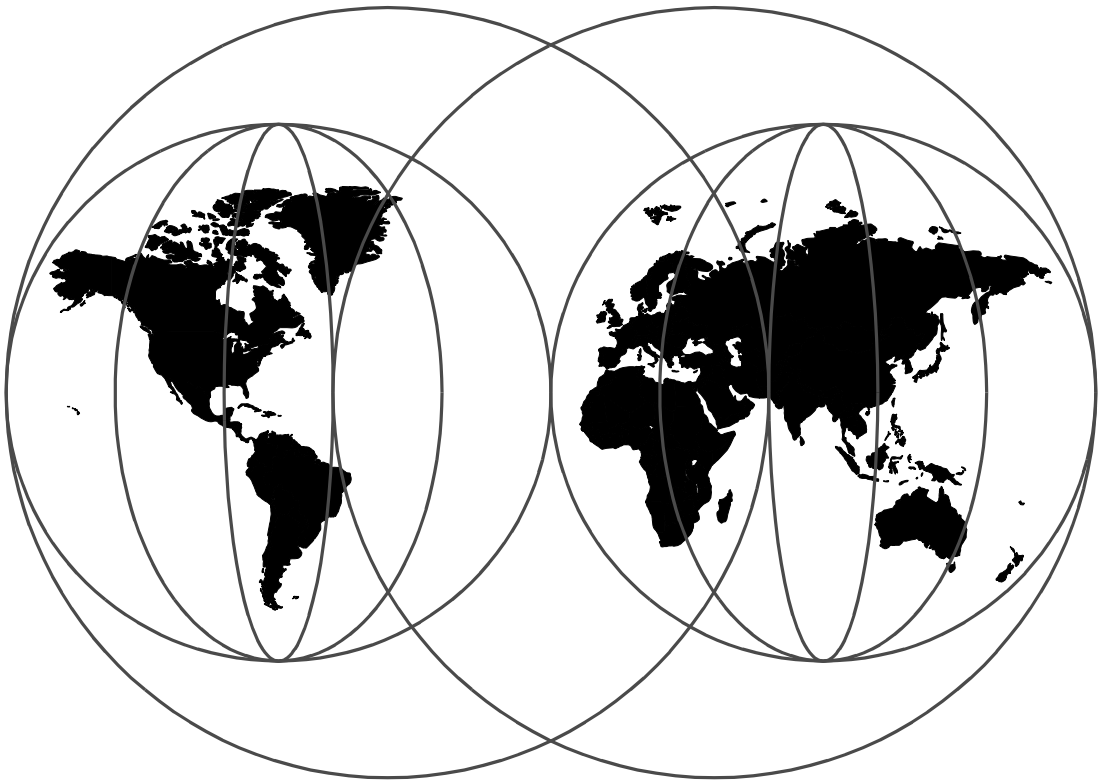
IBM

Network Management Using Nways Management Applications

Paul Fearn, Jim Abercrombie, Thomas Alexandra, Andrew Palmer,
Bernie Newnham, Sontiya Nujeenseng, Kevin Treweek



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5302-00

International Technical Support Organization

SG24-5302-00

Network Management Using Nways Management Applications

January 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix D, “Special Notices” on page 417.

First Edition (January 1999)

This edition applies to Nways Manager Version 1.2.2, Nways Workgroup Manager Version 1.1.1 and Tivoli NetView Version 5.1 for use with the AIX and Windows NT Operating System.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JN9B Building 045 Internal Zip 2834
11400 Burnet Road
Austin, Texas 78758-3493

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

Contents

Figures

Tables

Preface

This redbook will help you install, tailor and configure the Nways Management applications and Tivoli NetView for the AIX and NT platforms, in order to provide network management solutions for the IBM networking devices.

This book uses practical examples based on typical network topologies to illustrate how the Nways applications can be utilized to provide management functions for status monitoring, configuration management, performance management and fault management. In addition the book takes an in-depth look at the Java management components and also shows how to integrate with additional management software such as RouteVision, Remote Monitor and the 8210 and 2216 configuration applications.

This book provides a valuable addition to the product documentation when implementing a network management solution, and is a good reference for I/T architects designing such solutions.

Chapter 1 contains an introduction to the project and an outline of the design and implementation phases that were performed.

A knowledge of 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 International Technical Support Organization, Raleigh Center.

Paul Fearn is an Advisory ITSO Representative working as a project leader at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on all areas of Tivoli and network management applications. Before joining the ITSO two years ago, Paul worked in the global services division in the UK, working on large customer engagements providing consultancy for systems and network management.

Jim Abercrombie is a Networking Specialist working for IBM in Scotland. He has 25 years of experience in IT, six in networking. He holds a BA degree in Mathematics and Physics and an MSc in Computing for Commerce and Industry, both from the Open University in the UK. His areas of expertise include network management, LAN and ATM. He is currently involved in the installation of two major ATM networks in Scotland.

Bernie Newnham is a Network Management Consultant in UK. He has three and a half years of experience in the systems and network management field. He has thirteen years real-time experience. His areas of expertise include UNIX and NT-based LAN management design, implementation and event management and correlation.

Kevin Treweek is a Network Consultant in South Africa. He has 11 years of experience in the WAN and LAN network design field. He holds a degree in Electrical Engineering from the University of Witwatersrand. His areas of expertise include ATM and campus network design, specifically in the large corporate environments. He lectures extensively on all network related subjects in his home country.

Thomas Alexandra is a Networking Specialist in Abu Dhabi, United Arab Emirates. He has eight years experience in campus networking, and currently works for the Product Support Services department providing both pre-sales and post-sales support for the entire IBM networking product line. He holds a Bachelor's degree in Computer Science from Cyprus College in Cyprus, and is currently undertaking an MBA in IT management. His areas of expertise include multiprotocol networking with Ethernet, token-ring, ATM, WAN, and network management, along with varied activities such as network design, project management, implementation, training, and troubleshooting. He is also an IBM certified Networking Solutions Engineer III, and a Certified Internet specialist.

Andrew Palmer is a Network Support Specialist within the PSS organization in IBM UK. His main responsibility is the post-sales support of IBM's network management products for the Nways WAN and Campus solutions. Andrew also provides pre-sales support and technical education within this arena and work that has involved a lot of foreign travel. Andrew has ten years of experience in IT, the last seven in networking. His main areas of expertise are Network Management and the Broadband WAN environment. He is currently involved with several network management implementation and customization projects in the UK.

Sontiya Nujeenseng is a networking specialist with IBM Thailand.

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

John Parker
The Editing Team
International Technical Support Organization, Raleigh Center

Carol Sirkis
Mark Frank
Mike Zibiae
Sallie Matlack
IBM Raleigh

Jim Kellock
IBM USA

Garry Rawlins
IBM Networking Division

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 431 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 `redbook@us.ibm.com`

Chapter 1. Introduction

This chapter provides a set of guidelines and considerations for the implementation of an IBM Nways network management solution and discusses what issues we faced while planning for such an installation.

No two customer network management scenarios are exactly the same. Each customer has their own unique management challenges and requirements that have to be addressed. However, with the aid of this section, certain basic design principles may be followed to ensure that a smooth start to implementing an IBM Nways network management solution can be achieved.

We have provided guidelines on what to consider and what issues you might face when designing a management solution. Next we look at how to select the management tools required to provide the management services.

Once we have installed the software we show, using examples, how to access the management information for status monitoring, configuration, performance and fault management. In addition we decided to document the Java Performance Manager and RouteVision in separate chapters.

The fundamental information we require before initiating the design stages are:

- What are the management considerations?
- What type of information do we need to obtain from the customer?

Also covered in this chapter is the network management design section that covers our approach to the implementation.

1.1 Network Management Considerations

Careful consideration and attention must be given to the planning stage of a proposed network management solution.

A secure and stable management platform that addresses the issues listed below will provide the customer with the optimum design that will be most beneficial for a network management scenario.

- Ease of use

  Working with the management platform is a complex and elaborate procedure. Operation of the management tools should be effortless and uncomplicated.

- Simplified installation

  The user should not experience long and tedious procedures when installing new or additional hardware into the network.

- Reduced maintenance

  A managed network should reduce the amount of maintenance required to keep the network operational.

- Enhanced network performance

  Improved network response times for existing applications and users.

- Scalability

The installed solution must be able to cater for the support of future technological enhancements for example, ATM.

- Investment protection

  The management platform must be able to cater for the co-existence with existing hardware for example, network adapters and other vendor's hardware.

- Streamlined network management

  Shorten and disentangle cumbersome operations procedures that previously limited the performance of the management solution.

- Reduced cost of ownership

  The overall cost of ownership should be reduced by diminishing network down times and outages through more expeditious diagnostics, alarm and event management.

- Minimal complexity

  In the past, management solutions have frequently been too confusing and complicated to operate, and subsequently have not been utilized to their full potential.

- Access to information

  The operation personnel need access to the information stored for each device, whether this is configuration or performance data.

- Reporting

  Report on asset, performance and availability information held in the databases.

- Serviceability

  The management applications must be able to be upgraded with little or no disruption to the operational personnel

With these considerations in mind we look at the information that we need before we can design the network solution.

1.2 Information Required

In order to be able to commence and eventually invoke a network management solution for a customer, certain essential and imperative information is required. This technical information, in conjunction with certain assumptions and customer preferences, is needed in order to be able to install the required solution.

Usually the customer should have records, documentation and network diagrams of their installed base; however this is not always the case. Once the criteria has been determined the following prerequisites have to be obtained from the customer with the use of pre-installation tables.

1.2.1 Installed Hardware

Different methods are used to configure devices. Some devices only support out-of-band configuration using a console connected to an RS232 port on the device, while other devices also support Telnet access.

For devices that require a direct connection, the location and contact information of the device and a terminal or emulator software, which can act as a console will be required. It is recommended that a null modem cable with support for both 9-pin and 25-pin connections is available.

1.2.1.1 Network Adapters

Not only the physical characteristics of the network adapter for the management host has to be validated. The following also has to be validated:

- Multimode fiber (MMF)
- Single-mode fiber (SMF)
- Twisted pair (TP)

Also the connectivity speed (for example, 10/100Mbps or ATM 155Mbps) of the network adapter for the management platform has to be verified.

1.2.1.2 Software and Firmware Levels

The Nways Manager applications have prerequisite software, firmware versions and levels that have to be loaded onto:

- Hosts
- Network adapters
- All network-related hardware

The correct levels allow the managers to communicate with these devices.

1.2.1.3 Microcode Levels

To be able to manage network devices with IBM's Nways Management platforms, both AIX and NT, validation of the microcode levels of the hardware devices already installed in the network needs to take place. If the installed levels of microcode are not supported by the Nways Managers, then these levels have to be updated immediately.

Information on the supported levels of microcode can be acquired by referring to Appendix B, "Microcode Levels Supported by Nways Manager" on page 401 of this document.

Also this information is on the Internet site at:

`http://www.networking.ibm.com/cma/Mcodespt.html`

The latest microcode for almost all IBM's products can be obtained from the Internet at:

`http://www.networking.ibm.com/netsupt.html`

1.2.2 TCP/IP Configuration

Information regarding TCP/IP addressing is required. Typically the following addresses need to be acquired:

- Hosts
- Default gateway
- Routers, switches and hubs

Also the Network Management Station (NMS) must be able to get to each of the managed devices in the network. This means that you may need:

- DNS
- Static routes
- Modifications to be made to the TCP/IP configuration

1.2.3 Community Name

To be able to manage network devices, Nways managers must be able to communicate with their SNMP agents. This means that the managers must read and write to the device MIBs and receive traps from the agents. Security is provided by the community names.

When a manager issues an SNMP Get (read) or Set (write) command to a device, it passes a community name with the request. The agent checks the community name to see if it is defined and to verify the level of access.

1.2.4 SNMP Connectivity Requirements

In order to have SNMP connectivity between the Nways manager workstation and a hardware device, the following must be true. You can use this as a checklist if you ever lose or cannot gain SNMP connectivity:

- Ability to ping all network devices successfully.
- The community name set in the Nways manager must match one of the community names set in the device.
- If you are using Nways manager to perform an action on the hardware device that requires write access such as reset, the community name set in the Nways manager application must exist in the hardware device with read-write authority.

For some hardware devices, the community name setup allows you to specify the IP address of workstations that are to be granted access using that community name. In this case, you must either specify the IP address of the Nways manager workstation or all that will allow access by any workstation.

1.2.5 Cabling Infrastructure

The customers implemented network connectivity for example:

- Ethernet
- Fast Ethernet
- FDDI
- Token-ring
- ATM
- Gigabit Ethernet

This will affect the choice of the network adapter that is installed in the proposed management hardware platform. Not all network topologies are supported by IBM’s management hardware platforms. So the network connectivity and topology must first be determined before a management platform can be implemented.

1.2.6 Geographical Site Locations

Not all management implementations are limited solely to a Campus network. Many customer networks traverse wide area networks (WANs).

While SNMP update traffic has minimal impact on the bandwidth utilization of WAN links it never the less must be factored into the equation. Bandwidth reservation systems such as IBM's BRS running in IBM's MRS routing software suite can be used to prioritize WAN network traffic. This insures that management traffic will not interfere with customer payload traffic.

1.2.7 Required Customers Skills

The customer requires a base level of skill prior to the installation of the Nways Manager by an IBM service specialist. It is essential that the customer has the available skills to be proficient in both AIX and NetView for AIX. In addition to these skills RDBMS, TCP/IP, network hardware concepts and performance management are also important.

1.3 Network Management Design - Our Approach

This section focuses on the actual management requirements. Here we show how we can select the management applications we use and for what purpose. These tables include information such as:

- The managed devices and resources
- The management functions required
- The events we receive from the hardware

We created this process based on experience from previous implementations of the Nways and NetView management tools.

1.3.1 Devices to Be Managed

We started by building a list of the managed devices. Table 1 on page 5 shows a sample table for the managed hardware device the 8260.

Table 1. List of Managed Devices

Device	Component	Subnet	Microcode Levels
IBM 8260	CPSW	9.14.104	Vx.x.x

This table should also include future hardware that may be added to the network.

1.3.2 Type of Management Required

The next step was to create a table containing the managed devices. For each of these devices we addressed the main areas of management. The areas we focus on are:

- Availability
  - Status reporting
  - View MIBs
  - Graphical representation of the device
- Configuration

    - Perform configuration changes on device
    - Keep log of changes made to a device
- Performance Monitoring
    - Monitor performance MIBs on device
    - RMON
- Fault
    - Receive traps
    - Perform actions

The first step was to decide if we need to provide the functions above for all the devices we are to manage. Some considerations are:

- Monitored availability from the management station
- Faults will be shown on the management station
- Ability to configure the device from the management station
- Performance monitoring from the management station

We could extend this table even further to include additional management disciplines such as:

- Problem management
- Change management
- Capacity planning
- Service level agreements

Depending on the customer requirements you may need to break down the table event further to include the specific device components. For instance the 8260 may include each blade, such as a CPSW.

1.3.3 Management Software Requirements

To meet the defined requirements we must understand the capabilities of the management tools. The tools can provide a comprehensive list of functions for the Nways devices. Based on our criteria we can create a list of the tools that we will implement for the management requirements. An example of this is shown in Table 2 on page 6.

Table 2. Example Software Management Tool Selection Table

Device/Resource	Availability	Fault	Configuration	Performance
8260				
ATM	NetView	NetView	JMA/HUB Man.	JPM

The resources can contain protocols (IP or IPX) or device components (ATM switch module in an 8260).

1.3.4 Event Management

Event management is critical to the overall management of a network. Some of the considerations here are as follows:

- What and where are the event sources?
- What are the filtering requirements?
- Where will these events be filtered?
- What thresholding do we need?

- What event correlation is required?
- Which operator needs to see which events?
- What information can we see from the network events?

The 8260 events will require customization in order to allow the operators to handle the events from the 8260. The number of events is in excess of 200 so we need to perform some event handling.

The first thing we did was to sort through the events and assign a filter flag to the less important events, that is, any events that are sent to the events console that will not be acted on.

Also we added a column stating whether this event should be considered for correlation with other events for example, whether a port up will be correlated with port down.

Chapter 2. Product Overview

This chapter provides an overview of the management products that are used throughout this redbook. Nways Manager for AIX provides the functions to effectively manage medium-to-large, LAN-based campus networks, including high-speed backbones built with ATM and LAN switches. The Nways Manager for AIX takes advantage of Tivoli NetView for the management of LAN topologies, fault and event recording and error logging.

Note

The Nways Manager for AIX order number (also available as SK2T-0420) is the 60 day time-bombed code and is a pre-requisite to the ordering of the licenses for the components of LAN, ATM, ReMon and Traffic. Nways Manager for AIX is simply a name of the package and is not a product itself. The product is comprised of the four components.

The management tools that can be used and are referred to in this book are shown in Table 3 on page 9.

Table 3. Software Tools

Application	Version
Nways Manager for AIX	1.2.2
Campus Manager-LAN	3.3.2
Campus Manager-ATM	3.3.2
Remote Monitor	2.1.2
Traffic Monitor	1.1
Tivoli NetView with Tivoli Framework 3.6	5.1
Nways RouteSwitch Network Management Suite	3.2
MSS Configuration Tools	2.1 PTF 1
MRS Configuration Tool	3.1 PTF 2
Nways Workgroup Manager	1.1.2

The next sections provide a brief overview of the applications. Further information can be found at:

`www.networking.ibm.com/netprod.html`

2.1 Nways Manager for AIX

IBM Nways Manager for AIX consists of four components that are included on a single CD-ROM. The Nways Manager for AIX components include:

- **Campus Manager LAN:** The Campus Manager LAN component provides graphical device-management applications for the various SNMP-enabled IBM networking devices (including the IBM ATM devices formerly included in the Campus Manager ATM product). This component does the following:
  - Enables graphical management of over 30 different IBM hubs, hub modules, concentrators, routers, bridges and switches on Ethernet and token-ring LANs.
  - Provides Java Web-based device management support to manage IBM and non-IBM SNMP-enabled devices from the intranet and the local AIX workstation.
  - Provides Java-based performance management to collect and maintain performance data. Customers can create customized performance graphs and reports or take advantage of the library of existing performance reports for IBM and non-IBM devices for problem solving and analysis.
  - Supports large networks through the use of Java-enabled, distributed intelligent agents, which off-load the polling of performance information from the manager workstation, freeing bandwidth across WAN links.
  - Runs on Tivoli NetView for AIX.
- **Campus Manager ATM:** The Campus Manager ATM component provides easy-to-use, efficient management for ATM networks, including virtual networks formed from Emulated LANs (ELANs). This component does the following:
  - Automatically discovers, maps and monitors ATM Forum-compliant devices in the network
  - Manages switched virtual networks including ATM Forum-compliant ELANs
  - Supports LAN Emulation (LANE) including automatic discovery of LAN Emulation Servers (LESs), LAN Emulation Clients (LECs), proxy clients (in LAN switches/bridges) and legacy LAN devices assigned to the VLANs
  - Runs on Tivoli NetView for AIX
- **Remote Monitor:** The Campus Manager Remote Monitor (ReMon) component, in conjunction with RMON- and RMON-2 (ECAM) agents, provides remote analysis of token-ring and Ethernet LANs. This component does the following:
  - Supports remote network performance monitoring for token-ring and Ethernet LAN segments
  - Takes advantage of the ECAM (RMON-2) capabilities to provide address translation, protocol distribution and protocol-matrix analysis of Layer 3 or higher protocols within the network
  - Runs natively on the AIX operating system
- **Traffic Monitor:** The Traffic Monitor component provides the ability to graphically display and manage end-to-end connection traffic in the network. This component does the following:
  - Performs trend analysis and network troubleshooting
  - Monitors network performance and enforces policies regarding business and non-business use of the network

- Provides network tuning based on real application usage patterns by focusing on the traffic for a particular workgroup, VLAN, subnet or organization
- Runs natively on the AIX operating system

The new features are discussed in the next section.

2.1.1 Nways Manager Version 1.2.2

With the new release of Nways Manager for AIX the following new features are available with Version 1.2.2:

New Operating System Support:

AIX 4.3.1 now supported.

New Device Management:

- 8245 Ethernet Stackable Hub using the Java Management Application (JMA)
- 8239 Token-Ring Stackable Hub using the JMA
- 8271 Ethernet LAN Switch using the JMA
- 8275 Ethernet LAN Switch using the JMA
- MSS Client/Domain Client using the JMA

New Software Functions:

- RMON/JMA Coupling - available on 8271s, 8239s and 8245s
- SNMP V3 Support in JMAs
- Performance Analyzer for Java Managed Devices - Capability to browse information in the JPM Database and create custom reports. Also a specialized report is available that provides response time data for groups of TN3270e clients.
- Config Tool Locator - The Config Tool Locator utility scans the installed system for configuration programs and saves information on location so that device management applications can locate them. Configurations can be installed anywhere on the system. Running the config tool locator will provide location information to the device management applications. Available for 2210, 2216, MSS, MSS Client/Domain Client and network utility device management applications and configurators.

Enhanced Device Management:

- 8210 MSS JMA
  - Graphic for Version 2
  - CPU Utilization
- 2210 Multiprotocol Router JMA
  - MRS 3.1.0.0 Support
  - APPN Extended Border Node
  - TN3270e
  - Remote LAN Access
  - CPU Utilization
- 2216 Multiaccess Connector JMA
  - MAS 3.1.0.0 Support

        - Parallel Channel Adapter
        - Fast Token-Ring Adapter
        - 4/8 Port ISDN Primary Adapter
        - APPN Extended Border Node
        - TN3270e
        - Remote LAN Access
        - CPU Utilization
    - Ethernet and Token-Ring Adapters JMA (Version 1.40)
    - 8260 Switching Module Series JMA
        - 20 Port 10BASE-T Ethernet
        - 18 Port Fast Ethernet
    - 8271 PSM - MSS Domain Client UFC
    - 8272 PSM
        - MSS Client/Domain Client UFC
        - 8270 Model 600
    - New or modified MIBs in JMA MIB browser consisting of:
        - RFC1659 RS232 (obsoletes RFC1317)
        - RFC2239 MAU (obsoletes RFC1515)
        - Agentcmn 8245 and 8275 Common Agent
        - ibmMSSClient MSS Client MIB
        - ibm-trsu IBM Token Ring Surrogate MIB
        - ibmnetu Network Utility MIB
        - ibm8239 8239 MIB
        - ibm8245 8245 MIB
        - ibm8275 8275 MIB
        - 3COM0006 3COM SETUP
        - 3COM0017 3COM STACK-CONFIG
        - 3COM0019 3COM RMON-REMOTE-POLL
        - 3COM0021 3COM PORT-SECURITY
        - 3COM0022 3COM MACRO-SCRIPTS
        - 3COM0024 3COM EVENT-EXTENSION
        - 3COM0025 3COM STACK-UNIT-TYPES
        - 3COM0026 3COM IF-EXTENSIONS
        - 3COM0027 3COM RMON-EXTENSIONS
        - 3COM0028 3COM ALARM-PEAK
        - 3COM0030 3COM LINKSWITCH-MIB
        - 3COM0039 3COM GENERIC-BRIDGE
        - 3COM0054 3COM BRASICA2-SPECIFIC
        - MG005 3COM NRM-MIB
        - SnmpV3MD Message Processing and Dispatching
        - SnmpV3Framework SNMP Management Architecture MIB
        - SnmpV3USM SNMP User-Based Security Model

Nways Campus Manager ATM Enhancements:

- ATM ESI tracking allows users to track UNI and multicast connections from one end point to another on switched virtual connections.
- A new 8270 3-slot blade is now available for the 8260 and 8265. This module supports UFC inserts for various functions, including the MSS client.

