service two LECs (1, 2).

The LES Error Log Control Table The MIB identifier is lesErrCtlTable. This table is used to control the error logging capability of a LES. The network manager may enable or disable error logging on a particular LES managed by the agent. It can also reset the error log of an LES. The object lesErrCtMaxEntries describes the maximum number of errors an LES can log. If this object is set to 1, then the LES will only save the last error event. The object lesErrCtlLastEntry gives a pointer to the last error log saved by an LES in the lesErrLogTable.

The LES Error Log Table The MIB identifier is lesErrLogTable. This table contains all the error logs of the LES instances enabled in the lesErrCtlTable. Each entry describes when the error occurred, the nature of the error, and the ATM address of the client whose LE_(JOIN,REGISTER)REQUEST resulted in the error. The lesErrLogIndex ranges from 2 to 32 minus 1 down 1. It is assigned consecutively in descending order. The network manager can easily retrieve the most recent N entries by using the get-next on the value of this object. The entries after 1 are discarded.

B.6 The BUS MIB

The BUS MIB enables network managers to create, delete, configure and determine the current status of BUSs and the topology of ELANs served by BUSs. This MIB is divided into the following groups:

BUS Configuration Group This group includes the busNextId, the BUS Configuration table, the BUS VCC table and the BUS-LEC Topology table. The busNextId provides the network manager the next available index used to create a BUS instance.

BUS Configuration Table MIB identifier: busConfTable. This table contains all the BUS instances this agent manages. There can be more than one BUS per ELAN. Conversely a BUS can service only one ELAN. This table allows a network manager to create, delete, activate, de-activate, and configure BUS instances in this agent. As far as the BUS ATM address is concerned, the same principles apply to the BUS as to the LES and LECS; three objects deal with the notion of BUS ATM addresses: the busConfAtmAddrSpec, the busConfAtmAddrMask and the busConfAtmAddrActual. A busConfElanName allows network managers to reference directly the ELAN serviced by the BUS instance. The BUS handles data sent by an LEC to the broadcast MAC address (FFFFFFFFFFFF), all multicast traffic, and initial unicast MAC frames that are sent by an LEC before the appropriate data direct target ATM address has been resolved.

BUS VCC Table MIB identifier: busVccTable. This table contains all the multicast forward VCCs used by the BUS to forward multicast traffic to the participating LECs. The multicast forward VCC can either be point-to-point or point-to-multipoint. This table is read-only if SVCs are used and writable if PVCs are used.

BUS-LEC Topology Table MIB identifier: busLecTable. This table contains the BUS and the actual LECs being serviced by the BUS. It can be used as the actual mapping between the BUS and the LECs. This table provides information for multicast send VCCs between the BUS and the LECs. Objects busLecMcastSendAtmIfIndex, busLecMcastSendVpi and busLecMcastSendVci can only be modified if PVC is used.

BUS-LEC Statistics Table MIB identifier: busLecStatTable. This table contains all LEC counters the BUS maintains, and can be also be used to retrieve all LECs to which a BUS is providing service. The counters point to the number of frames received, forwarded and discarded by the BUS.

BUS Fault Management Group This group provides fault management information for managing a BUS. The network manager can enable/disable the error logging capability of a BUS. The enabled BUS will log the error event until the maximum number of error log entries is reached. The logged events are saved in the BUS Error Log table. This group contains two tables.

BUS Error Log Control Table MIB identifier: busErrCtlTable. This table is used to control the error logging capability of a BUS. The network manager may enable or disable error logging on a particular BUS managed by the agent. It can also reset the error log of a BUS. The object busErrCtMaxEntries describes the maximum number of errors an LES can log. If this object is set to 1, then the BUS will only save the last error event. The object busErrCtlLastEntry gives a pointer to the last error log saved by an LES in the busErrLogTable.

The BUS Error Log Table MIB identifier: busErrLogTable. This table contains all the error logs of the BUS instances enabled in the busErrCtlTable. Each entry describes when the error occurred, the nature of the error, and the ATM address of the client on whose multicast send VCC the error occurred. The busErrLogIndex ranges from 2 to 32 minus 1 down 1. It is assigned consecutively in descending order. The network manager can easily retrieve the most recent N entries by using the get-next on the value of this object. The entries after 1 are discarded.

Appendix C. Special Notices

This publication is intended to help service professionals install and configure the Nways Campus Manager applications. The information in this publication is not intended as the specification of any programming interfaces that are provided by Nways Campus Manager for AIX. See the PUBLICATIONS section of the IBM Programming Announcement for Nways Campus Manager for AIX 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 information about non-IBM (″vendor″) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. 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.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

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

AIX	APPN
C Set ++	IBM
NetView	Nways
OS/2	POWER Gt4e
RISC System/6000	TURBOWAYS

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 D. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

D.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How to Get ITSO Redbooks" on page 253.

- *IBM 8260 As a Campus ATM Switch*, SG24-5003-00
- *Inderstanding and Using the MSS Server*, SG24-4915-00
- *Campus ATM Network Management Guidelines*, SG24-5006-00

D.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

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
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
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042

D.3 Other Publications

These publications are also relevant as further information sources:

- *NWAYS Campus Manager ATM for AIX*, G325-3633
- *NWAYS Campus Manager LAN for AIX*, G325-3632

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at http://www.redbooks.ibm.com.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO: type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Web Site on the World Wide Web**

  http://w3.itso.ibm.com/redbooks

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

Redpieces

For information so current it is still in the process of being written, look at ″Redpieces″ on the Redbooks Web Site (http://www.redbooks.ibm.com/redpieces.htm). 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.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** — send orders to:

	IBMMAIL	Internet
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29570	Calgary, Alberta T2P 3N5	DK-3450 Allerød
Raleigh, NC 27626-0570	Canada	Denmark
USA		

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1)001-408-256-5422 (Outside USA)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** - send note to `softwareshop@vnet.ibm.com`

- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to `announce@webster.ibmlink.ibm.com` with the keyword `subscribe` in the body of the note (leave the subject line blank).

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.htm`). 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.

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name   Last name

Company

Address

City   Postal code   Country

Telephone number   Telefax number   VAT number

- Invoice to customer number

- Credit card number

Credit card expiration date   Card issued to   Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

N

O

P

R

S

T

U

V

W

ITSO Redbook Evaluation

ELAN Management Using Nways Campus Manager for AIX
SG24-4821-00

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.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@vnet.ibm.com

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!)

____

____

____

____

____

Printed in U.S.A.

SG24-4821-00