- Support for 8270 Model 600 with UFC for FE router with ATM port.
- Support for deletion of SVCs, the user is now asked to confirm the deletion request before it is performed.
- Disabled BCM configuration possible with a BUS that is down.
- Improved description in the PNNI Node Configuration panel of summary addresses are used and what they are.
- Tivoli NetAccess integration for 8260 and 8265.

Intelligent Hub Manager Program (IHMP):

- 8260 Switching Module Series -
  - 20 Port 10BASE-T Ethernet (with DMM 5.2)
  - 18 Port Fast Ethernet (with DMM 5.2)

LAN Network Manager (LNM) Enhancements:

Media management for the 8239.

2.2 Nways Workgroup Manager

The Nways Workgroup Manager is a true 32-bit native Windows NT application that operates on Windows NT Version 4.0. Nways Workgroup ReMon operates on both Windows Version 3.1 or higher and Windows NT Version 4.0.

Nways Workgroup Manager provides graphical device management applications that lower network operating costs. The Nways Workgroup Manager applications have a common look and feel, so your network operator training is reduced and your personnel is more productive.

Nways Workgroup ReMon provides RMON support, which reduces network operation and administration costs by making users more productive and by identifying network problems before they occur. Cost-savings and staff productivity increases as the number of RMON-managed LAN segments increases.

Performance information available from both Nways Workgroup Manager and Nways Workgroup ReMon facilitates performance refinements. Key network features of the Nways Workgroup Manager include:

- Automatic Internet network discovery
- Real-time, graphical views of network topology
- Ability to browse, update and compile MIBs
- Color-coded and aggregated network and device real-time status
- Trouble-ticketing
- Trap management, including specifying trap severities
- Trap compiler
- Polling configuration and notification
- Performance threshold configuration and notification
- Inventory management
- Collection and presentation of real-time and historical statistics

To provide security you identify the level of access controls that you need. The management applications then use the security features inherent in the SNMP management platform to control access to networking devices.

2.2.1 Device Management

The graphical user interface of the device-management applications gives you real-time views of your network devices, with color-coded status of components and overall status of the device. The Nways Workgroup Manager device management applications provide a complete set of messages, traps and event notifications for devices in the network. In addition the device-management applications support hot spots for point-and-click problem determination and action for example, click on a port and status information and other actions are displayed immediately.

Key features of the Nways Workgroup Manager device-management applications provide the ability for you to:

- View or change device, module or port configurations
- Display statistics at a device, module or port level
- Select a specific component via point-and-click with a mouse
- Receive real-time, color-coded status at a glance
- Define and monitor performance thresholds
- Define and monitor real-time and historical statistics
- Monitor real-time events
- Download microcode
- Telnet and FTP to a device

Nways Workgroup Manager supports the following devices:

- IBM 8210 Nways Multiprotocol Switched Services (MSS) Server
- IBM 8224 Ethernet Stackable Hub
- IBM 8225 Fast Ethernet Stackable Hub
- IBM 8230 Token-Ring Controlled Access Unit
- IBM 8235 Dial-In Access to LANs (DIALs) Server, including
- IBM 8235 Dial-In Access to LANs (DIALs) Switch Model I40
- IBM 8238 Token-Ring Stackable Hub
- IBM 8245 Ethernet Stackable Hub
- IBM 8239 Token-Ring Stackable Hub using the JMA
- IBM 8250 Multiprotocol Intelligent Hub
- IBM 8260 Nways Multiprotocol Switching Hub
- IBM 8271 EtherStreamerÆ/Nways Ethernet LAN Switch
- IBM 8272 LANStreamerÆ/Nways Token-Ring LAN Switch
- IBM 8273 Nways Ethernet RouteSwitch (requires IBM Nways RouteSwitch Network Manager, sold separately)
- IBM 8274 Nways LAN RouteSwitch (requires IBM Nways RouteSwitch Network Manager, sold separately)
- IBM 8281 Nways ATM LAN Bridge
- IBM 8282 Nways ATM Workgroup Concentrator
- IBM 8285 Nways ATM Workgroup Switch
- IBM 2210 Nways Multiprotocol Router
- IBM 6611 Network Processor

Additional support is included for the MSS Client running on the 8270/2 devices.

Nways Workgroup Manager includes Web-based management using Java technology for the following devices:

- IBM 8210 Nways Multiprotocol Switched Services (MSS) Server
- IBM 8273 Nways Ethernet RouteSwitch
- Generic Java-based management for any device in your network

2.2.2 RMON

RMON defines a standard set of MAC-layer statistics provides the ability to filter and capture data packets for analysis. RMON2, using RFCs 2021 and 2074, provides additional statistical information at the network and application layers of the protocol stack. IBM's RMON2 support is based on the ECAM that will be migrated to RMON2.

Nways Workgroup ReMon provides not only the RMON functions but also takes advantage of the ECAM capabilities to provide address translation and protocol distribution within your network. Address translation translates MAC addresses to network layer addresses. Protocol distribution allows you to view the protocols and applications being used on the network.

Use Nways Workgroup ReMon to proactively manage your network performance. It enables you to perform key functions such as:

- Watching for emerging problems and short-term trends
- Checking network performance and utilization
- Setting network service objectives
- Planning short-term and long-term network capacity
- Determining the busiest stations in your network
- Troubleshooting network problems and outages
- Capturing and analyzing network traffic based on definable filter criteria
- Analyzing network-traffic trends, including protocol distribution
- Associating MAC layer addresses to network layer addresses
- Configuring RMON and RMON2 agents

Nways Workgroup ReMon provides support for these RMON-enabled products:

- IBM 8225 Fast Ethernet Stackable Hub
- IBM 8230 Token-Ring Controlled Access Unit
- IBM 8238 Token-Ring Stackable Hub
- IBM 8245 Ethernet Stackable Hub
- IBM 8250 Advanced Token-Ring Management Module
- IBM 8260 Token-Ring Media Access Daughter Card
- IBM 8260 Ethernet Media Access Daughter Card
- Other RMON-compliant probes

Nways Workgroup ReMon provides support for these RMON and RMON2-enabled products:

- IBM 8239 Token-Ring Stackable Hub
- IBM 8250 Ethernet RMON Probe
- IBM 8260 High-End Token-Ring Media Access Daughter Card
- IBM 8260 High-End Ethernet Media Access Daughter Card
- Other RMON2 probes that implement the ECAM

2.2.3 Virtual LAN Configuration

A virtual LAN (VLAN) is a subnetwork defined by software instead of physical wiring. The IBM 8271 Nways Ethernet LAN Switch and IBM 8272 Nways Token-Ring LAN Switch have VLAN capability built in. You can set up a VLAN remotely, using the drag-and-drop feature of Nways Workgroup Manager, without having to go to the wiring closet.

Both the IBM 8285 Nways ATM Workgroup Switch and the IBM 8260 Nways Multiprotocol Switching Hub provide ATM switch/control points. The Nways Workgroup Manager provides management of:

- The ATM switch/control point
- The ATM modules in the 8285 or 8260
- The ATM interfaces (ports) in the ATM modules, including displaying information about the attached and registered ATM devices
- The permanent virtual circuits (PVCs)
- The switched virtual circuits (SVCs)
- IBM 8270 VLAN Support

2.3 Tivoli NetView Version 5.1

Tivoli NetView is a network management platform that allows users to view network topologies, discover the TCP/IP network, manage events and SNMP traps, and monitor the health of a network. In summary, Tivoli NetView will:

- Manage the network by using the auto-discover function to discover the network and all attached devices, then create graphical view of the network topology. Users can find the status of hardware devices, manage SNMP traps, and get notification when thresholds are exceeded.
- Understand events and changes in the network.
- Pinpoint problem areas and quickly resolve them.
- View relationships between devices.
- Share and correlate network data with information about applications, systems, and databases.

Tivoli NetView enables users to discover TCP/IP networks, display network topologies, correlate and manage events and SNMP traps, monitor network health, and gather performance data.

Tivoli NetView also provides a Web-based management user interface. This interface provides information such as:

- Node status
- Dynamically updated display of nodes that downloads fast, graphic displays show the topology layout.
- View object collections, events, and object information.
- NetView process status.
- Diagnostics such as ping, MIB browser and trace route.

Tivoli NetView provides graphical ruleset editor to easily define event management and correlation. The object collections enable users to group the devices by common characteristics and monitor them while they are updated dynamically.

The Nways JAVA applets can be launched from the NetView Version 5.1 Web interface providing further integration.

2.3.1 Rulebase Engine

A sophisticated rules-based event correlation engine allows you to graphically build rules that define how you want to implement business policies. Tivoli NetView enables you to manage events locally, centrally or pass them to other Tivoli applications for correlation. In essence, implementing business policies as a set of rules enables you to quickly diagnose root problems rather than report only symptomatic events. Further, when defined thresholds are violated, exception reporting declares serious problems with specific network devices.

For more information refer to the redbook *Integration Solutions using NetView V5.1,* SG24-5285 (available soon).

2.4 Nways RouteSwitch Network Manager Suite

Enhanced IBM Nways RouteSwitch Network Management Suite Version 3.2 includes the following:

- **IBM Nways RouteVision Campus Manager (NRCM)** includes previously known applications: Nways RouteSwitch Network Manager, Nways RouteTracker Manager, Nways RouteMonitor and Nways RouteDirector. This integrated suite of network management applications can be used to manage the entire RouteSwitch products including IBM 8277 Ethernet RouteSwitch, IBM 8273 Ethernet RouteSwitch, IBM 8274 LAN RouteSwitch, and RouteCell platforms.

  The Nways RouteMonitor and Nways RouteDirector no longer exist as separate products.

  NRNM supports the hardware chassis and modules, including the RouteSwitch wide-chassis and the RouteCell ATM switch and related modules. Each hardware chassis and module is represented by an individual bitmap and is SNMP manageable. RouteSwitch Manager also supports all of the new Version 3 features. In Version 3.2, RouteSwitch Network Manager is available for the following operating systems:

  - IBM AIX
  - HP-UX

  The RouteSwitch Manager can run in stand-alone mode or in conjunction with an enterprise manager, such as HP OpenView for UNIX and Tivoli NetView for AIX. In summary, Routevision provides the following:

  - Complete configuration, monitoring, and diagnostic information for IBM 8277.
  - Ethernet RouteSwitch, IBM 8273 Ethernet RouteSwitch, IBM 8274 LAN RouteSwitch and RouteCell platforms.
  - Creation and management of policy-based virtual LANs.
  - Statistic and Alarm monitoring of a switched network.
  - Draws logical network map of the switch network.
  - The NRCM is available for Windows 95/NT.

- **IBM Nways RouteVision Workgroup Manager (NRWM)** includes previously known applications: Nways RouteSwitch Network Manager, Nways

RouteTracker Manager, Nways RouteMonitor and Nways RouteDirector. This integrated suite of network management applications can be used to manage IBM 8277 Ethernet RouteSwitch, and IBM 8273 Ethernet RouteSwitch lines. RouteVision Workgroup Manager provides the following functions:

2.4.1 RouteVision Components

IBM Nways RouteSwitch Network Manager(NRNM) provides a suite of network management applications that administrators can use to manage the switches, media and services on the networks. Administrators can create VLANs, monitor the network, configure services, and manage switches.

- **Switch Management -** Network managers can use the Switch Management application to configure, control, monitor and manage the switches on the networks locally or remotely via SNMP.
- **VLANs Management** - Consists of policy-based VLAN planning and management. Using the VLAN application, administrators can create VLANs. The VLAN application allows administrators to create VLANs based on physical port, MAC address, layer 3 address, protocol type, multicast address, authenticated user, custom bit mask and/or a combination of these VLAN types. The VLAN application is an intuitive graphical VLAN planning and management application.
- **Management of Services -** An intuitive service for connection management. The Services application provides an intuitive interface that allows administrators to configure and manage the connections and services in their network. Every ATM connection on a switch can be individually configured and managed. Since ATM is a connection-oriented technology which often requires more configuration than legacy LAN protocols, this type of comprehensive management is extremely valuable.
- **Event and Performance Management -** Provides proactive monitoring of network events and statistics. The Events and Statistics applications use SNMP to gather data from switches throughout the enterprise. Using criteria set by the network administrator, these applications gather events or statistical data from switches throughout the LAN and WAN.

2.5 Device Specific Configuration Tools

IBM Nways Multiprotocol Access Services (MAS), Multiprotocol Routing Services (MRS), and Multiprotocol Switched Services (MSS) are the software that support Nways devices. The software has two components:

1. Base code which consists of:
   - The code that provides the routing, bridging, data link switching, and SNMP agent functions for the device.
   - The router user interface, which allows you to configure, monitor, and use the Multiprotocol Routing Services base code installed on the device. The router user interface is accessed locally through an ASCII terminal or emulator attached to the service port, or remotely through a Telnet session or modem-attached device.
2. The Configuration Programs for IBM Nways Multiprotocol Access Services (MAS), Multiprotocol Routing Services (MRS), and Multiprotocol Switched Services (MSS) are graphical user interfaces that allow you to configure the

device from a stand-alone workstation. The Configuration Programs includes error checking and online help information.

The base code is installed at the factory on Nways devices. The Configuration Program is not preloaded at the factory; it is shipped separately from the device as part of the software order.

Chapter 3. Planning for the Nways Management Installation

This chapter discusses the planning stages required before we implemented the network management tools and how these tools are installed and customized to manage our network.

By using the outlined planning process as documented in 1.3, “Network Management Design - Our Approach” on page 5 we completed the tables where appropriate. Our main objectives are outlined below:

- Ability to centrally configure the network devices
- Ability to pro-actively manage the network environment
- Ability to receive events based on network issues and problems
- Ability to produce performance reports for the network device

We divided the management functions into status, configuration, performance and fault.

3.1 Implementation Stages

With the assumption that the network was already configured and running, the planning stages we performed are outlined below:

Network Topology	Obtain and understand the network topology and structure
Devices	Build a list of the managed devices and the resources we want to manage
Applications	Understand which management applications are required and what functions we need to provide
Event/Performance	Build a list of SNMP traps that can be generated for our environment and make decisions on how to handle these traps from a management perspective

3.1.1 Network Topology

The network layout is shown in Figure 1 on page 22.

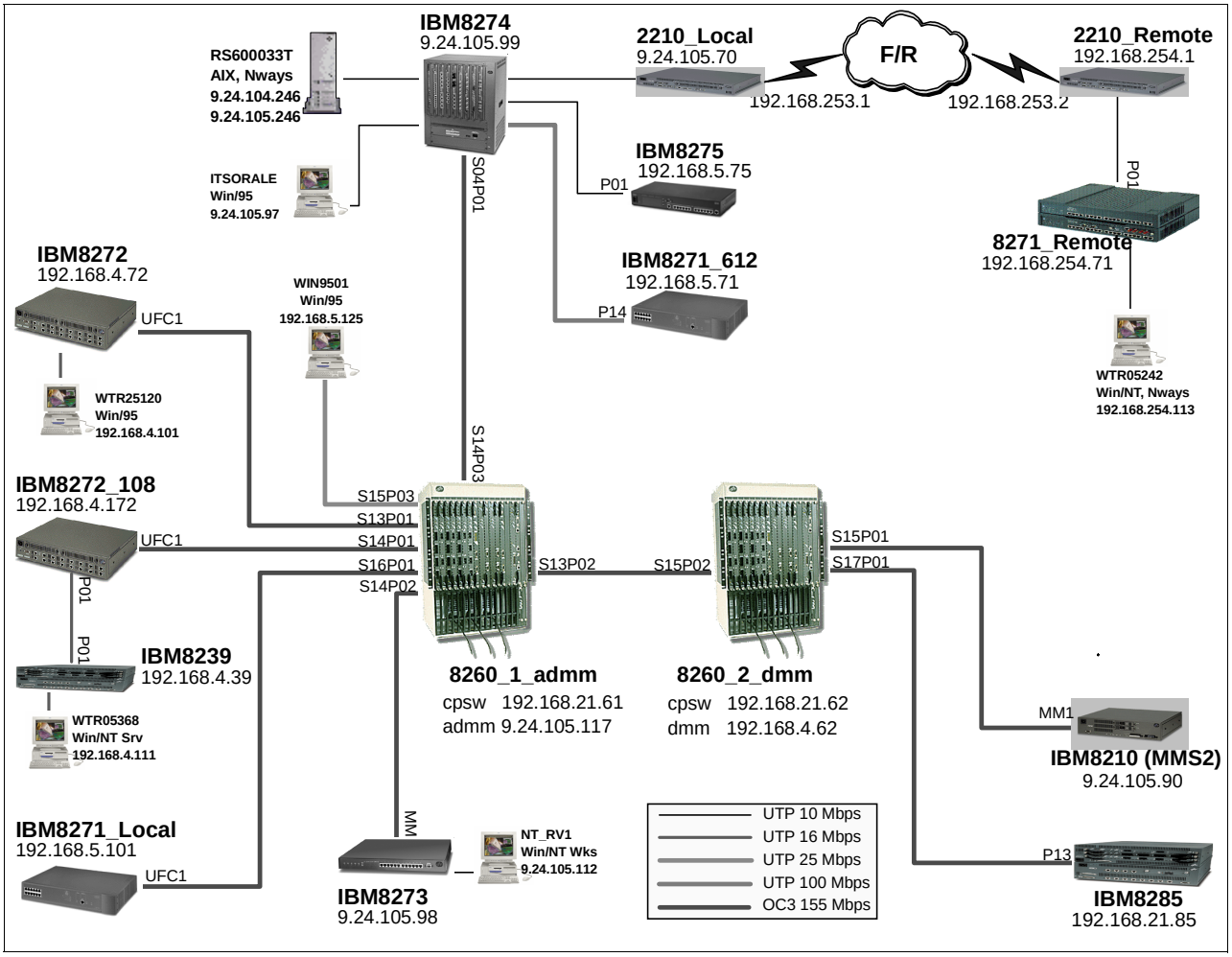


Figure 1. The Network Layout for Scenario 1

As you can see from the diagram we have included most of the Nways networked devices for the example. This was done to show the available functions for each device. We used a typical customer setup showing both the legacy and ATM functions.

In essence the network consists of:

- ATM backbone consisting of two CPSWs and one 8285
- Two 2210s routers providing a WAN link
- Various switches providing token-ring and Ethernet connections
- Two MSSs providing ELAN support (LECS and LES/BUS)
- Two ELANs defined; one Ethernet and one token-ring
- ATM uplinks installed in the switches
- PNNI configured for CPSWs

Using the information from the network diagram we are able to build a table showing the devices that are to be managed.

We connected the management station to the 8274 via ethernet and set up an ELAN for management purposes across our ATM environment called mgtelan. The 8274 provided us with an ATM uplink to the ATM network. However there are

a number of ways we could have achieved this connectivity, for instance we could have used a classical IP connection.

3.1.2 Devices

All devices used for the example are listed by device type. For each device we generated a list of the components. Some of the components have TCP/IP addresses assigned to them. By grouping the managed devices we can address each one in turn for specific requirements. This will enable us to resolve the required management tools list more efficiently.

This is also a good time to document the SNMP community names required to access each device. Table 4 on page 23 shows the output.

Table 4. Device and Element Information

Hostname	Device Components	IP Address	Microcode Level
8260 Devices			
8260_1_admm	CPSW ADMM MSS1 SWE10F2-F SWE12TP-RJ45 A-CAR (MSS1) A04-FB100MIC A03-MB155 A03-MB155 A12-TP25-RJ	192.168.21.61 9.24.105.117 9.24.105.114	V3.1.1 V5.21-H MSSV2.1 V2.00 V2.00
8260_2_dmm	CPSW DMM T20MS TMAC CPSW (backup) A04-FB100MIC A01-MB155 A02-MB155 A02-MB155	192.168.21.62 192.168.4.62	V3.1.1 V2.30-H V1.50 V4.00 V2.05
Stand Alone 8210			
MSS2	PCI ATM 155MB	9.24.105.90	MSS V2.1
8285			
IBM8285	155MB ATM MMF	192.168.21.85	V1.5.2
2210 Devices			
2210_local	LAN port WAN port	9.24.105.70 192.168.253.1	MRS V3.1
2210_remote	LAN port WAN port	192.168.254.1 192.168.253.2	MRS V3.1
8271 Devices			
IBM8271	ATM UFC	9.24.105.101	V4.0.0 V1.14.0
IBM8271_612	IBM8271_612	192.168.6.71	V3.10

Hostname	Device Components	IP Address	Microcode Level
8271_remote	ATM UFC	192.168.254.71	V4.0.0 V1.14.0
8272			
IBM8272	ATM UFC	192.168.4.72	V4.0.0 V1.14.0
IBM8272_108	ATM UFC	192.168.4.11	V4.0.2A
8273/4/5			
IBM8274	MPM II MPM II Ether/12 HSM2 ATM 2Meg ATM 2Meg	9.24.105.99	V3.2.3 Patch 33
IBM8273	MPMII	9.24.105.98	V2.1.1
IBM8275		192.168.5.75	V1.2
8239			
IBM8239	IBM8239	192.168.4.39	V0.2

This also provided the required naming for the DNS or host file configuration. Specifically if we are using a limited discovery, we can take the contents of this table and use it in the creation of a seefile to use with NetView discovery.

For more information, see Appendix B, “Devices Management Options” on page 427.

3.1.3 Management Applications

The next step was to build a table that match the tools to each management function. This will assist us in deciding which management tools we require. This high-level view provides the customer with information on the functions that the tools will provide and eliminates any unnecessary management applications from being installed. The table gives us some control over what we need to deliver and whether we meet the customer requirements.

The management tools by function are shown in Table 5 on page 24.

Table 5. Applications To Perform Required Management

Management Functions				
Device	**Status**	**Configuration**	**Performance**	**Fault Management**
2210 Router	2210 Device Manager NetView SNMP Bridge Manager	2210 Device Manager MRS Configurative SNMP BridgeManager 2210 Web Interface	JPM SNMP Bridge Manager	NetView Event Desk NetView Rulesets JPM

Management Functions				
Device	**Status**	**Configuration**	**Performance**	**Fault Management**
8210 MSS	8210 DeviceManager NetView ATM Manager SNMP Bridge Manager MSS Web Interface	8210 Device manager MSS Configurator SNMP Bridge Manager MSS Web Interface	JPM SNMP Bridge Manager NetView Thresholding ATM Manager MSS Web Interface	NetView Event Desk NetView Rulesets
8239 Token-Ring Stackable Hub	8239 JMA NetView IP MAP Token-Ring Media Manager	8239 Dev Manager Remote Monitor Token-Ring Media Man	JPM Remote Monitor Traffic Monitor Token-ring Media Man.	NetView Event Desk NetView Rulesets
8260 Switching HUB	8260 Device Manager SNMP Bridge Manager ATM Manager	8260 Device manager ATM Manager Remote Monitor SNMP Bridge Manager	8260 Device Manager SNMP Bridge Manager NetView Thresholding Remote Monitor Traffic Monitor ATM manager JPM	NetView Event Desk NetView Rulesets 8260 Hub Manager ATM Manager
8271 Switch Model 108	8271 Device Manager NetView SNMPBridge Manager ATM Manager	8271 Dev Manager SNMP Bridge Man. ATM Manager	8271 Dev Manager SNMP Bridge Manager ATM Manager	NetView Event Desk NetView Rulesets ATM Manager
8271 Switch Model 612	8271 Device Manager NetView SNMP/Bridge Manager ATM Manager	8271 Dev Manager SNMP BridgeManager ATM Manager Remote Monitor	JPM SNMP Bridge Manager Remote Monitor ATM Manager	NetView Event Desk NetView Rulesets ATM Manager
8272 Switch Model 216	8272 Device Manager SNMP Bridge Manager ATM Manager NetView	8272 Dev Manager SNMP BridgeManager ATM Manager	8272 Dev Manager JPM SNMP Bridge Man. Remote Monitor ATM Manager	NetView Event Desk NetView Rulesets ATM Manager
8273	8273 Device Manager NetView ATM Manager RouteVision	8273 Dev Manager	JPM ATM Manager RouteVision Remote Monitor	NetView Event Desk NetView Rulesets RouteVison
8274 LAN RouteSwitch	RouteVision NetView ATM Manager	RouteVision	RouteVision Remote Monitor	NetView Event Desk NetView Rulesets RouteVision
8275 Ethernet LAN Switch Model 113	8275 Device Manager NetView Remote Monitor	8275 Dev Manager	JPM Remote Monitor	NetView Event Desk NetView Rulesets
8285 ATM Workgroup Switch	8285 Device Manager NetView ATM Manager	8285 Dev Manager ATM Manager	JPM ATM Manager	NetView Event Desk NetView Rulesets ATM Manager

Some additional product information is detailed below:

- SNMP Bridge Manager is also known as LNM.
- Remote Monitor is also known as LANRemon.
- The device managers are either JMAs or PSMs.
- By default the Campus Manager LAN component is installed.

Device manager refers to either the PSM or the JMA except for the 8260.

Note

The above is a listing of all of the possible management functions available per specified device. Therefore, the addition of an MSS blade to an 8260 would also add the associated MSS management functions to those listed for the 8260.

Now we have selected the tools. Before we begin installing the applications we look at the SNMP trap configuration.

3.1.4 SNMP Trap Configuration (Fault)

In order to provide event management such as correlation, and to describe what actions the network operators need to perform on receipt of a specific event we need to evaluate each trap source. For each source we perform an in-depth analysis of what we expect to see, and typically what information we will be receiving to give us a better understanding of the type of problems we need to react to. For each trap we asked the following questions:

- Do we need to see this trap?
- Is there potential to provide correlation with other traps?
- Do we need to log this trap for analysis?
- Does this trap need to be filtered, and if so where?
- Does this trap need to be forwarded to an enterprise management system?

Note: A full listing of all the generated events from IBM hardware are listed in Appendix A, “Nways Devices - Generated Events” on page 367.

The tables were defined from information retrieved from sources such as the networking URL:

`http://www.networking.ibm.com/support/products.nsf`

and also the MIB definition files provided by Nways Manager for AIX in directory /usr/OV/snmp_mibs

These tables can be used to assist with the following decisions:

- Should the events be log only?
- Do we need to view these events from NetView?
- Do we need to forward these events to a problem management system?
- Can we perform any correlation using NetView rulesets?

All status traps will be logged automatically.

This will provide the information on what traps we can filter using NetView if these traps cannot be filtered from the device level.

3.1.5 8260 Trap Definitions

The traps for the 8260 are slightly different in that the events that appear in the event window are not the original traps sent to the NetView management station. The hub manager application internally generates a new trap with additional formatting. The original traps are set to log only.

The mapping is one-to-one and it is simple to identify the new trap number that needs to be modified.

The 8260 events are mapped internally to the application traps, therefore we have to be aware of what trap actually appears in the event window. The column titles Mapped To shows the internal trap ID.

Table 6 on page 27 shows an example of the types of actions we considered.

Table 6. Nways 8260 Multiprotocol Switching Hub (Subset)

Trap No.	Trap Name	Description	Action(s)
ibm8260.mib (Enterprise 1.3.6.1.4.1.49)			
2	ibm8250SlotDown	This trap indicates that the module in the indicated slot is down. Usually, this trap is sent when the module has been removed. Sometimes, this trap is sent when management communications with this module have been broken.	- View event from NetView events desk - Provide correlation with Slot Up - Status Setting to Critical - Send event to problem management - Event converted by application (hmp6000 enterprise - event 2)
3	ibm8250SlotUp	This trap indicates that a blade in the indicated slot is up. Usually, this trap is sent when the module is inserted into the hub. Sometimes, this trap is sent when management communications have been restored to a module where they had previously been broken.	- View events from NetView events desk - Provide Correlation with slot down - Status Setting to Clear - Send event to problem management - Event converted by application (hmp6000 enterprise - event 3)

Using the two traps as an example we documented that these events will be shown on the NetView event window, therefore we do not need to perform any filtering. Also we could perform correlation with these two events, for instance, when a slot up events arrives after a slot down event we can remove both events from the events window.

Also by using the trap tables we can see how many traps can be generated by the device.

In summary the event tables can assist with defining filters, dynamic workspaces, event correlations and problem management interfaces.

3.1.6 Event Logging System (ELS) Messages

The 2210 and 8210 have a different mechanism to send most of the traps to NetView. They convert the ELS messages to SNMP traps.

It is possible to enable ELS events by individual messages or by subsystem, for instance ATM, LEC and BBCM. The following table breaks down the message

types by subsystem as defined in the *Event Logging System Messages Guide*, SC30-3682. Table 7 on page 28 shows the subsystems for the 2210.

Table 7. ELS Subsytem

Msg Prefix	Subsystem	Activate
LEC	LAN Emulation Client	ERROR
LECS	LAN Emulation Configuration Server	ERROR
LES (LES/BUS)	LAN Emulation Server and Broadcast Unknown Server	ERROR
TCP	Transmission Control Protocol (TCP)	ERROR
SVC	ATM Signalling	ERROR
STP	Spanning Tree Protocol	WARNING/ ERROR

3.1.7 Events and Performance

In addition to the SNMP events generated directly from the devices we also need to provide a number of performance threshold traps. These traps will also appear in the NetView events console.

These traps are generated from a number or sources such as:

- RMON
- NetView
- Java Performance Manager
- RouteVision

An example of the 8260 ATM performance MIBs that will be polled is shown in Table 8 on page 28

Table 8. Performance Traps Based on Thresholds

Device (Resource)	Application	MIB(s) Polled	Events Generated
8260	Campus Manager ATM	ATM	No
8210	Campus Manager ATM	ATM	No
8274	RouteVision	8274 MIBs	Yes
2210	JPM	2210 MIBs	Yes
8239	Remote Monitor	RMON II	Yes

Throughout this redbook we refer to these performance applications.

3.2 Summary

At this stage we have built our list of managed devices and decided on what tools we need in order to provide the management functions. We also know what filtering we need to perform.

The complete list of software is as follows:

- NetView Version 5.1 including the Tivoli Framework

- Nways Campus Manager - LAN
- Nways Campus Manager - ATM
- Device Managers in the form of PSMs for 8271s, 8272s and 8285s
- Device Managers in the form of JMAs for the 2210s, 8210s, 8239s, 8272s, 8273s and 8275s
- 8260 Device Manager
- Java Performance Management (JPM)
- Nways Manager - Remote Monitor (ReMon)
- Nways Manager - Traffic Monitor
- RouteVision
- MSS Configuration tool
- MRS Configuration tool

The LNM SNMP Bridge Management and LNM Token-ring Media Management are used for MAC level status, configuration and performance management.

Chapter 4. Nways Manager for AIX Installation

This chapter describes the installation of the management software for AIX using step-by-step instructions.Table 9 on page 31 shows a summary of the applications we installed.

Table 9. Applications to Install

Management Software				
Devices	**Status**	**Configuration**	**Performance**	**Fault Management**
2210 **8210** **8238** **8260** **8271(108)** **8271(612)** **8272** **8273** **8274** **8275** **8285**	Device Managers NetView Maps NetView Collections SNMP Bridge Manager ATM Manager RouteVision TR Media Manager	Device Managers MRS Config Program SNMP Bridge Manager 2210 Web interface 8210 MSS Config ATM Manager RouteVision	SNMP Bridge/Switch 2210 Web Interface ATM Manager MSS Web Interface Remote Monitor Traffic Monitor RouteVision	NetView Event Desk NetView Rulesets ATM Manager Nways RouteSwitch Device Managers

Next we can install the applications.

4.1 Tivoli Framework and NetView

We installed Tivoli Framework Version 3.6 on rs600033t. We followed the instructions contained in the Tivoli documentation. This process is covered in detail in the redbook *Integrated Management Solutions Using NetView 5.1*, SG24-5285 (available soon).

In short, we installed the rs60033t as a TMR server and then installed the NetView code using wserver to create the TMR server (from the Tivoli Framework CD-ROM) and then installed the NetView application on the TMR server using the standard Tivoli installation screens.

4.2 Hardware Prerequisites

The following hardware prerequisites are required in order to install Nways Manager for AIX V1.2.2:

- RS/6000 Server with:
  - 77-MHz CPU speed or higher
  - 166-MHz 604e PowerPC CPU or higher
- Minimum memory requirements:
  - 256MB if you install only one Nways Manager component
  - 512MB if you install all Nways Manager components (768MB is recommended.)

The total amount of required memory depends on the size of the network to be managed and the number of other applications and X-stations to be supported.

- Minimum disk space requirements:

- Campus Manager - LAN: 400MB
- Campus Manager - ATM: 100MB
- Remote Monitor: 61MB
- Traffic Monitor: 42MB

- Swap space requirements:
  - Two and a half times the amount of RAM for 128MB to 256MB
  - Two times the amount of memory for 256MB and above

    Note: Larger networks will require more swap space.

  - 256-color (8-bit plane) display device of at least 16 inches
- Display/graphics adapter that is configured for and supports 1280x1024x8 pixel resolution
- Mouse
- CD-ROM

4.2.1 Software Prerequisites

The following software is required in order to install Nways Manager applications:

- One of the following versions of AIX:
  - AIX Version 4.1.5 with APAR IX64753 and the Value Option (or latest APARs/PTFs)
  - AIX Version 4.2.0 with APARs IX65070, IX62144, and the Bonus Pack (or latest APARs/PTFs)
  - AIX Version 4.2.1 with the Bonus Pack
  - AIX Version 4.3.1 with latest APARs/PTFs

Note

If you are using AIX Version 4.2.0, it is recommended that you install the free upgrade to AIX Version 4.2.1.

It is recommended that you download and install the latest PTFs for AIX before installing this product.

- Other AIX components include:
  - bos.adt.lib
  - Other bos components that NetView requires
  - AIX/windows environment/6000 X11R5
  - OSF/Motif Version 1.2
  - ipfx.rte
  - bos.dos.utils (if routes/MSS config programs are required)
- Java Runtime Environment(JRE) 1.1.4.4. To check your JRE current version, use the command:

  ```
  lslpp -h 'Java*'
  ```

Note

The java -fullversion command does not gives the details of the PTF level. To get the installable code of the latest JRE version, see the WWW links below:

`http://w3.hursley.ibm.com/java/codedemos/quickdl.html or`
`ftp://hurftp.hursley.ibm.com/pub/java/aix`

The JDK is required for the installation process, although only the JRE is used by Nways once the software is installed.

4.2.1.1 Nways Manager LAN/Nways Manager ATM

Campus manager LAN and ATM require the following:

- NetView for AIX Server Version 4 (with PTF U450745 or later) or Tivoli NetView Server Version 5.0
- Web Server for Web access to the Nways Management workstation; for example, IBM Internet Connection Server, Netscape, Lotus Domino
- Java Development Kit (JDK) Version 1.1.4-compliant Web browser for access to the Nways Manager management workstation such as:
  - UNIX platform

    Sun HotJava Browser 1.0 or 1.1.4 *only*
  - Windows platform

    Microsoft Internet Explorer 4.0 or 4.01 with the RMI patch
    Netscape Communicator Professional Edition 4.0.5 or later
    Sun HotJava 1.0 or 1.1.4

4.2.1.2 Nways Manager - LAN

Campus manager LAN requires the following prerequisites:

- IBM Nways RouteSwitch Network Manager program if you intend to manage the IBM 8274 Nways LAN RouteSwitch or IBM 8276 Nways Ethernet RoutePort. IBM 8273 Nways Ethernet RouteSwitch can also be managed by IBM Nways RouteSwitch Network Manager.
- IBM Nways RouteTracker Manager if you intend to configure VLANs for the IBM 8273 Nways Ethernet RouteSwitch or the IBM 8274 Nways LAN RouteSwitch.
- JDBC-compliant database to use with Java-based performance management functions in the Campus Manager LAN (DB2 Universal Database Enterprise Edition Version 5.0 is provided with Campus Manager - LAN License Use Certificate.)

Important

If you are using IBM DB2 Universal Database Version 5.0, you must apply APAR JR11296 (available from the IBM DB2 Support).

- Tivoli Distributed Monitoring feature Version 2.3.1 if more than one instance of the mid-level manager is required.
- IBM Multiprotocol Access Services (MAS) program if you want to configure the IBM 2216 Multiaccess Connector. MAS is shipped with the IBM 2216.

- IBM Multiprotocol Routing Services (MRS) program if you want to configure the IBM 2210 Nways Multiprotocol Router. MRS is shipped with the IBM 2210.
- IBM Multiprotocol Switching Services (MSS) program if you want to configure the IBM 8210 Nways Multiprotocol Switching Services (MSS) server. MSS is shipped with the IBM 8210.
- IBM LAN Adapter Agent for OS/2 and Windows NT workstations containing IBM Ethernet and token-ring adapters. Visit the IBM LAN Adapter Agent Web page for instructions on obtaining and installing the agent. This page can be reached at the following location:

  `http://www.networking.ibm.com/trl/trllma.html`

  The DIA is an optional pre-requisites to the LAN component.

4.3 Installing Nways Manager for AIX

To install Nways Manager for AIX Version 1.2.2 follow the steps described below.

First stop all NetView daemons using the command ovstop.

If you intend to install the Performance Monitoring Using Router and Bridge Manager feature, ensure that the LANG environment variable is set to the appropriate value. The catalog files are installed in the directory defined by the current $LANG variable.

Log in as the root user and create the mount point directory for the CD-ROM by entering the command `mkdir /cdrom`.

Important

You must use /cdrom as the mount point. If you use a different mount point, the installation program will not work correctly.

Insert the IBM Nways Manager for AIX Version 1.2.2 CD-ROM and mount the CD-ROM by entering the command:

```
mount -r -v cdrfs /dev/cd0 /cdrom
```

Execute the shell script to start the installation program by entering the command:

```
/cdrom/install.nways
```

This script will check that you have the correct version of Java installed and will prompt you to continue.

```
#/cdrom/install.nways
Java runtime environment is at the right level
/usr/bin/jar
We are going to stop all NetView daemons and EUIs.
Do you want to continue [yes]
```

Figure 2. Installation Screen

The script will close all NetView EUIs and daemons (if you have not already done so). The Welcome window for the installation program is displayed.

Figure 3. Nways Manager for AIX Installation Window

Click on **OK** to continue.

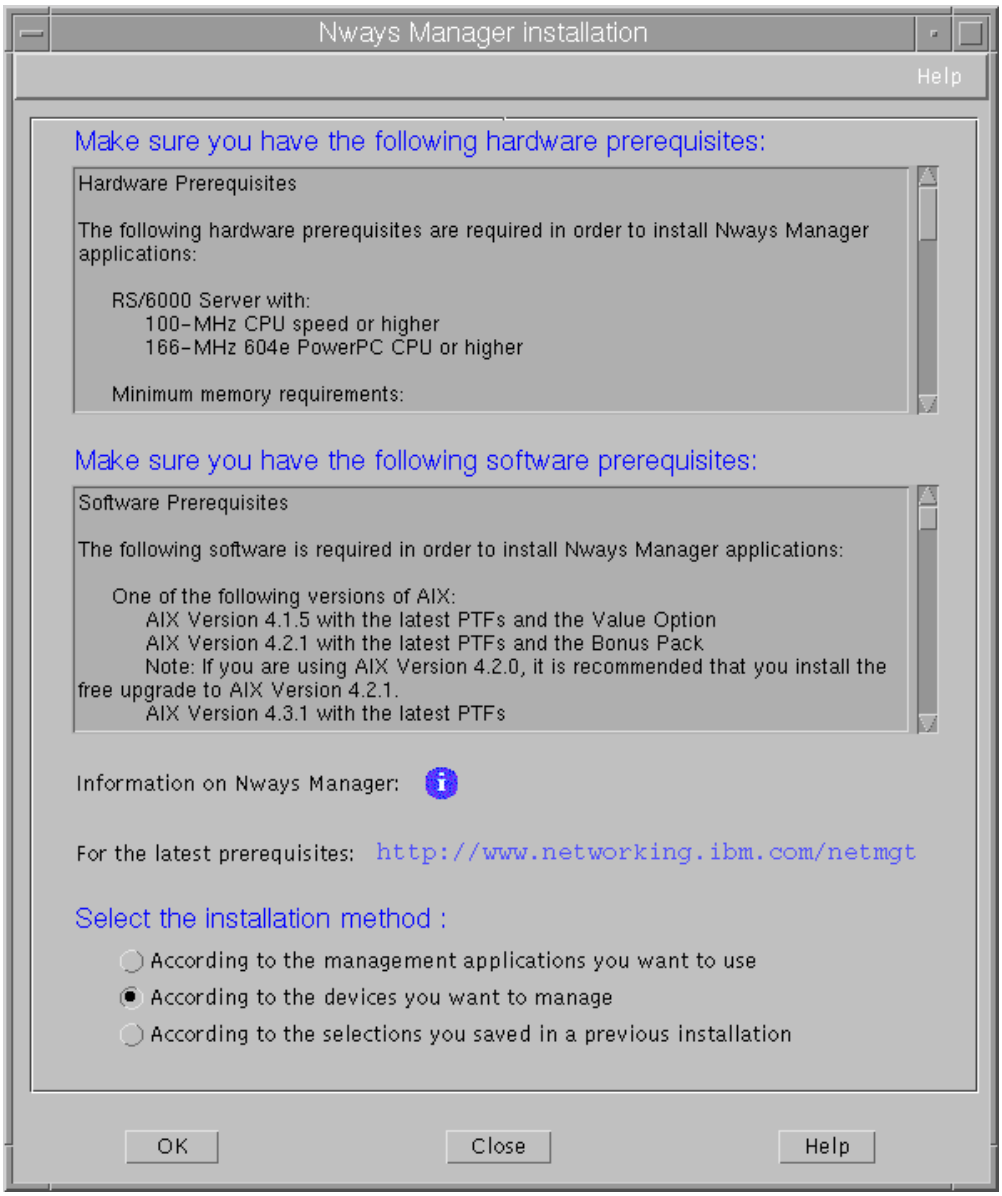


Figure 4. Nways Manager for AIX Installation Method Selection

You can choose to install individual modules if you know which ones you need or you can indicate which devices you want to manage and allow the installation process to select the appropriate modules for you.

If you choose to install by application, Figure 5 on page 37 will appear.

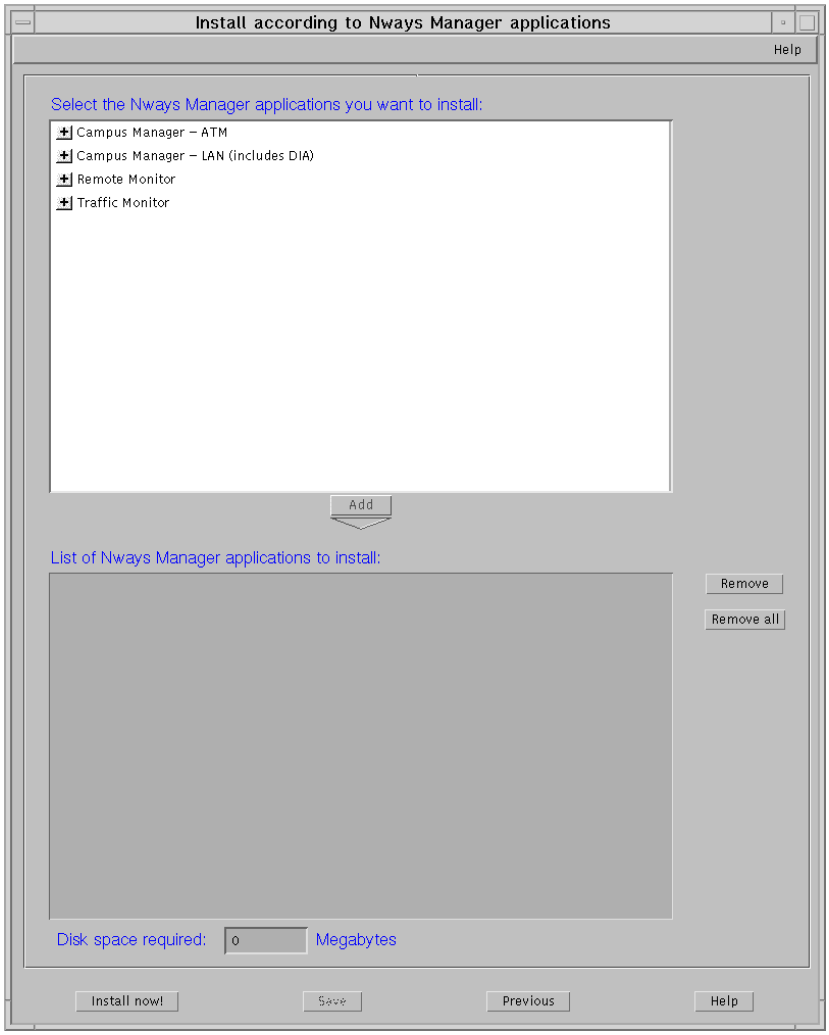


Figure 5. Nways Installation by Application

You can install sub-modules by clicking on **+** to expand one section as shown in Figure 6 on page 38.

.

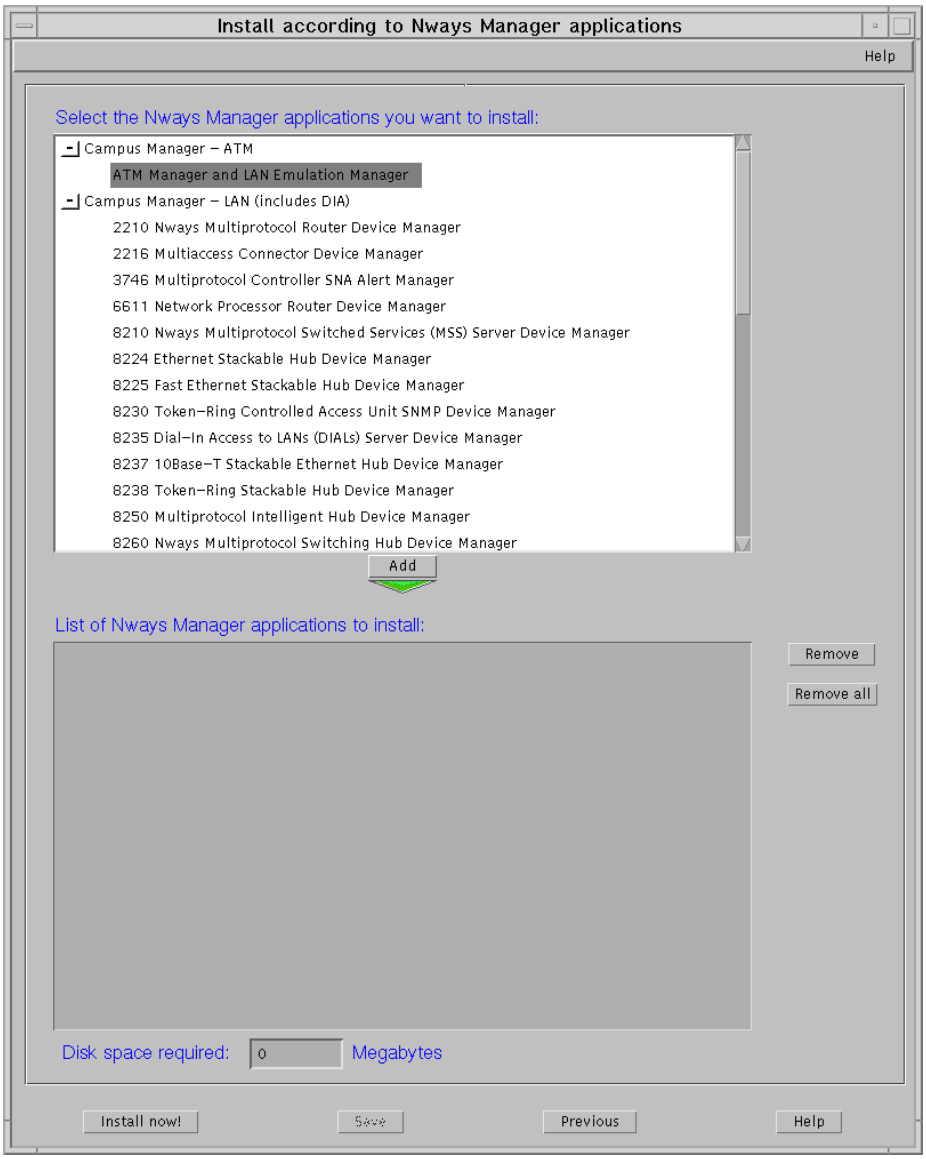


Figure 6. Nways Installation by Application - Expand

Select the modules and sub-modules you wish to install and click **Add** to add these to the list of applications to be installed. If you choose to install by device (see Figure 7 on page 39.)

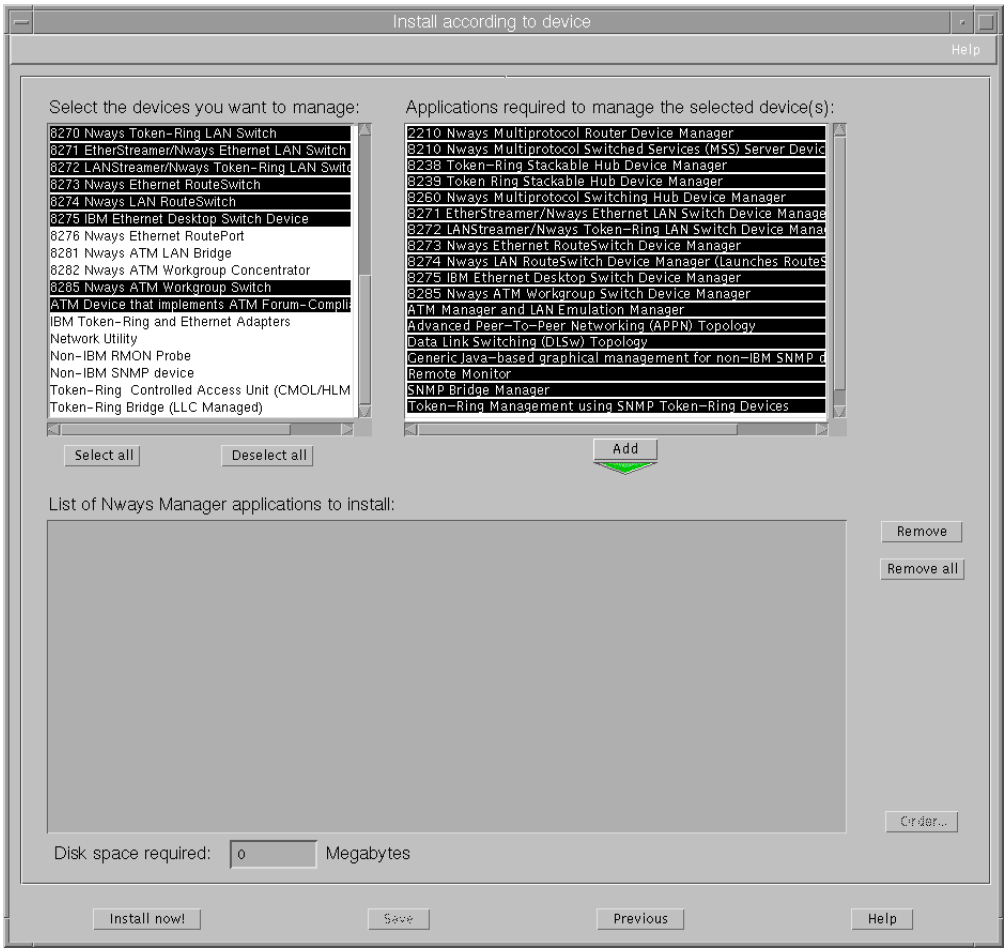


Figure 7. Nways Installation by Device - Select

Selecting a device will show the relevant applications to be installed. Click **Add** to add these to the list of applications to be installed. Screen Figure 8 on page 40 will appear next.

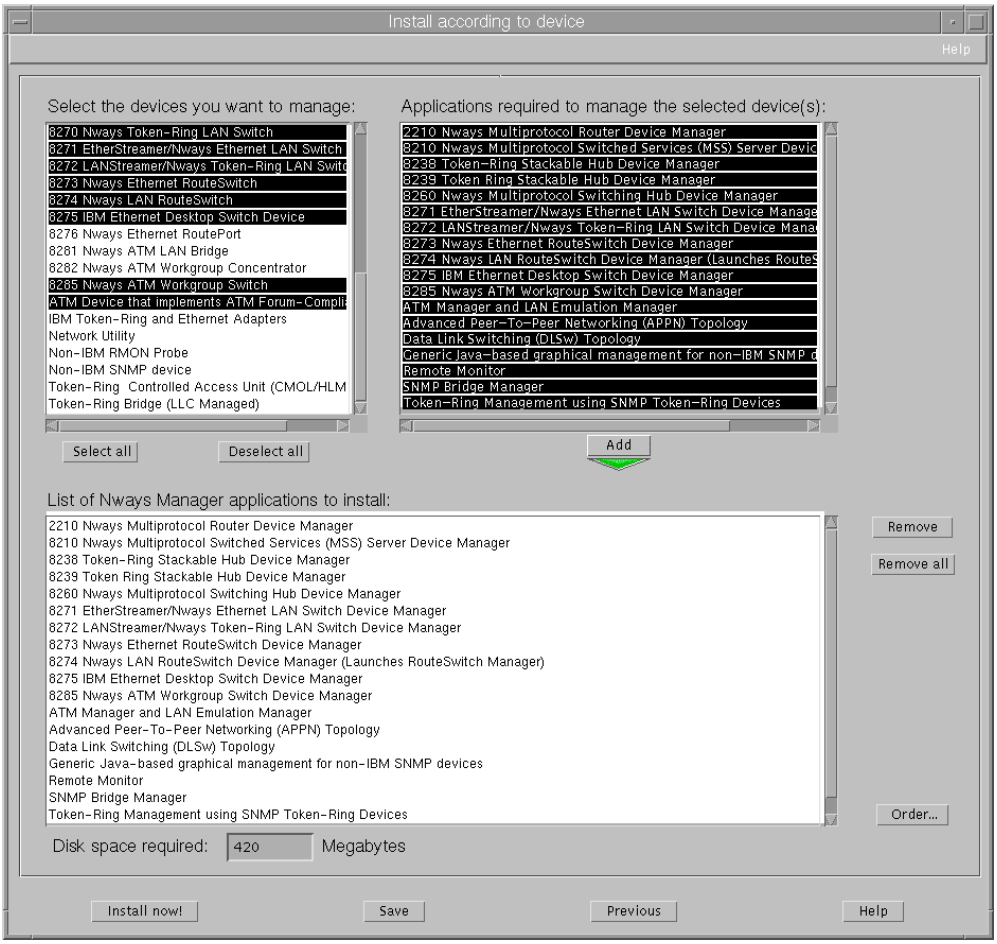


Figure 8. Nways Installation by Device

Once the list is complete, click **Install Now!** to start the install process. Choose **Yes** when the Confirmation dialog comes up. Figure 9 on page 41 shows the installation progress window.

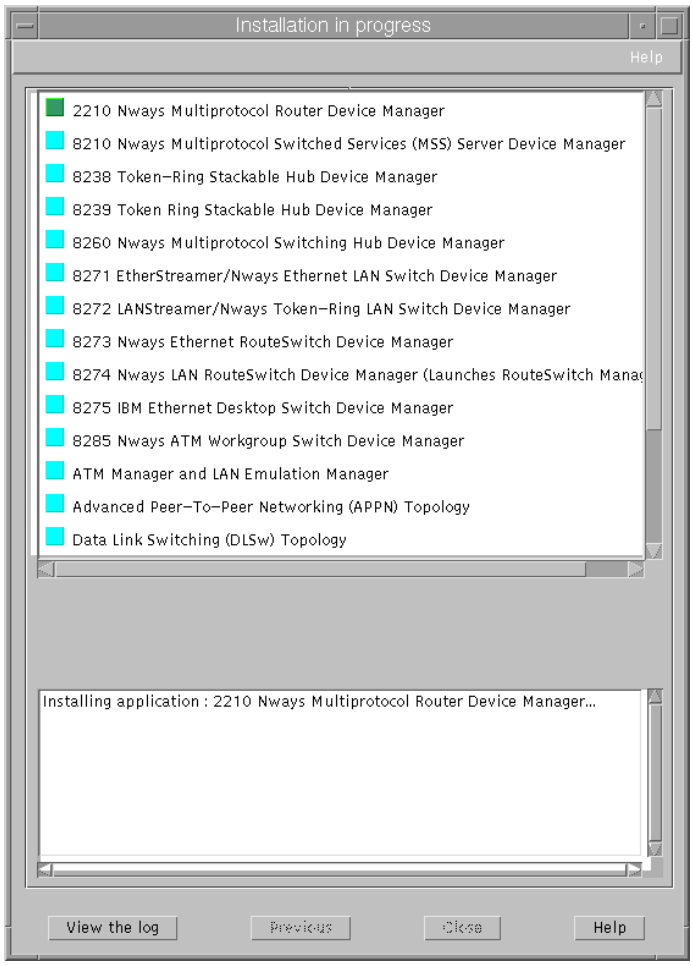


Figure 9. Nways Installation Progress Window

During the install process, you can monitor progress by watching the colored icons beside each module in the list.

- Flashing green means the module is being installed.
- Solid green means the module installed successfully.
- Solid yellow means the module installed with some minor errors.
- Solid red means there was some serious error.

Typically, minor errors occur if some of the applications in a particular module are already installed on the system, for example, the 2210 management application is the same as the 2216 and the 8210 (MSS) application. So if you choose to install all three, the last two will report minor errors since the first will have already installed all the necessary applications.

You can view more details of the installation's progress by clicking **View Log** the logfile window is shown in Figure 10.

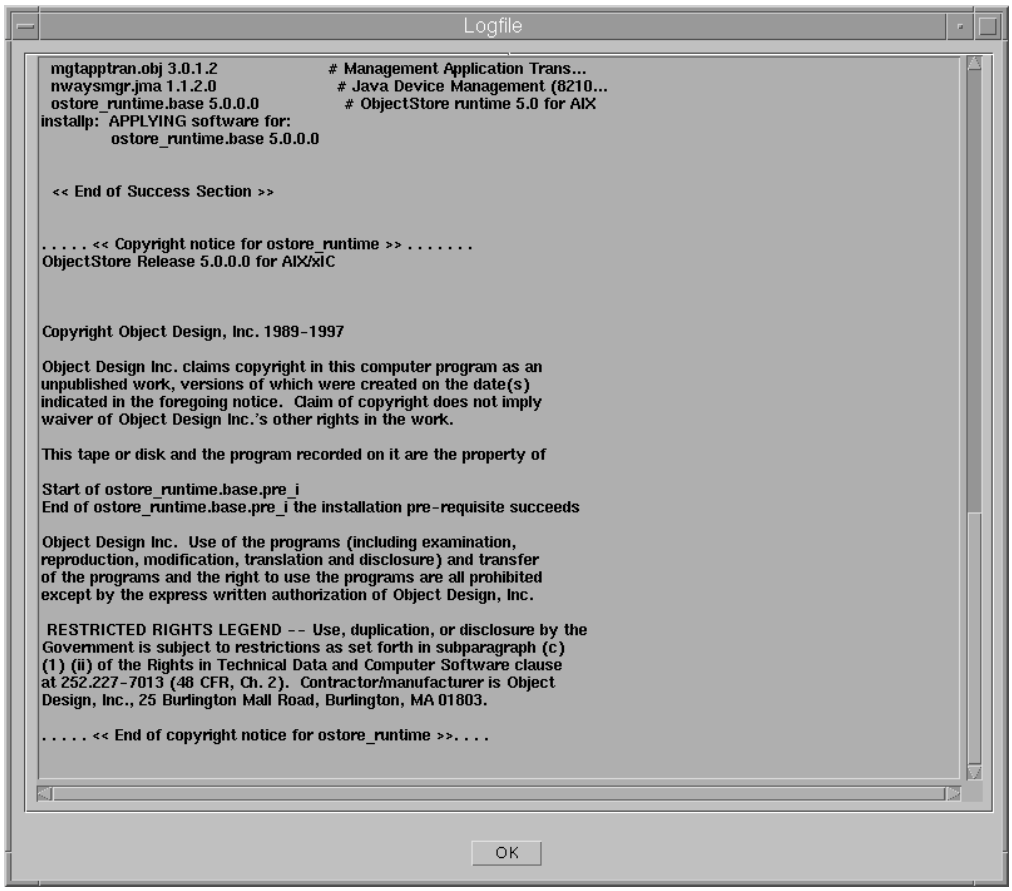


Figure 10. Logfile Window

4.3.1 Temporary Fixes for Nways Manager V1.2.2

There are two fixes that we had to implement for Nways V1.2.2 directly after the installation. These are:

1. Modify the ed.conf file as follows:
   - Move the entry Rnvch to the line before the Rnvgate entry.
   - Save and quit.
2. Replace the NwaysJavaWrapper file as follows:
   - Download NwaysJavaWrapper to the /tmp directory. This file can be found at `http://www.networking.ibm.com/support/code.nsf/maix12code?OpenView`.
   - Exit all NetView for AIX end-user interfaces.
   - Change the directory to /usr/CML/JMA/bin and issue the following commands:

     ```
     cp NwaysJavaWrapper NwaysJavaWrapper.org
     cp /tmp/NwaysJavaWrapper NwaysJavaWrapper

     chown bin.bin NwaysJavaWrapper
     chmod 555 NwaysJavaWrapper
     ```

Enter **nv6000** to restart NetView.

4.4 Post Installation Setup for Nways Manager Applications

This section describes additional configuration steps that we performed after installing Nways Manager for AIX.

4.4.1 Nways for AIX Integration

The Nways Campus Manager products are well integrated to provide different views for the same device. Campus Manager LAN and ATM can be coupled to provide full management of the ATM modules in the 8260 Hub. The integration is automatically enabled when Camus Manager LAN is started. This allows you to switch from a device element view of an 8260 to an ATM view or vice-versa.

The default coupling can be changed from the NetView pull-down menus by selecting **Netview Menu bar -> Administer->Campus Manager SMIT Control->Coupling between Hub Manager and Campus.**

The options are:

Stop	Stop the coupling
Start	Start the coupling
Re-Sync	Re-synchronize the coupling
Show Status	Shows the status of the coupling

When ATM and switch modules remain blue in the Hub Manager view, use the Re-sync option to re-synchronize the coupling between Campus Manager LAN and ATM.

Similarly when Remote Monitor installs, it integrates with NetView and Campus Manager LAN, allowing you to launch Remote Monitor from a device element view.

4.4.2 Accessing the Java-Based Device Manager Help

The Java-based managers use a Web browser to display their HTML help panels. If the Web browser is installed in a directory that is not included in the search path, then you will not be able to access the online help.

The installation program assumes that you are using Netscape as your Web browser.

To use a Web browser other than Netscape or to specify a browser that is not in the search path, edit the /usr/CML/JMA/java/websvr/properties/BrowserApplet.txt file and specify the fully qualified name for the Web browser on the following line:

```
webBrowser.path=/tools/bin/netscape
```

4.4.3 The 2210, 2216 and 8210 Configuration Programs

The 2210, 2216 and 8210 devices provide configuration programs that correspond to the microcode level of the device. These programs are installed in a directory of your choice for example, /usr/mrs210 for the 2210 config program and /usr/mss210 for the 8210 config program.

1. Install the MSS Configuration Program.
   - The MSS to be installed in this scenario is Version 2.1 PTF 1 and will be installed from diskettes.

```
mkdir /usr/mss210
cd /usr/mss210
```

- Insert the first configuration program diskette.
- Copy the AIX installation script to the RS/6000 using the command:

  ```
  dosread -a install.aix install.aix
  ```

Note: The AIX DOS utilities must be installed to run this command.

- Next, change the execution permissions to the following:

  ```
  chmod 777 install.aix
  ```

- Execute the script as follows:

  ```
  ./install.aix
  ```

- You will be asked where you want to install the configuration program and then prompted for each of the diskettes.

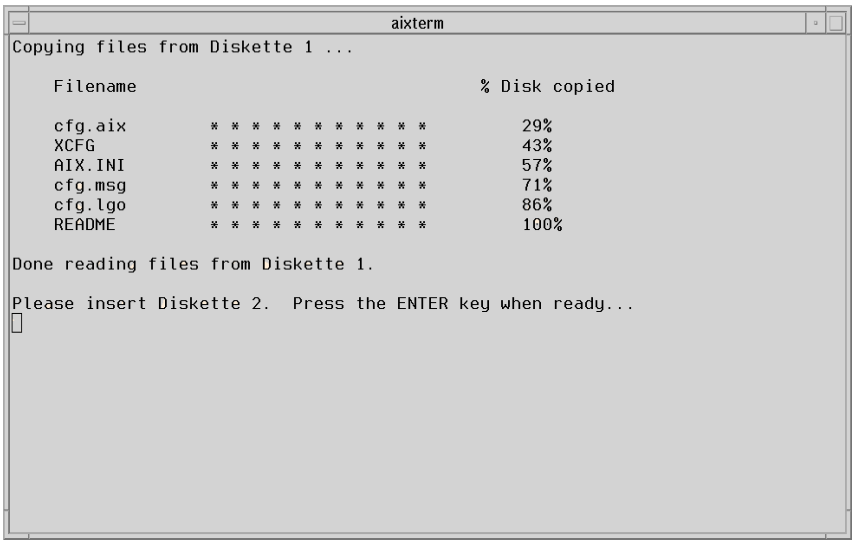


Figure 11. MSS Installation Screen

- To start the config program, change the directory to your chosen install directory as follows:

  ```
  cd /usr/mss210
  ./cfg
  ```

  You can also launch these configuration programs from the Java-based device managers when using the local interface.

2. Install MRS Configuration Program
   - The MRS Version 3.1 (with PTF NP00905) was installed from an image. For more details see the README file associated with MRS installation code.
   - We downloaded the mrsv31aix file to a temporary directory. This file is 27 MB in size.

Run SMIT and do the following:

- Select **Software Installation and Maintenance**.

- Select **Install and Update Software**.
- Select **Install and Update from ALL Available Software.**
- Input the full path of the temporary directory that the mrsv31aix file was downloaded to.
- Select the **List** button to list software and select **MRSV31** to install.
- Select **OK**.

For installation of MAS Configuration Program, please refer to the README file on the MAS installation diskette.

3. Next we modified the following file to associate the device managers with the configuration programs. This informs the device manager program the location of the config programs. We edited the file using the vi command.

   ```
   vi /usr/CML/JMA/java/websvr/properties/Cfg.txt
   ```

   A portion of the file is shown below. We are using the MSS configuration tool Version 2 Release 1.

```
# ------------------------------------------
# - Directory 2210 Config Tool on UNIX      -
# ------------------------------------------
AIX_2210_V1R2              = "/usr/rfcg120"
AIX_2210_V1R3_1_PTF795     = "/usr/rfcg131"
AIX_2210_V1R3_2            = "/usr/rfcg132"
AIX_2210_MRSV1R1_PTF793    = "/usr/mrsc110"
AIX_2210_MRSV2R1           = "/usr/mrsc210"
AIX_2210_MRSV2R2           = "/usr/mrsc220"
AIX_2210_MRSV3R1_PTF2      = "/usr/lpp/mrsv31"
AIX_2210_DEFAULT           = "/usr/lpp/mrsv31"

# ------------------------------------------
# - Directory MSS Config Tool on UNIX       -
# ------------------------------------------
AIX_MSS_V1R1_0_PTF1        = "/usr/mss110"
AIX_MSS_V1R1_1             = "/usr/mss110"
AIX_MSS_V2R0               = "/usr/mss200"
AIX_MSS_V2R0_1             = "/usr/mss201"
AIX_MSS_V2R1               = "/usr/mss210"
AIX_MSS_DEFAULT            = "/usr/mss210"

# ------------------------------------------
# - Config Tool executable and environment.  -
# - These should not be changed.             -
# ------------------------------------------
AIX_CFG_TOOL_NAME          = "cfg.aix"
CFG_TOOL_NAME              = "cfg.exe"
CFG_TOOL_APP               = "cfg.app"
```

Figure 12. MSS Configuration Sample

4.4.4 Accessing the Device Managers from a Web Browser

There are three components involved in Web browser-based access to the device managers:

- Nways Manager Workstation
- Web Server
- Web Browser - Client

4.4.4.1 Nways Manager Workstation

The Nways Manager maintains the Nways Web pages that are sent from the Web Server to the Web browser clients.

The html file subsys.html, when created during the installation should never be removed. This file is updated each time NetView rediscovers, changes or deletes IP objects. Sometimes the actual device HTML's do not match the list in the subsys.html, this is caused when old or inactive IP interfaces are still present in the NetView database.

4.4.4.2 Web Server

The Java device management applications can be run in client mode on any station connected to the network management station without configuring a Web server. However, for true intranet access through a Web browser you must configure your Web server to locate the Nways Java Management Web pages subdirectory. Web servers supported for the Nways Web access include:

- IBM Internet Connection Secure Server
- Lotus Domino Go Server
- NetScape Enterprise Server
- Apache Server

On the network management station do the following:

1. Assign a new port number for use by the HTTP server (higher than 8000). The default value is 80. This action adds an additional level of security to Web browser access, and prevents port conflicts with other applications using the server. In our sample network, we used 8001.

> **Note**
>
> If you are using the Apache server that is installed with Tivoli NetView, you do not need to change the port number in the httpd.conf file. If you do, you may experience the NetView Web access error.

2. Assign an alias or logical name to the directory in which the HTML pages are stored on the management system. For the Apache server that comes with Tivoli NetView Version 5.1, the default directory for user URLs is /usr/OV/web/httpd/htdocs and the Nways Web pages are stored in the directory /usr/CML/JMA/java/websvr. We created a softlink to the directories by issuing the command:

   ```
   ln -s /usr/CML/JMA/java/websvr /usr/OV/web/httpd/htdocs/nways
   ```

   So the alias name for the Nways directory in the srm.conf file will be:

   ```
   Alias /nways  /usr/OV/web/httpd/htdocs/nways
   ```

3. Verify that the properties assigned to this directory by the server include allowing Web browser access. For the IBM server included with Nways Manager, the default location of the HTTP server definitions is /etc/httpd.conf.

4.4.4.3 Web Access for ATM Manager

Before you can use the ATM Manager via the Web browser you must configure your Web server. The following configuration is for the IBM server shipped with the Nways application.

If you are using the Apache server the following two lines must be added to your /usr/OV/web/httpd/conf/srm.conf file:

```
ScriptAlias      /atm-bin/          /usr/CML/ATMWEB/bin/
Alias            /atm-html/         /usr/CML/ATMWEB/html/
```

For the IBM Internet Connection Server, enter the following in the configuration file of the Web server. Make sure that the two Pass statements are entered in the sequence shown below:

```
Exec             /atm-bin/*         /usr/CML/ATMWEB/bin/*
Pass             /atm-html/*        /usr/CML/ATMWEB/html/*
Pass             /*                 /a directory path/*
```

Reset the Web server by entering the command:

```
refresh -s httpd
```

or use the commands nvwebstop then nvwebstart.

4.4.4.4 JMA Client Access

The Java support is provided with the browser. The Web browser can dynamically load the Java application. For better performance we copied the class definition files to the Web client machines.

1. Copy the following files in directory /usr/CML/JMA/java/websvr/code from the Nways manager workstation to any subdirectory in the Web browser client.

   ```
   ClientClasses.jar
   CommonClasses.jar
   Mlsoft.jar
   ```

2. Set the CLASSPATH environment variable in the Web browser client to include the full path and file name of the copied class files.

   CLASSPATH=*path*\ClientClasses.jar;*path*\CommonClasses.jar;*path*\mlsoft.jar;

   where path is your full path to copied class files.

Java communications use the IP host name and not the IP address; therefore both the client and server need the correct host names with which they are communicating.

If the client dynamically assigns an IP address, ensure that this IP address is associated with your client's IP host name. This process works correctly with Dynamic Host Configuration Protocol (DHCP).

If your client uses the PPP protocol to connect to the server the client will be dynamically assigned both an IP address and an IP host name. In this situation Windows clients such as NT or 95 do not provide the correct IP host name to the Java applications running in the client. Hence, the Java applications will not provide the correct IP host name to the server and the server will not be able to send asynchronous (unsolicited) events to the client.

To correct this problem, change the IP host name on the Windows client to the value localhost for the PPP connection's TCP/IP protocol. The Java code in the Windows client will then provide the server with the correct (dynamically assigned) IP host name.

When you access the Nways Web pages, your browser may ask if you want to allow unsigned applets. To use the Web functions of the Nways Manager, you must allow unsigned applets.

Note

If you are using the HotJava Browser, you must start it using the following parameters:

```
hotjava -mx96M
```

4.4.5 DB2 Universal Database

Performance management for these device managers uses a Java Database Connectivity (JDBC) compliant database. A version of the DB2 database is provided. You will need to create a database instance that can be accessed using JDBC by the device managers.

The following steps show how to do this using DB2:

Use the **smit->Security** and **smit -> Users** menus to add the following users and groups to AIX as described below:

4.4.5.1 Adding the AIX Group

Add the group nwaysdb2. This group will be used for the DB2 Instance and Administrative Server. Using SMIT, the Add Group menu requires the name to be entered first. After entering the name, set the Administrative Group field to True.

4.4.5.2 Adding/Modifying the AIX Users

The following users must be added or modified:

- nwaysdb2 is the DB2 instance owner. Enter the name of the user to be added first, then complete only the following fields:

  ```
  ADMINISTRATIVE USER = true
  Primary group = nwaysdb2
  Group SET = nwaysdb2,system
  ADMINISTRATIVE GROUP = nwaysdb2
  ```

- nwaysadm user is the owner of the administrative server. This value is optional. Follow the same steps used to define the user nwaysdb2, using the user name nwaysadm.

- root must be modified to add nwaysdb2 to the group SET.

  After you have completed these changes, use the following commands to confirm the correct settings of the new group and users:

  ```
  lsgroup nwaysdb2
  lsgroup system
  ```

  All three users should show up as users in both groups.

After you have created these users, select passwords for them and log in as each user to change the temporary status of the root-generated ones. You will need these passwords when configuring DB2, so be sure to write them down.

To begin the installation, mount the CD-ROM using the following command:

```
mount -r -v cdrfs /dev/cd0 /mnt
```

You can install using SMIT or the db2setup script included on the CD. Installing using the script assists you in selecting the components to install and allows you to set up users during installation.

Change the directory to the mount point and run the script db2setup.

```
cd /cdrom
db2setup
```

The DB2 Installer screen will appear.

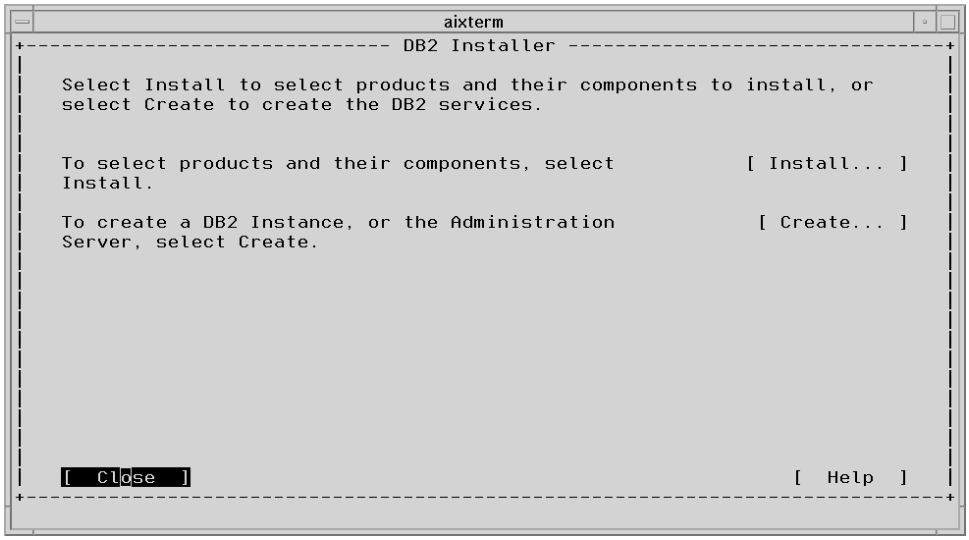


Figure 13. DB2 Installer Program

Select Install for the field Select Products and their components.

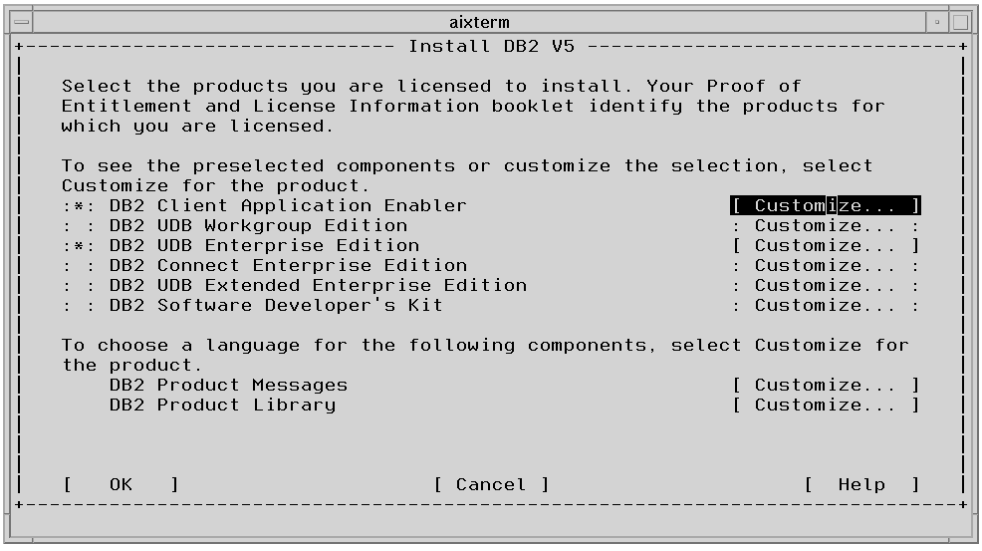


Figure 14. DB2 Installation Panel

Select the Universal Enterprise Database option to install. You can select only one major product group. Use the Spacebar to choose the options. When you have completed a panel click on **OK.**

After the installation is complete you will be asked if you want to create the instance and administrative server. Select **Instance**, then click **Customize** to set up the server. For the instance user, use nwaysdb2 as the user name, nwaysdb2 as the group, and the password you configured earlier. Click **OK** to finish.

You are then prompted to configure another user. Enter the same user you entered above. This is referred to as the fence user.

Note: You will receive a warning that you have used the same user ID for the fence user. Ignore this message.

Use the same procedure to configure the administrative server, using nwaysadm as the user name and nwaysdb2 as the group.

After creating the user, check the ownership of the nwaysdb2.profile. If ownership is not assigned correctly, log on as root and change the ownership of the file $HOME/.profile using the command `chown nwaysdb2:nwaysdb2 .profile`

Note

The next two steps refer to the application of a PTF to DB2. It is strongly recommended that you apply the PTF before configuring DB2 for use with the Nways Manager.

If you choose not to install the PTF now, you can skip the next two steps and complete the installation. If you install the PTF at a later date, you must then rebind the DB2 files.

There is a recommended APAR, JR11296, which addresses a memory leak in the DB2 product. This fix is contained within PTF U452737, which is in turn part of a larger PTF, U452196. You can order this PTF from AIX support, or you can obtain it via:

```
ftp://aix.boulder.ibm.com
http://www.software.ibm.com/data/db2/db2tech/version5.html
```

Select the file:

```
/ps/products/db2/fixes/english-us/db2aixv5/U452196.tar
```

As preparation for the DB2 PTF installation, perform the following steps while logged on as nwaysadm or the selected administrative user to stop DB2:

```
. $HOME/sqllib/db2profile (note the ‘space’ after the dot).
db2 force applications all
db2 terminate
db2 stop
db2licd end
exit
su - nwaysadm
. $HOME/sqllib/db2profile
db2admin stop
exit
/usr/sbin/slibclean
```

Install the PTF using the smit install command and install the following software:

- db2_05_00.client

- db2_05_00.cnvucs
- db2_05_00.conn
- db2_05_00.cs
- db2_05_00.das
- db2_05_00.db2
- db2_05_00.esrv
- db2_05_00.jdbc
- db2_05_00.repl

Log on as nwaysdb2 or issue the command `su - nwaysdb2`.

1. If you have an existing database, you must update the database instances using the following command:

   ```
   /usr/lpp/db2_05_00/instance/db2iupdt nwaysdb2
   ```

2. Add the following lines to nwaysdb2's profile after the existing PATH statements:

   ```
   . sqllib/db2profile
   CLASSPATH=.:$HOME/sqllib/java/db2java.zip
   export CLASSPATH
   ```

3. Activate the new profile.
4. Execute the following command to automatically start the instance on subsequent reboots:

   ```
   db2set -i nwaysdb2 DB2AUTOSTART=YES
   ```

5. Start the DB2 instance:

   ```
   db2start
   ```

6. Start the Command Line Processor (CLP):

   ```
   db2
   ```

7. At the CLP prompt, enter:

   ```
   CREATE DATABASE IBMNMPDB
   ```

   You will need to have about 25MB disk space free in /home filesystem for this to succeed.

8. After the database is successfully created, enter:

   ```
   QUIT
   ```

9. Log in as root and, if the directory /usr/CML/JMA/java/websvr/code was not created during Nways Manager Installation, create it.
10. Move the DB2 JDBC drivers into the Nways class path:

    ```
    cp /usr/lpp/db2_05_00/java/db2java.zip /usr/CML/JMA/java/websvr/code
    ```

11. Use the jar command to unzip the file:

    ```
    cd /usr/CML/JMA/java/websvr/code
    jar -xvf db2java.zip
    ```

12. Modify the existing PATH statement in /etc/environment to include:

    ```
    PATH=/home/nwaysbd2/sqllib/bin:/home/nwaysdb2/sqllib/adm:/home/nwaysdb2/sql
    lib/misc
    ```

13. Add the following lines to /etc/environment:

    ```
    DB2DIR=/usr/lpp/db2_05_00
    ```

```
DB2INSTANCE=nwaysdb2
LD_LIBRARY_PATH=/home/nwaysdb2/sqllib/lib
```

14. In the file /etc/inittab move the following line:

    ```
    rcdb2:2:once:/etc/rc.db2 > /dev/console 2>script
    ```

    immediately before the line below:

    ```
    rctcpip:2:wait:/etc/rc.tcpip > /dev/console 2>script
    ```

15. Edit the files /usr/CML/JMA/bin/dpadmin and /usr/CML/JMA/bin/dpconfig to add the following to the end of both CLASSPATH statements:

    ```
    :/usr/jdk_base/lib/classes.zip
    ```

16. Reboot the machine for the modifications to take effect.

17. Start the Nways Performance Management Configuration applet by entering one of the following commands:

    ```
    /usr/CML/JMA/bin/dpadmin
    /usr/CML/JMA/bin/dpconfig hostname
    ```

    In our sample network, our RS/6000's hostname is rs600033t, so we entered:

    ```
    /usr/CML/JMA/bin/dpconfig rs600033t
    ```

    For more information on using the dpadmin and dpconfig commands, read the associated script files, dpadmin script and dpconfig script.

Note: When you run dpadmin a graphical window is displayed. To use this window, you must have X-access to your console.

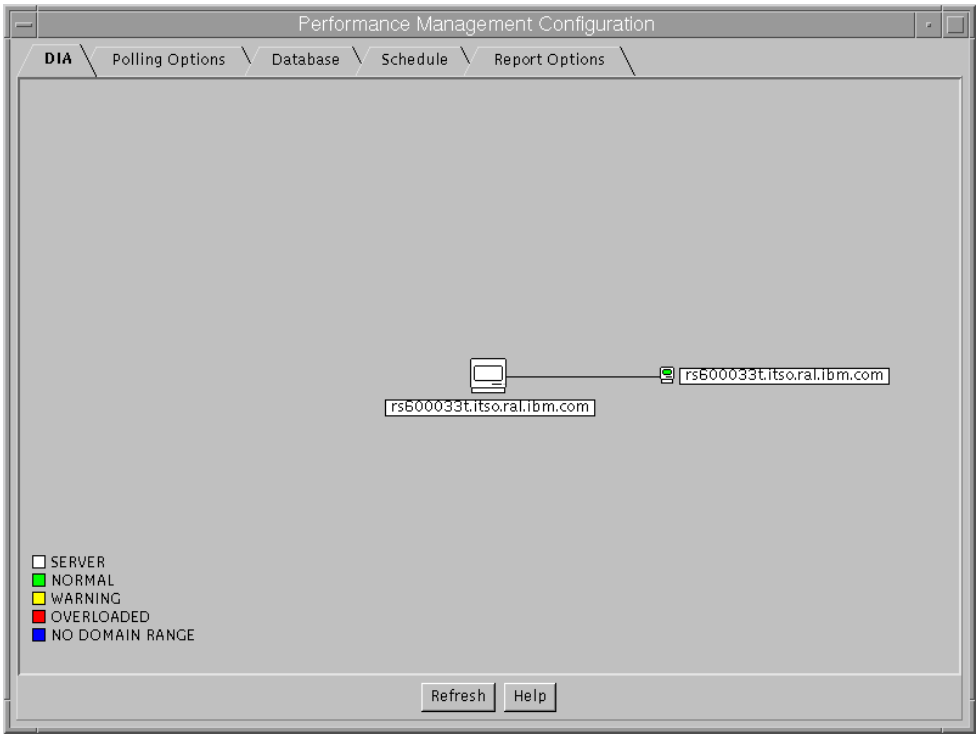


Figure 15. Performance Management Configuration: DIA Topology

From the dpadmin window select the **Database** tab. There are four fields, two are filled for DB2. The third and fourth fields are User id and Password, which can be ignored.

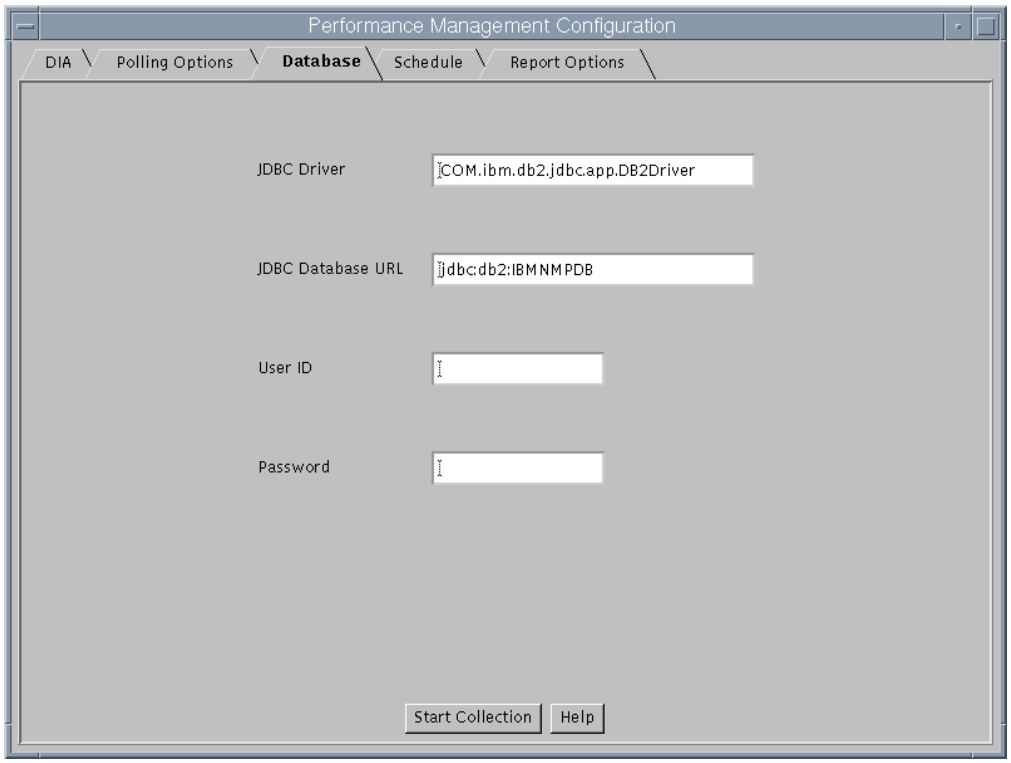


Figure 16. Performance Management Configuration: Database Screen

The dpadmin screens show the polling list, templates, reports, and other features. Once the collection is started, you can close this window and the collection will continue running. To stop the collection, reopen this window and click on **Stop Collection.**

4.4.6 Remote Distributed Intelligent Agents (DIAs)

The Campus Manager LAN component provides DIAs that can be placed in remote Java-enabled workstations to off-load performance management polling for these device managers. Refer to the following file for complete instructions:

```
/usr/CML/JMA/dia/readme.txt
```

Briefly, we performed the following to configure the DIA on AIX:

1. Install 1.1.4 or later version on the DIA target system.
2. Create a DIA directory:

   ```
   mkdir /usr/dia
   ```

3. ftp the following files from the management system to the target system's /usr/dia directory:

   ```
   /usr/CML/JMA/java/websvr/code/LoadDIA.class
   /usr/CML/JMA/dia/runDIA.ksh
   ```

4. Ensure the runDIA.ksh file is executable:

   ```
   cd /usr/dia
   ```

```
chmod 777 runDIA.ksh
```

5. Edit the runDIA.ksh file on the target system as follows:

```
export DIA_JAVA_PATH=/usr/jdk1.1.4/bin/java
export DIA_JAVA_LIBPATH=/usr/jdk1.1.4/lib
export DIA_DIA_PATH=/usr/dia
export DIA_URL=http://rs600027t.itso.ral.ibm.com:8001/nways
export DIA_NWAYS_SERVER=rs600027t.itso.ral.ibm.com
export DIA_ECHO=/usr/bin/echo
$DIA_JAVA_PATH -classpath /usr/jdk1.1.4/lib/classes.zip:$DIA_DIA_PATH LoadDIA
$DIA_URL/code/ -serverHostname $DIA_NWAYS_SERVER
```

6. Execute the script:

```
./runDIA.ksh
```

   You should see the following messages:

```
Waiting for tracer service to get ready
Tracer service is now ready
Bound successfully to the server ...
```

You should now see the DIA on the JPM screen on the management station. Click on **Refresh** to update if necessary.

4.4.7 Remote Monitor

Before you can use Remote Monitor, you must set the RMONHOME environment variable to point to the directory where it was installed by default this is the directory /usr/LANReMon/rmon. To set the RMONHOME environment variable in your .profile and add it to your default path, add the following to your .profile:

```
RMONHOME=/usr/LANReMon/rmon
export RMONHOME
PATH=$RMONHOME:$PATH
export PATH
```

You can also add the directory to the PATH statement in /etc/environment and include the RMONHOME=/usr/LANReMon/rmon statement.

4.4.8 Traffic Monitor

Before you can use Traffic Monitor, you must set the TRAFFICMONHOME environment variable to point to the directory where it is installed, by default this is in /usr/LANReMon/trafficmon. To set theTRAFFICMONHOME environment variable in your .profile and add it to your default path, add the following to your .profile:

```
TRAFFICMONHOME=/usr/LANReMon/trafficmon
export TRAFFICMONHOME
PATH=$TRAFFICMONHOME:$PATH
export PATH
```

Also you can add the directory to the PATH statement in /etc/environment and include the TRAFFICMONHOME=/usr/LANReMon/trafficmon statement.

4.5 Verifying the Nways Installation

This section shows how we verify the installation and check that the applications are functioning correctly.

The first time you start an application, be sure to log on as the root user. To start the Nways Manager applications, enter the command `nv6000`.

The NetView root map is displayed. From here we can launch the Nways Manager applications.

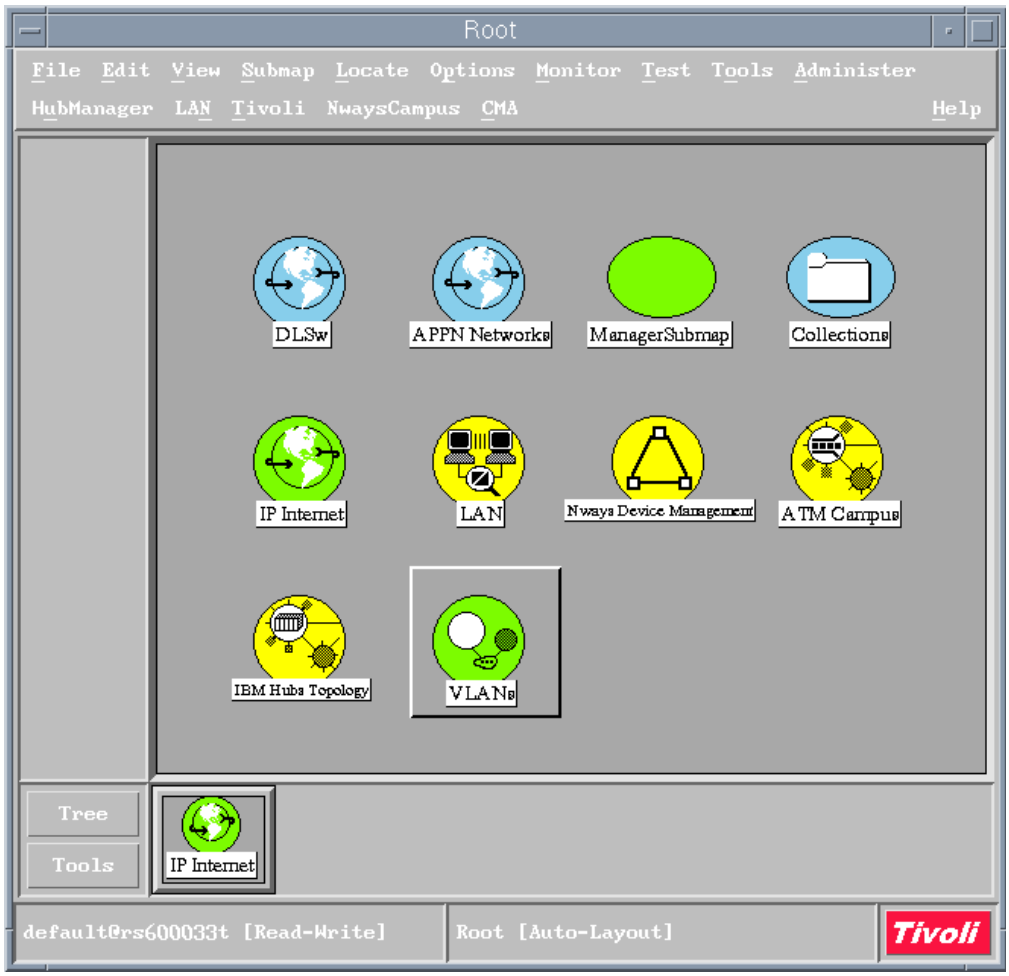


Figure 17. Main NetView Screen: Root Map

Each submap is detailed further in Chapter 5, “Status and Configuration Using Nways Manager” on page 73.

4.5.1 NetView Process Status

After the NetView user interface was started all the required NetView and Nways processes should have the status of running. There are three common methods to check the status of these processes:

Issue ovstatus from the command line or using smit select **SMIT --> Communications --> TME 10 NetView --> Control -->Display TME 10 NetView Status --> Display status of daemons**

From NetView web access, use the browser to check the NetView processes from the link:

`http://Hostname/NetViewTemplate/TME10/NetView/Daemons/SubApplication.html`

The browser will show the NetView Process status as Figure 18.

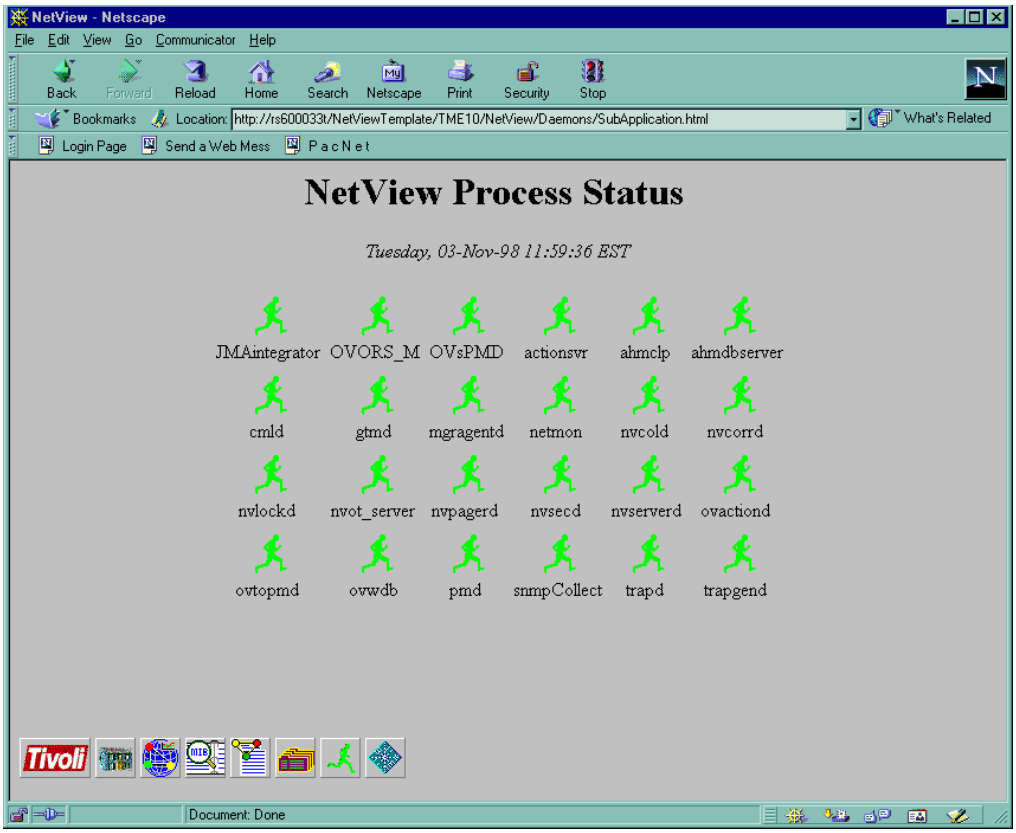


Figure 18. NetView Process Status by Web Access

You can check the Nways processes by issuing the command:

`/usr/CML/bin/cmlstatus.`

4.5.2 Web Access to Nways Manager

To use the Web browser to access the Nways Manager function, use the following Web page:

`http://hostname:rs600033t/Nways/SubSys.html`

The Nways Java Management SubSystem can also be accessed from the NetView main screen as shown in Figure 19 on page 57.

Note: SubSystem.html cannot be used across a remote link.

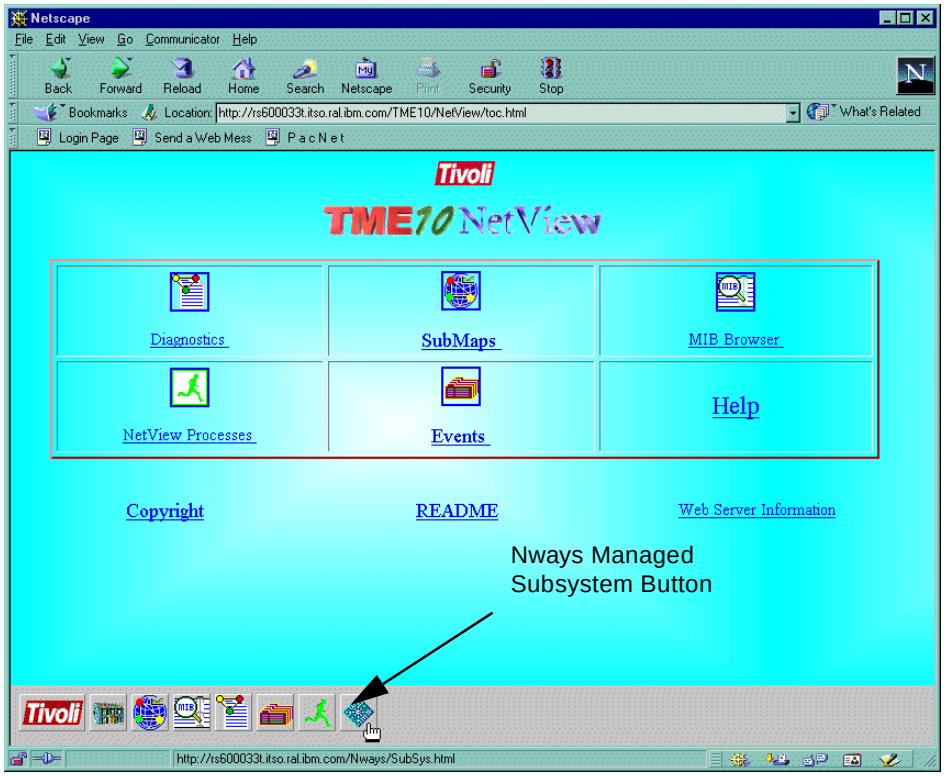


Figure 19. TME 10 NetView Web Interface: Main Screen

When you click on the **Nways Managed Subsystem** button, Figure 20 on page 58 will appear.

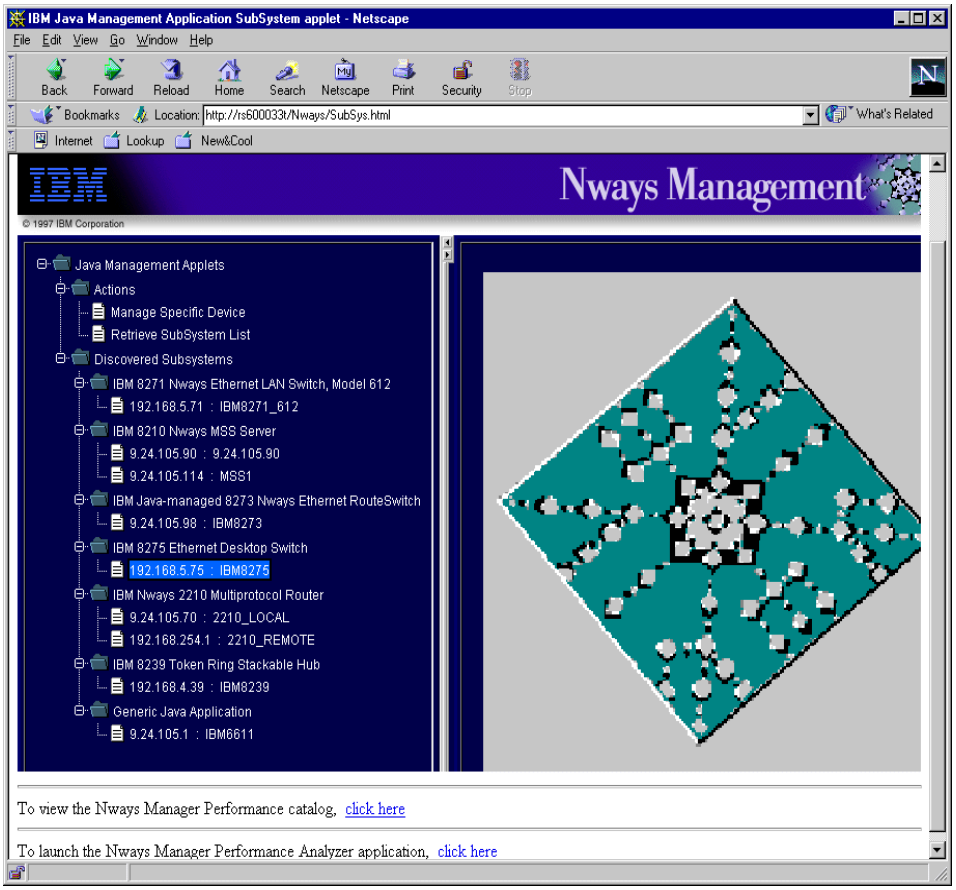


Figure 20. Nways Java Management SubSystem Applet

Click on **Retrieve Subsystem List** and select one of devices listed. Next click on **Apply**. We selected the 8275 JMA, (see Figure 21 on page 59).

Figure 21. Nways Java Management Application: IBM8275

Starting the JMA confirms that the java daemons are running correctly.

4.5.3 Web Access to the ATM Manager

To use the Web browser to access the ATM Manager function, use the following Web page:

`http://rs600033t/atm-html/AtmWebMngt.html`

In our sample network, the RS/6000's hostname is rs600033t and for the port number we used the default value of 80 (see Figure 22).

Figure 22. ATM Web-Based Manager

From here we can view the ATM topology and the function menus from the browser.

4.6 Community Names

Problems that may occur during discovery can be related to incorrect community names having been set up. The following sections show where the community names are configured for our devices.

4.6.1 8260/CPSW

To configure the SNMP and trap configuration for the 8260/65 use the commands show community and set.

```
8260> show community
Index Community_Name  IP_Address            Accesses
--------------------------------------------------------------------------------
   1  public          ***.***.***.***   Read -No write-No trap
   2  public          9.24.105.115      Read -No write- Trap
   3  public          9.24.105.113      Read -No write- Trap
   4  private         9.24.105.113      Read -  Write -No trap
   5  private         9.24.105.115      Read -  Write -No trap
   6  public          9.24.105.246      Read -No write- Trap
   7  private         9.24.105.246      Read -  Write -No trap

8260> set community public 9.24.104.246 all
```

Figure 23. SNMP Access for the CPSW

By using the set community command we can set the read/write access and the trap destination for our management station by selecting all.

4.6.2 IBM 8210

To set the community details for the MSS use the commands shown in Figure 24. These commands are entered using talk 6.

```
MSS1> prot snmp
MSS1>set community access write_read_trap
MSS1>add address public 9.24.104.246 255.255.255.0

MSS1> SNMP Config>list all

      Community Name          IP Address        IP Mask
-------------------------------  ---------------  ---------------
public                       9.24.105.115     255.255.255.255
                              9.24.105.246     255.255.255.255
private                      9.24.105.246     255.255.255.255

       Community Name               Enabled Traps
-------------------------------  --------------------------------
private                      None
public                       Cold Restart, Warm Restart,
                              Link Down, Link Up,
                              Authentication Failure,
                              EGP Neighbor Loss, Enterprise Specific

       Community Name                 View
-------------------------------  --------------------------------
private                                 All
public                                  All
```

Figure 24. SNMP Access fpr the 8210

Using the command set community and add address we defined the SNMP and trap parameters for our management station.

4.6.3 8271 Model 108

Access to the community menu by using telnet is shown in Figure 25 on page 62.

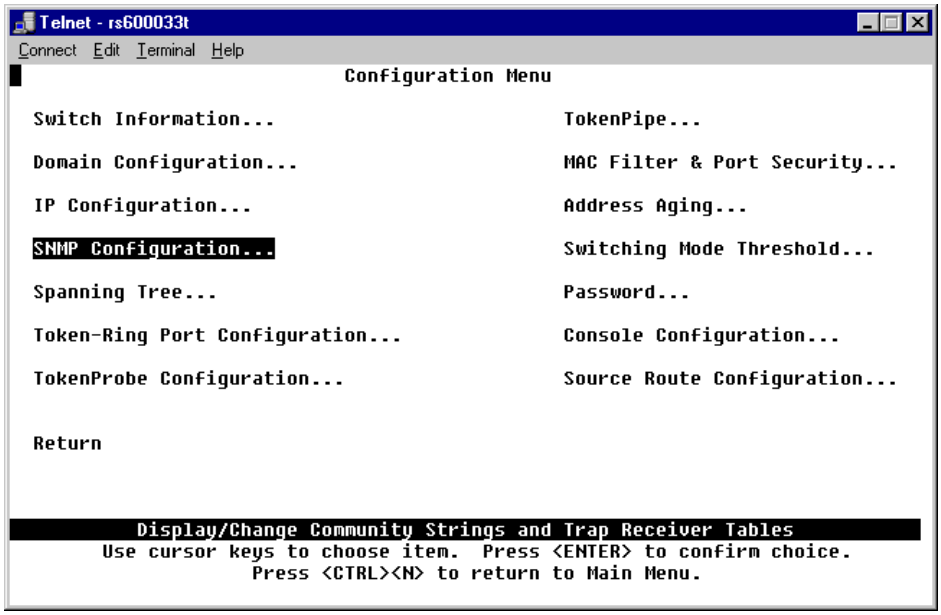


Figure 25. 8271 SNMP Access

Select **SNMP configuration** followed by **Return** (see Figure 26 on page 62).

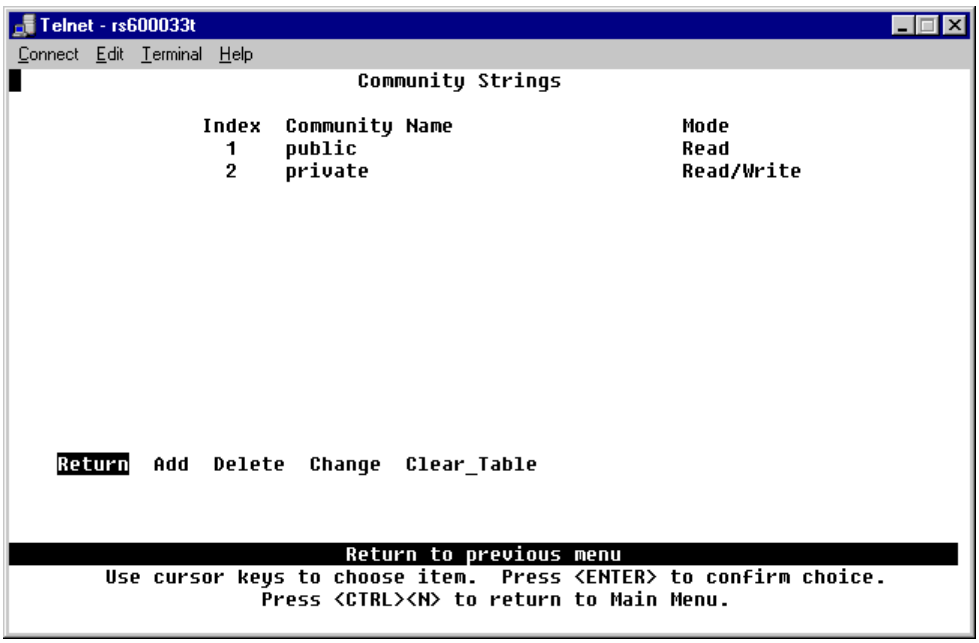


Figure 26. SNMP Access for the 8271

Here we added the community names by clicking on **Add**.

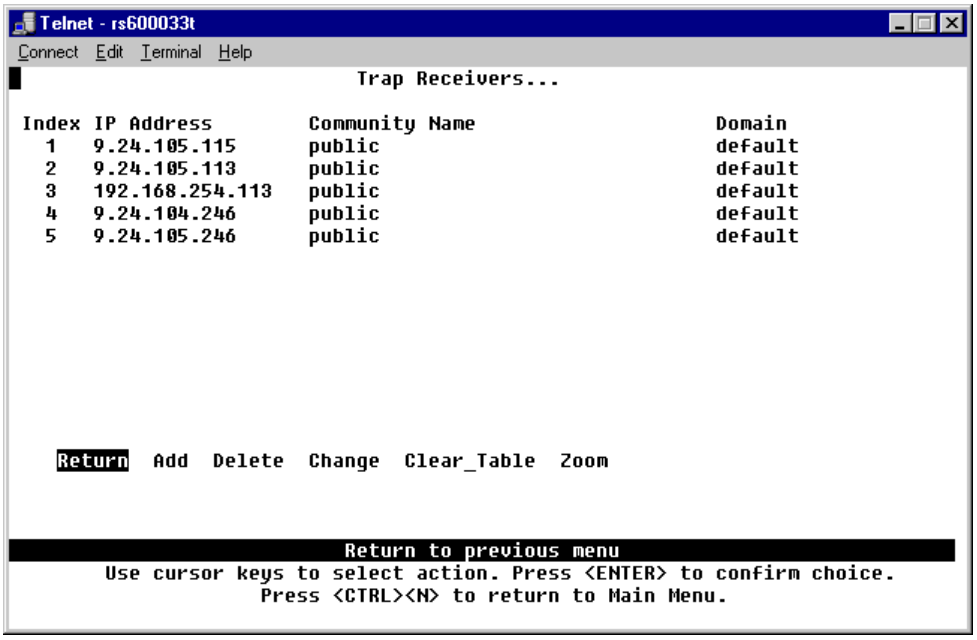


Figure 27. 8271 - Setting the Trap Destination

Figure 27 on page 63 shows where to enter the IP address of the management station.

4.6.4 8273/4

The 8274 is accessed by menus; here we used telnet. The SNMP configuration is performed using the command snmpc, (see Figure 28 on page 63).

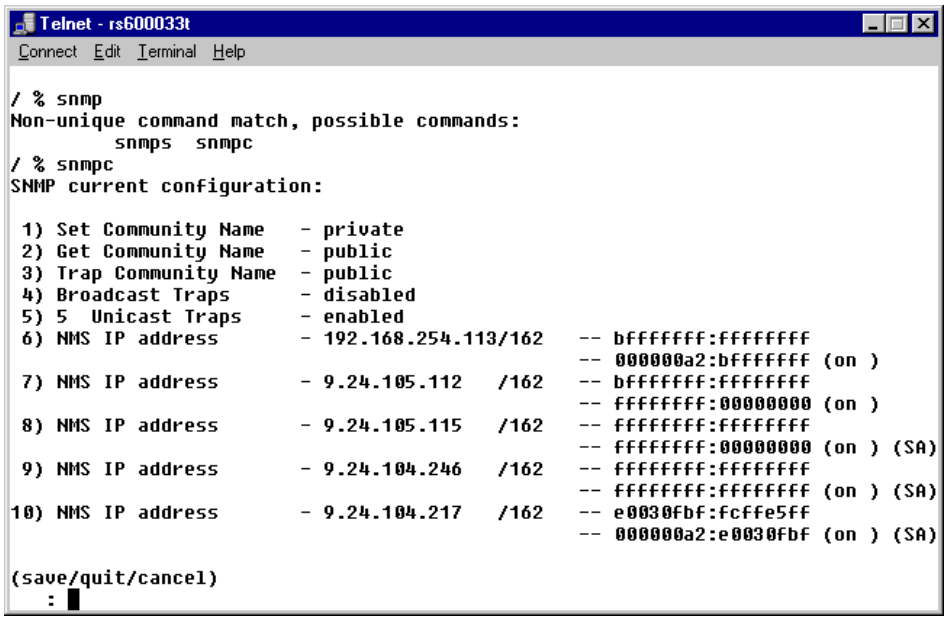


Figure 28. SNMP Configuration for the 8273/4

All of the SNMP configuration is performed from here.

4.6.5 8271 Model 612

To access the SNMP and Trap configuration for the 8271 we used telnet. The initial configuration screen is shown in Figure 29.

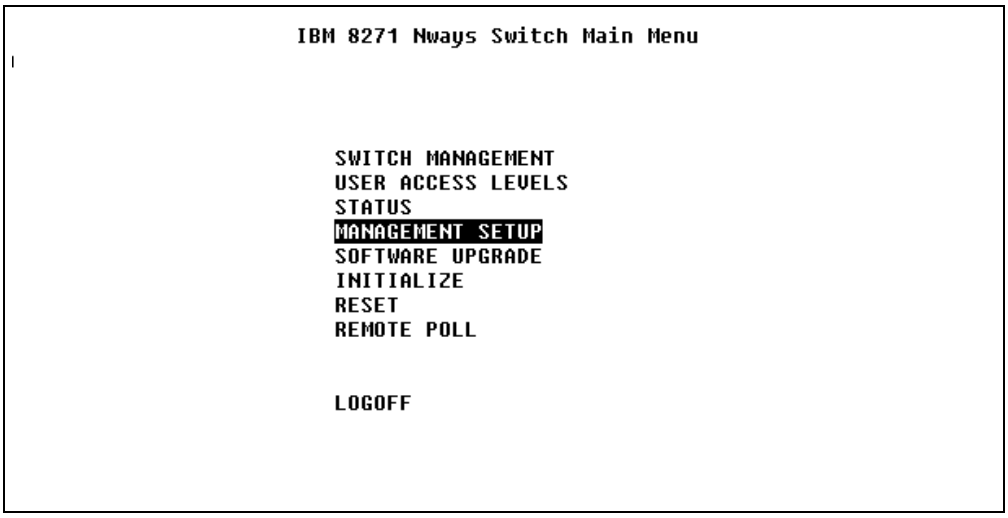


Figure 29. SNMP Access for the 8271 Model 612

Select **MANAGEMENT SETUP** followed by pressing **Return**, (see Figure 30 on page 64).

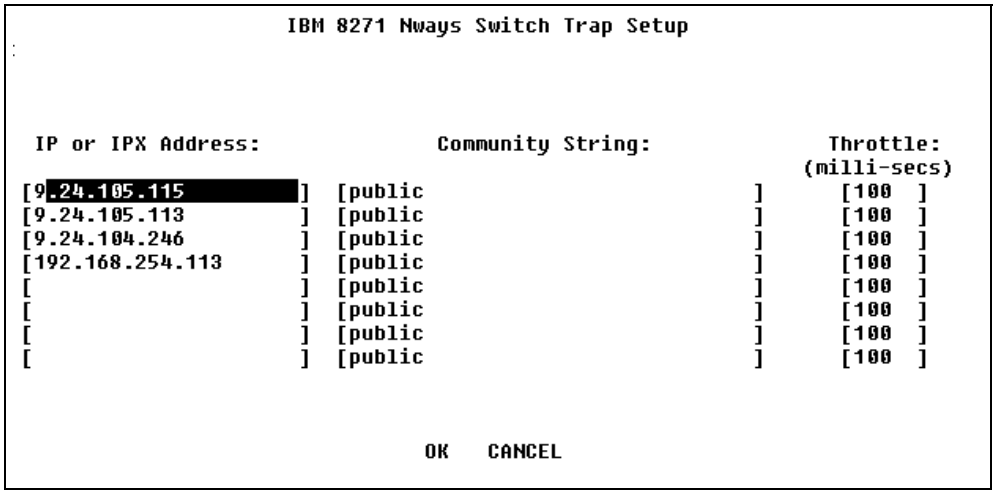


Figure 30. Community Name Configuration for the 8271 Model 612

We entered the IP address of the NMS and the community name. Finally we selected **OK**.

4.7 Useful Commands

Below are some useful commands we used during the project:

cmlstatus Shows active daemons for Nways Managers

ovorsutil -d Produces a formatted listing of all the entries in the object registration service database. Each active entry will be formatted and sent to standard output.

ovstatus Displays the NetView daemon status.

netstat -a Displays socket information.

netstat -i Displays the configured interfaces.

netstat -I tr0 Shows the status of a token-ring card.

netstat -m Shows memory information.

netstat -rn Shows routing information.

netstat -v Shows statistics.

nslookup Resolves the host name for the IP address in the domain name server.

iptrace Traces IP packets.

traceroute Traces a route from the NMS to a given destination.

ovobjprint -s Prints the objects contained in the NetView database.

osvrping Pings the object store server.

osverifydb Verifies the object store database.

snmpwalk Tests SNMP connection to a device by interrogating the MIBS.

Some AIX Commands include:

lspv hdisk0 Checks disk space on the AIX.

lsdev -Cc "memory" Lists memory for the AIX server.

lsps -a Shows paging space on the AIX server.

lsattr -El'sys' Lists system attributes for the AIX server.

no -a Lists system parameters such as IPFORWARDING.

Also for the Tivoli Framework we used the odadmin odlist command to display our TMR server connection.

4.8 Accessing README Files and Online Documentation

The following README files are also installed:

Campus Manager LAN - /usr/lpp/cml/lpp.README
Distributed Intelligent Agent - /usr/CML/JMA/dia/readme.txt
Campus Manager ATM - /usr/lpp/ahm6000/lpp.README
Remote Monitor - /usr/lpp/lanReMon/lpp.README
Traffic Monitor - /usr/lpp/trafficMon/lpp.README

Information about how to use ObjectStore is located in the file:
`/usr/lpp/ODI/OS5.0/common/doc/mo/index.htm`

After starting Nways Manager you can access the online user guides for the Nways applications. For Campus Manager LAN select **Help -> Campus Manager -> LAN User's Guide**. The following can be accessed:

- 8250 Multiprotocol Intelligent Hub Device Manager

- 8260 Nways Multiprotocol Switching Hub Device Manager
- 8265 Nways ATM Switch Device Manager
- FDDI Management using 8244 FDDI Workgroup Concentrator
- SNMP Bridge/Switch Manager
- Token-Ring Management accessing LAN Network Manager for OS/2
- Token-Ring Management using SNMP Token-Ring Devices

For the ATM components select **Help->Campus Manager->ATM User's Guide** to access on line documentation for the following applications:

- ATM Manager
- LAN Emulation Manager
- Remote Monitor and Traffic Monitor

Use the Acrobat Reader 3.0 to access the online documentation about the IBM 8260 LAN Switching Modules Series called:

```
/usr/CML/doc/cml.nsmm.pdf
```

For the hub manager select **Help->IBM Device Managers User's Guide** to access the documentation for the following applications:

- 6611 Network Processor Router Device Manager
- 8224 Ethernet Stackable Hub Device Manager
- 8225 Fast Ethernet Stackable Hub Device Manager
- 8230 Token-Ring Controlled Access Unit Device Manager
- 8235 Dial-In Access to LANs (DIALs) Server Device Manager
- 8237 10BASE-T Stackable Ethernet Hub Device Manager
- 8238 Token-Ring Stackable Hub Device Manager
- 8270 Nways Token-Ring LAN Switch Device Manager
- 8271 EtherStreamer/Nways Ethernet LAN Switch Device Manager
- 8272 LANStreamer/Nways Token-Ring LAN Switch Device Manager
- 8273 Nways Ethernet RouteSwitch Device Manager
- 8274 Nways LAN RouteSwitch Device Manager
- 8276 Nways Ethernet RoutePort Device Manager
- 8281 Nways ATM LAN Bridge Device Manager
- 8282 Nways ATM Workgroup Concentrator Device Manager
- 8285 Nways ATM Workgroup Switch Device Manager
- Generic Java-based device management for the non-IBM SNMP devices
- IBM Token-Ring and Ethernet Adapter Manager

Select **Help->NetView** for access to the AIX Library. From here you can access the documentation for the following applications:

- Data Link Switching Topology
- APPN Topology
- Management Application Transporter
- Campus Manager - ATM

Use the Acrobat Reader 3.0 to access documentation for Remote Monitor and Traffic Monitor, these are listed below:

```
/usr/LANReMon/doc/ecam.pdf
/usr/LANReMon/doc/ttmm.pdf
/usr/LANReMon/doc/lanremon.pdf
/usr/LANReMon/doc/traficMon.pdf
/usr/LANReMon/doc/tmInstall.pdf
```

4.8.1 Acrobat Reader Installation

To install the Acrobat Reader 3.0 from the CD-ROM:

1. Extract the files from the aixreader.tar file located in the directory /cdrom/acrobat using the following commands:

   ```
   mkdir /usr/acrobat
   cd /usr/acrobat
   tar -xvf /cdrom/acrobat/aixreader.tar
   ```

2. Type `INSTALL`.
3. When prompted, enter the installation directory. By default it is `/usr/lpp/Acrobat3`.
4. Update your .profile with the Acrobat Reader installation directory:

   ```
   export PATH=$PATH:/usr/lpp/Acrobat3/bin
   ```

To start Acrobat Reader 3.0 enter the command `acroread` to access the pdf files.

4.9 Removing Nways Manager Applications

To remove Nways Manager applications follow the steps below:

1. Log in as the root user.
2. Make sure that you have stopped all NetView daemons.
3. From the SMIT main menu, click on **Communications Applications and Services**.
4. Select **Nways Campus Manager**.
5. Select **Maintain.**
6. Select **Campus Manager general maintenance**.
7. Select **Remove Nways Campus Manager Software**.

If you want to remove selected components, use the option that appears under the Campus Manager general maintenance menu.

Note: This procedure will not remove the Router and Bridge Manager component of Nways Campus Manager LAN, nor will it remove the Nways Remote Monitor. To remove these applications:

1. Log in as the root user.
2. Make sure that you have stopped all the NetView daemons.
3. At the prompt, enter `smit`.
4. From the SMIT main menu, click **Software Installation and Maintenance**. The software Installation and Maintenance menu is displayed.
5. Select **Software Maintenance and Utilities**.
6. Select **Remove Installed Software**.
7. In the Remove Installed Software window, select the filesets for the component you want to remove and then select **OK**. Filesets are listed in the following section.
8. Select **Exit -> Exit SMIT** from the menu bar to exit SMIT.

During the removal procedure, the removal and de-configuration steps are displayed in the SMIT window. These steps are logged in the smit.log file and in the log files for each component.

4.9.1 Removing the Filesets

In order to remove Nways Manager for AIX Version 1.2.2 applications, you must specify the filesets in each component.

Table 10. Campus Manager - LAN Filesets

Campus Manager - LAN Filesets		
R8281s10.obj	cml.8274	mgtapptran.book.obj
R8282s10.obj	cml.base	mgtapptran.obj
R8285s10.obj	cml.baseLan	nwaysmgr.jma
alertman.obj	cml.books	ostore_runtime.base
cml.8224	cml.br	rabm.obj
cml.8225	cml.COMM	rabmappn.obj
cml.8230	cml.fddi	rabmbook.obj
cml.8235	cml.Jcomm	rabmclt.obj
cml.8235-2	cml.Jjim	rabmdlsw.obj
cml.8237	cml.license.cat	smcfg.dtext.En_US.eui.obj
cml.8238	cml.license.ncml	smcfg.eui.obj
cml.8250-60	cml.lnme	smmlm.subagent.obj
cml.8271-1	cml.tr	
cml.8271-108	dtext.brwsr.obj	
cml.8272		

Table 11. Campus Manager - ATM Filesets

Campus Manager - ATM Filesets		
ahm6000.atmweb	cml.Jcomm	cml.license.ncma
ahm6000.base	cml.Jfault	cml.vnet
ahm6000.books.En_US.base	cml.Jpnni	dtext.brwsr.obj
cml.base	cml.license.cat	ostore_runtime.base

Table 12. Remote Monitor and Traffic Monitor Filesets

Remote Monitor Filesets	Traffic Monitor Filesets
cml.license.cat	cml.license.cat
lanReMon.base.obj	trafficMon.En_US.books
cml.license.rmon	cml.license.traffic
lanReMon.En_US.books	trafficMon.traffic_Mon
lanReMon.advance.obj	rmonCommon.rmon_Common
rmonCommon.rmon_Common	

4.9.2 Log Files

During the installation or removal procedures, the output that is displayed on the screen is also logged. Table 13 lists the log files.

Table 13. List of Log Files

Log Files Directories	
Component and Directories	**Log Files**
Campus Manager - LAN log files: /usr/CML/install_log /usr/CML/deinstall_log	R8281s10.obj.log ahm6000.R8282s10.obj.log R8285s10.obj.log cml.8224.log cml.8225.log cml.8230.log cml.8235.log cml.8235-2.log cml.8237.log cml.8238.log cml.8250-60.log cml.8271-1.log cml.8271-108.log cml.8272.log cml.8274.log cml.base.log cml.baseLan.log cml.books.log cml.br.log cml.COMM.log cml.fddi.log cml.lnme.log cml.smm.log cml.tr.log nwaysmgr.jma.log
Campus Manager - ATM: /usr/CML/install_log /usr/CML/deinstall_log	ahm6000.base.log cml.base.log
Remote Monitor:: /usr/LANReMon/install_log /usr/LANReMon/deinstall_log	lanReMon.base.obj.log lanReMon.advance.obj.log rmonCommon.rmon_Common.log
Traffic Monitor: /usr/LANReMon/install_log /usr/LANReMon/deinstall_log	trafficMon.traffic_Mon.log rmonCommon.rmon_Common.log
Management Application Transporter: /usr/lpp/mgtapptran/install_log /usr/lpp/mgtapptran/deinstall_log	mgtapptran.obj.log

4.10 Migration

If you are installing IBM Nways Manager for AIX Version 1.2.2 components over previous versions, follow the instructions in this chapter to maintain your current configuration.

4.10.1 ObjectStore

ObjectStore Version 5.0 is automatically installed when you install Nways Manager for AIX Version 1.2.2 Campus Manager - LAN and Campus Manager - ATM. If you already have ObjectStore Version 4.0 installed, you must modify the following parameters before installing the Campus Manager - LAN or Campus Manager - ATM components:

- The OS_ROOTDIR variable is located in:

  ```
  /etc/environment
  /etc/profile
  your $HOME/.profile
  ```

  Locate the correct file, and edit the line that defines the OS_ROOTDIR variable to point to the new version of ObjectStore as shown:

  ```
  export OS_ROOTDIR=/usr/lpp/ODI/OS5.0/cset
  ```

- In the .profile file delete $OS_ROOTDIR/bin from the line that defines the PATH variable for example:

  ```
  export PATH=$PATH:$OS_ROOTDIR/bin
  ```

4.10.2 Nways Manager - LAN

If you have not previously installed Nways Manager for AIX Campus Manager - ATM, you can install the Nways Manager for AIX Version 1.2.2 Campus Manager - LAN component over IBM Nways Campus Manager LAN for AIX Version 3.2 or higher (part of IBM Nways Manager for AIX Version 1.1). You will not lose the current configuration.

If you install Nways Manager for AIX Version 1.2.2 Campus Manager - LAN component over versions earlier than IBM Nways Campus Manager LAN for AIX Version 3.2, you must first completely remove the old Nways Campus Manager LAN version (and the old Nways Campus Manager ATM version, if also installed).

To remove the old Nways Campus Manager versions refer to the installation instructions that came with that version.

The Nways Manager for AIX Version 1.2.2 Campus Manager - LAN component can operate only with the IBM Nways Manager for AIX Version 1.2.2 Campus Manager - ATM component that is provided with it.

4.10.3 Nways Manager - ATM

If you install the Nways Manager for AIX Version 1.2.2 Campus Manager - ATM component over versions earlier than IBM Nways Campus Manager ATM for AIX Version 2.2, you must first completely remove the old Nways Campus Manager ATM version (and the old Nways Campus Manager LAN version, if also installed). If you do not remove the old installation, you will lose your current configuration.

To remove the old Nways Campus Manager versions refer to the installation instructions that came with that version.

The Nways Manager for AIX Version 1.2.2 Campus Manager - ATM component can only operate with the IBM Nways Manager for AIX Version 1.2.2 Campus Manager -LAN component that is provided with it.

4.10.4 Remote Monitor

You can install the Nways Manager for AIX Version 1.2.2 Remote Monitor component over all previous versions of Nways Campus Manager Remote Monitor or Nways Campus Manager Remote Monitor Advanced without losing your current configuration.

4.10.5 Traffic Monitor

You can install the Nways Manager for AIX Version 1.2.2 Traffic Monitor component over Nways Traffic Monitor Version 1.1 (part of Nways Manager for AIX Version 1.1) without losing your current configuration.

Chapter 5. Status and Configuration Using Nways Manager

This chapter covers the specific configuration of the Nways application for AIX by showing examples of how to use the applications. Here we customized the applications in order to manage our network scenario. The two areas covered are Status, what and where we can see status views of the network devices and Configuration, how to change and view the configuration of the managed devices.

We also show an example of how to use the tools to recognize a problem on an ATM connection.

5.1 Status Monitoring

Status monitoring is the ability to view the status of the network components for availability. First we only discovered the nodes we were interested in seeing. Also there is a number of tasks we performed to set up the environment.

The applications we use for status monitoring are:

- JMA(s)/PSMs
- NetView
- SNMP Bridge Manager
- ATM/ELAN Manager
- 8260 Hub Manager
- RouteVision

Before we start with the status applications we describe the status colors and where these are defined for NetView.

5.1.1 NetView Object Status

Table 14 on page 73 shows the possible status of an object under NetView, although other applications may not use all of them.

Table 14. NetView Object Status

Status	Meaning	Icon Color	Connection Color
Unknown	The object status cannot be determined.	Blue	Black
Normal	The object is in normal operational state.	Green	Black
Marginal	The object has at least some unsatisfactory condition.	Yellow	Yellow
Critical	The object is not functioning.	Red	Red
Unmanaged	The object status is not being monitored or managed.	Wheat	Wheat
Acknowledged	The object status is marginal or critical, but you acknowledge it and ignore the status.	Dark Green	Black
User Status 1	Defined by the administrator.	Pink	Black

Status	Meaning	Icon Color	Connection Color
User Status 2	Defined by the administrator.	Violet	Black

On the NetView EUI and Nways panels there is a legend that can be viewed by selecting **Menu bar Help --> Legend.** The legend is shown in Figure 31 on page 74.

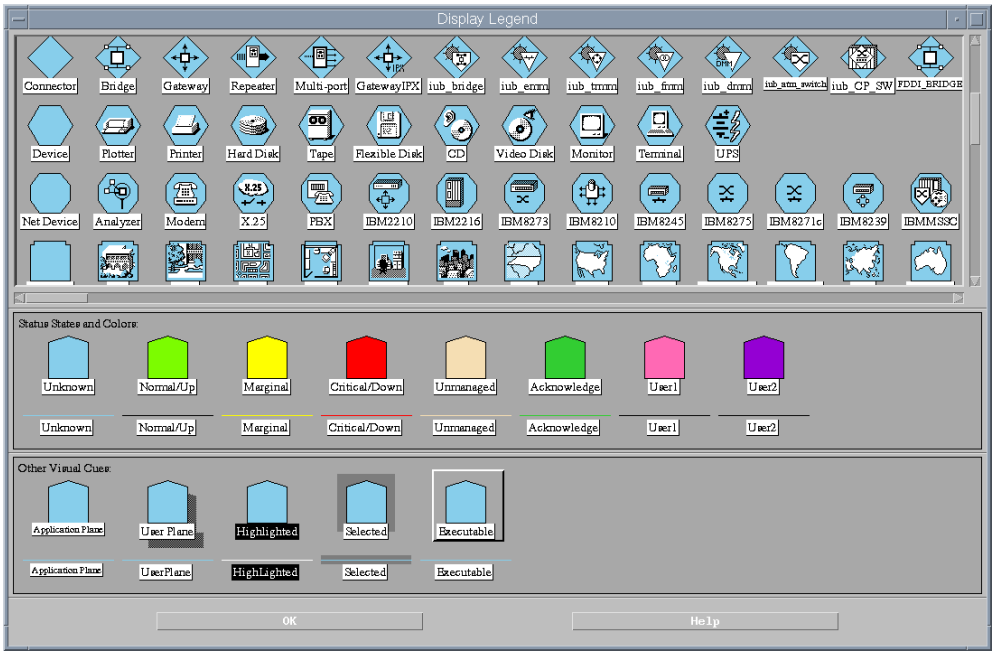


Figure 31. NetView Legend

Here we can also see the Nways symbols that have been installed.

5.1.2 Limited Network Discovery

The first task is to discover our network. After starting the NetView application we realized that some of our IP subnets were heavily populated with IP devices, mostly workstations. In order to avoid the additional overhead of polling and managing non-critical nodes we created a seedfile. This file is located in the directory /usr/OV/conf. This will restrict the Netview discovery to the devices that we want to manage.

The alternative to a seedfile option is to unmanage or hide objects on the NetView submaps using the pull-down menus, although this will still store information about the objects in the NetView database, using up unnecessary resources in terms of memory, cache, disk space.

Our seedfile contained the IP addresses of our critical devices such as hubs, switches and routers, that were part of our lab environment. Figure 32 on page 75 shows the seedfile contents.

Figure 32. Our Seedfile

To activate the seed file run smit nv601aa. Then select **Set Options for netmon daemon**, (see Figure 33 on page 75).

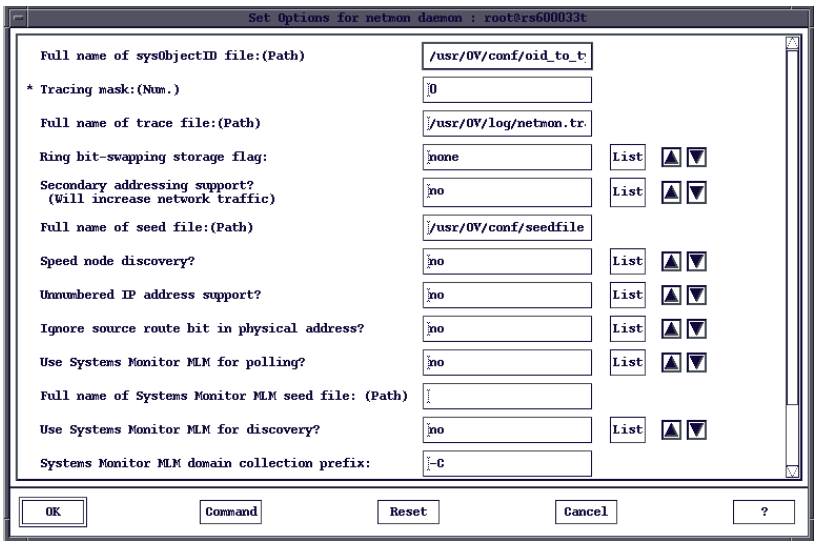


Figure 33. Netmon Settings

Enter the name of the seedfile and select **OK**.

Also the option exists to limit the discovery to Nways Campus Manager LAN components. This is implemented using the same principal as NetView discovery, but is narrowed down to just the Nways discovery. This gives more control to Nways, so an SNMP agent for a device could be discovered by NetView, but will not be managed by Nways and will not appear in Nways submaps.

We also stopped NetView from discovering new nodes by changing the option Discover New Nodes as shown in Figure 34.

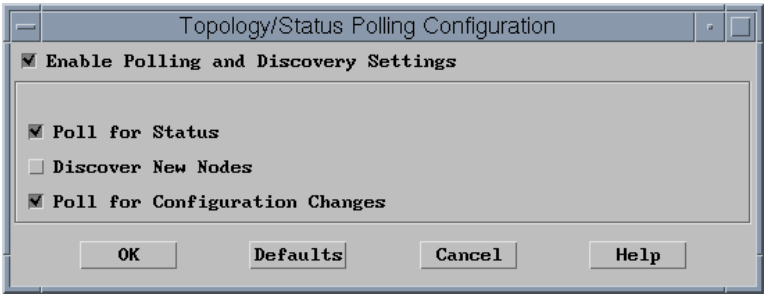


Figure 34. nmpolling Options

This screen is called by issuing the command nmpolling.

When the NetView application is started the initial discovery takes place. Once this has completed our main NetView screen is shown in Figure 35 on page 76.

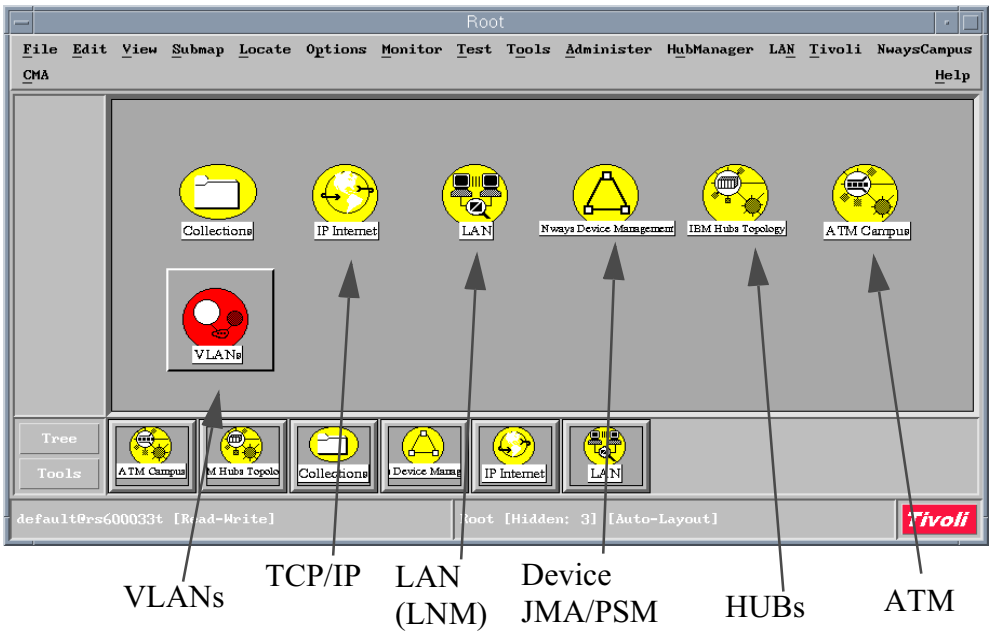


Figure 35. SubMaps After Nways Campus Manager LAN and ATM Installation

From this submap we can access all the management tools.

5.1.3 TCP/IP

The root submap contains the high-level view of the network, where you can drill down through the submaps to get IP network views, Hub views, module views, ports and several management options such as, configuration, fault and performance management. Also, you will see under the NetView pull-down menu three items. These are Hub Manager, NwaysCampus and CMA. Each of these submaps explained in detail further later in this chapter. Figure 36 on page 77 shows the IP network.

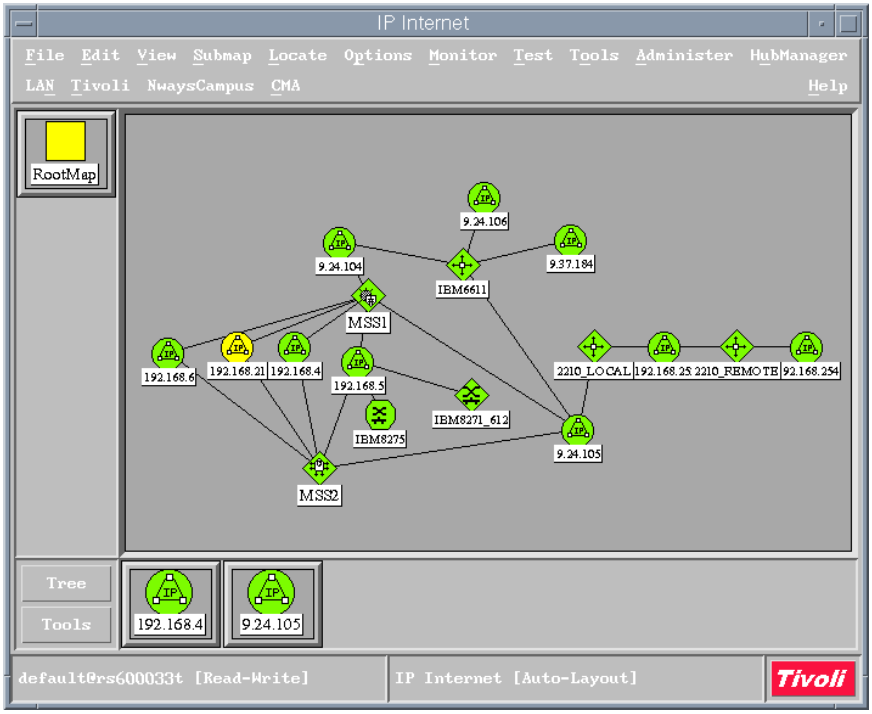


Figure 36. IP Internet Network Level View

The IP Internet submap is of interest to the network management personnel, as it depicts the IP networks and subnetworks. Drilling down the IP Internet submap, views can be seen on the entire IP topology including IP hosts, and workstations.

If we double-click on the submap icon **9.24.105** we can see our devices with IP addresses as part of the subnet 9.24.105. (See Figure 37 on page 78).

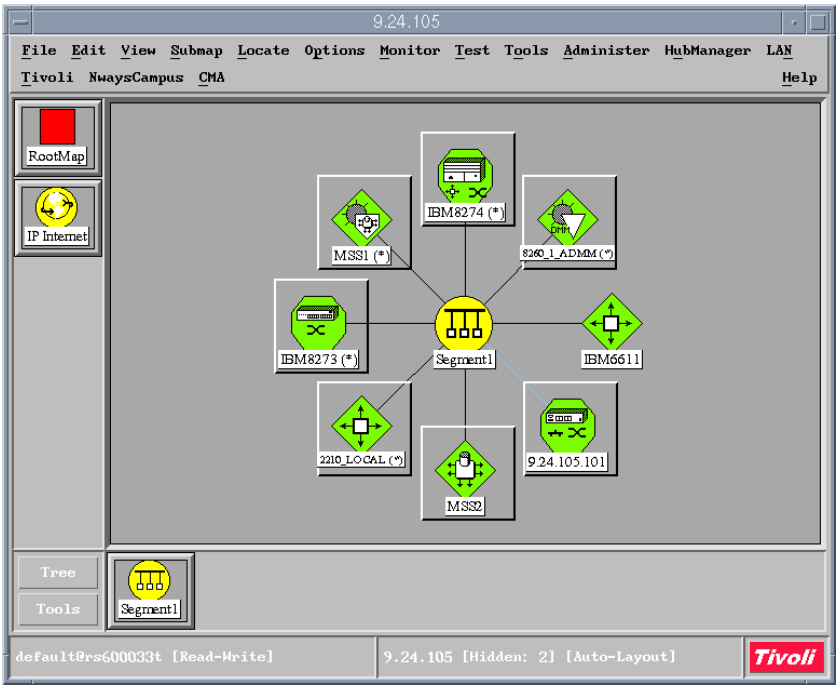


Figure 37. TCP/IP Status for Subnet 9.24.105

5.1.4 LAN

The LAN submap is used to access the LAN Network Manager (LNM) components that manage token-ring LANs, bridges, and FDDI LANs. The LAN view is built by LNM, using the bridge definitions and LAN configuration as reported by information gathered from the MIBs that are supported by the LNM-capable SNMP agents in the network. The submap label is derived from the spanning tree base root address which explains how the bridging devices end up in the same submap.

Click on the LAN icon from the root submap (see Figure 38 on page 79).

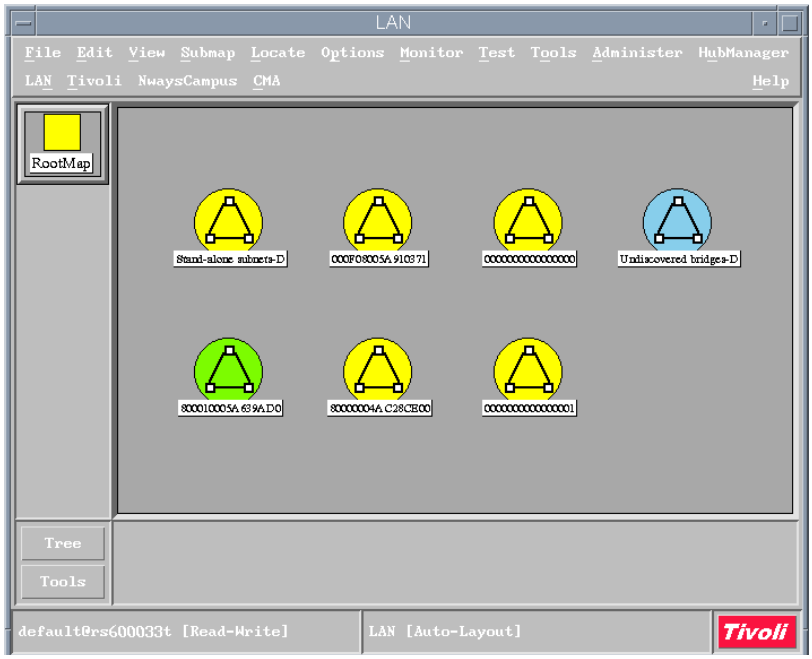


Figure 38. LAN Submap via LNM

Click on the LAN icon **80000004AC28CE00** to see the bridge configuration shown in Figure 39 on page 79.

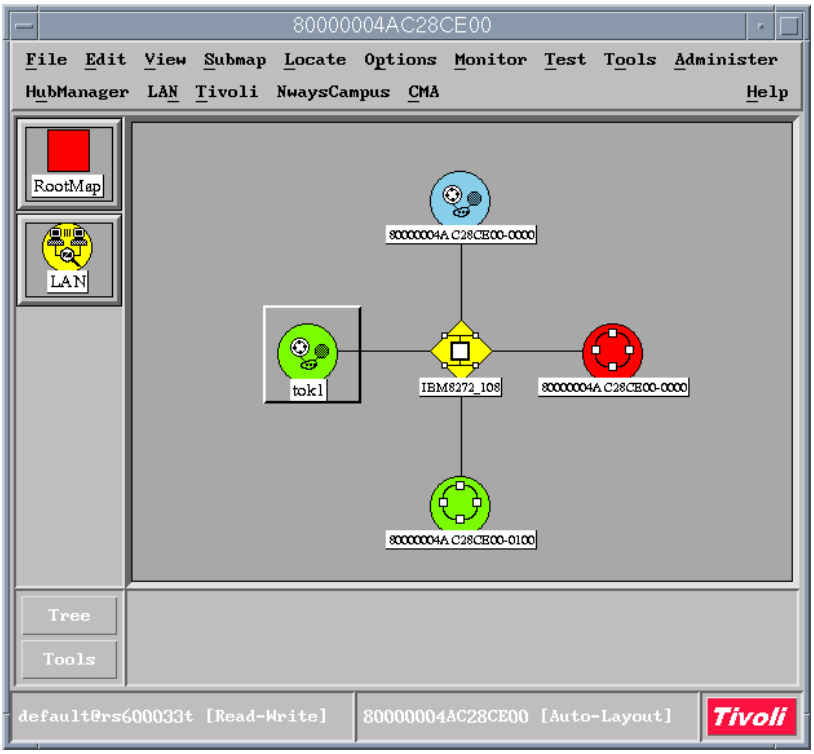


Figure 39. Bridge Configuration

Here we can see the 8272 performing the bridging role between three legacy LANs and an Emulated LAN called tok1. If we double-click on the 8272 icon we can see the specific port configuration status for the 8272 (see Figure 40).

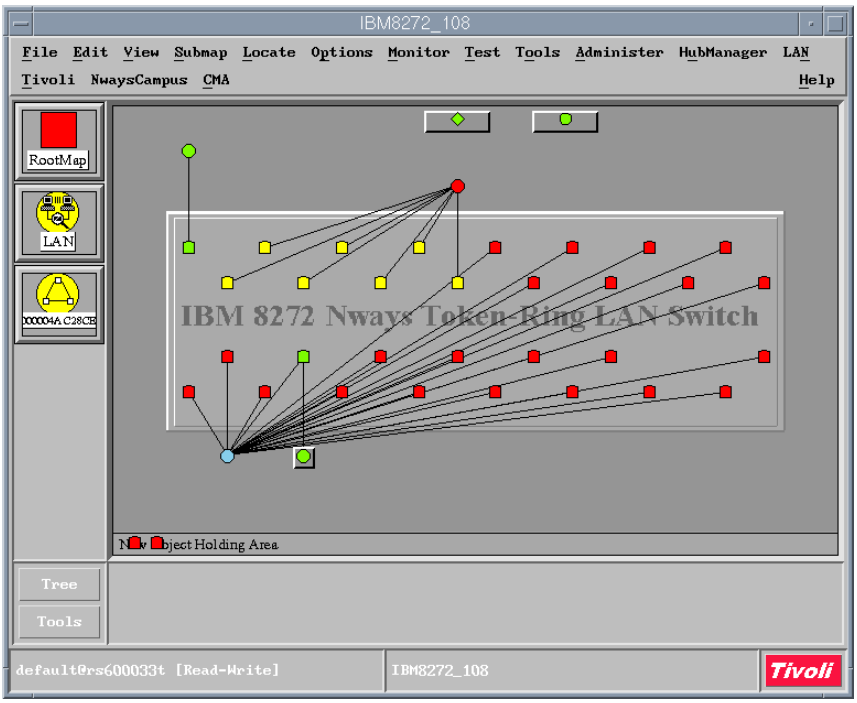


Figure 40. IBM 8272 Switch/Bridge Status

This view displays the bridging configuration by MAC addresses, based on all the ports on the 8272. This information is received from the bridge MIB 1493, which is one of the MIBs that the 8272 supports.

5.1.5 Hub Topology Submap

Hub Manager monitors the status of the hubs, and displays that status by showing the appropriate color for the icons on the IBM Hubs Topology submap.

This color status, by default, is determined by the composite status of the hub's components. These include ports, modules, trunks, fans and temperature. All these elements are treated equally.

This may not reflect the relative importance of the resources of a particular network. Often a hub will host a combination of critical and non-critical modules. For example, critical modules could include a module to which server connections and backbone connections are made, and failure of any of these connections may be critical to the operations of the network, therefore a compound status of red may be preferred. Conversely, user modules or ports to which users are connected may not be of high concern.

A resource can be assigned a monitoring value of Critical, Normal or None. By default, all resources in the system are assigned a monitoring value of Normal, meaning that all 8250 or 8260 Hub resources (that is, modules, ports, fans) will be assigned a monitoring value of Normal. The compound status, or propagated status of the hub with these values set will be based on the compound status

defaults that are set by NetView. The NetView documentation should be used to set status propagation thresholds on devices that differ from the installed defaults.

The Hub submap represents a collection of the hub devices such as the 8250, 8260 and 8265s. The devices contained in this submap are managed by the Hub Manager, PSMs and JMAs.

Note

It may be useful to edit this view and hide all objects other than 8250/60/65 as all of the other devices appear in the collection views of the Nways Management map. If there are a lot of IBM devices in the network, the Hub Topology becomes unusable.

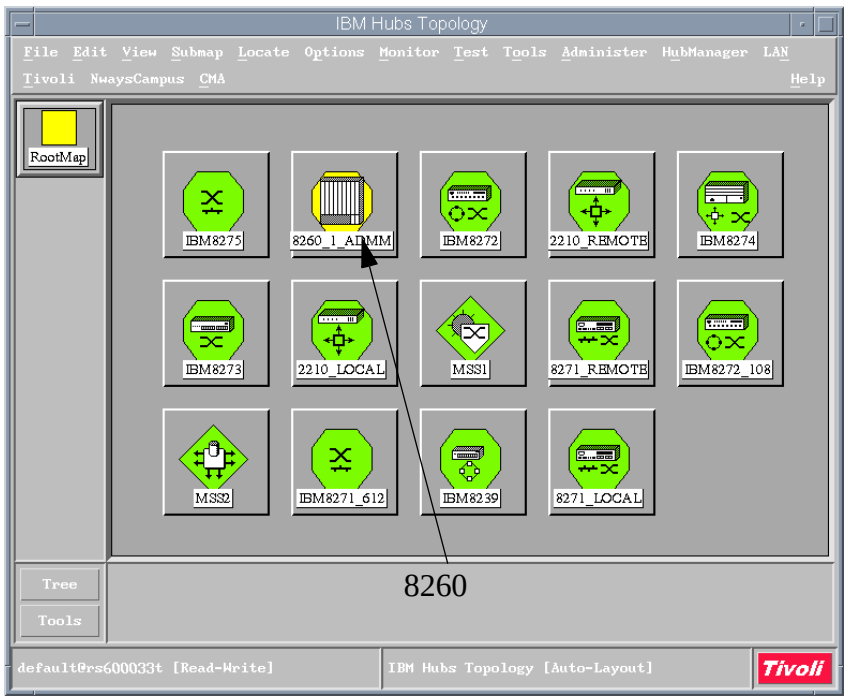


Figure 41. IBM Hubs Topology Submap

Double-clicking on any of the icons will produce a device-specific graphical view of that device. An example of the IBM 8260 is shown in Figure 42 on page 82.

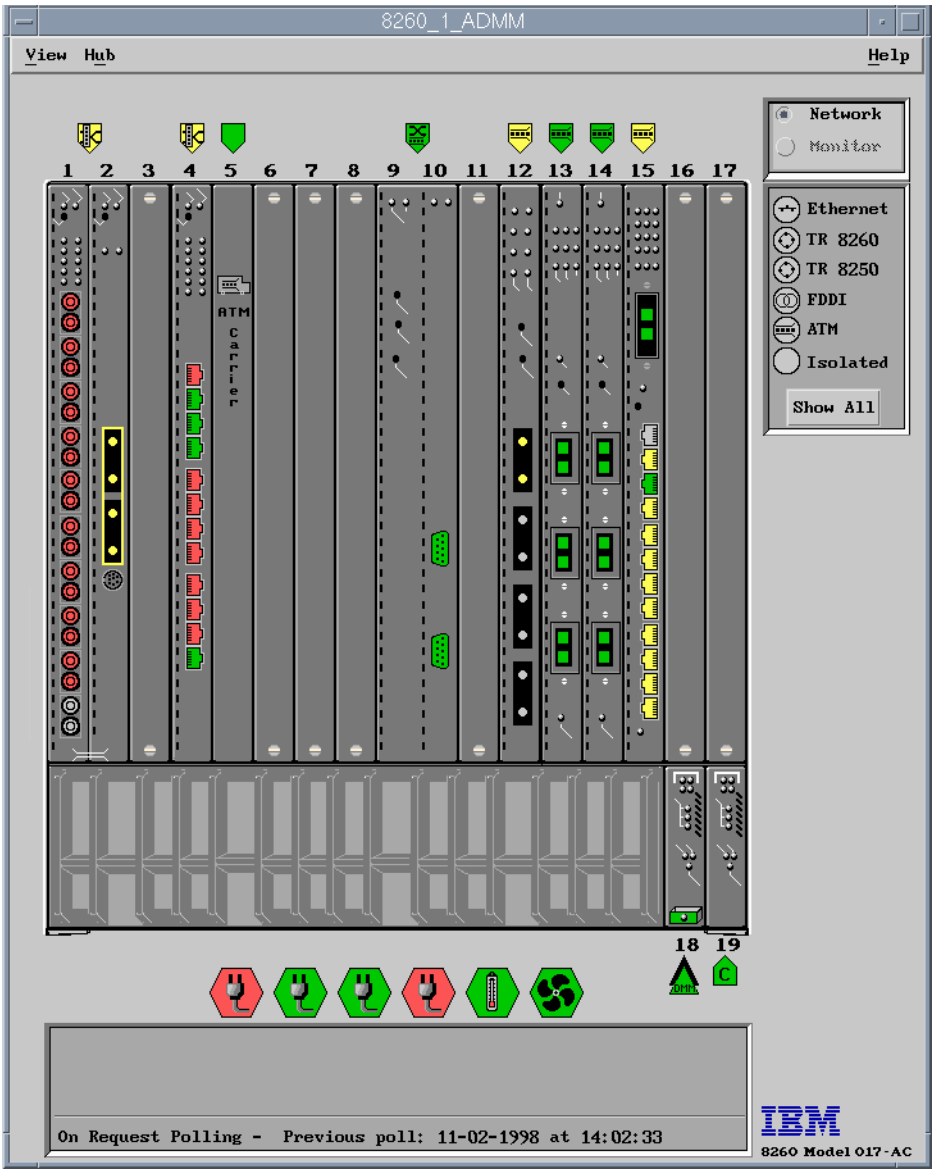


Figure 42. Hub Manager (IHMP) View of 8260 Hub 8260_1_ADMM

Here we can see the status of the logical ports and networks from the hub as well as the status of the modules, physical ports and other hardware components. Status is shown using the following color codes:

Green	Normal status
Yellow	Marginal status
Red	Critical Status
Blue	Unknown
Wheat	Unmanaged
Grey	Disabled

5.1.6 Device Management Submap

The Nways device submap contains a collection for each type of device except for the 8250, 8260 and 8265 Hubs. Each icon represents a collection of a specific model type of each device. This configuration can be refreshed at any time by

selecting **Tools-> Application Transporter -> Refresh Device Management submap** from the pull-down menus. The collection of the devices in our scenario is shown in Figure 43 on page 83.

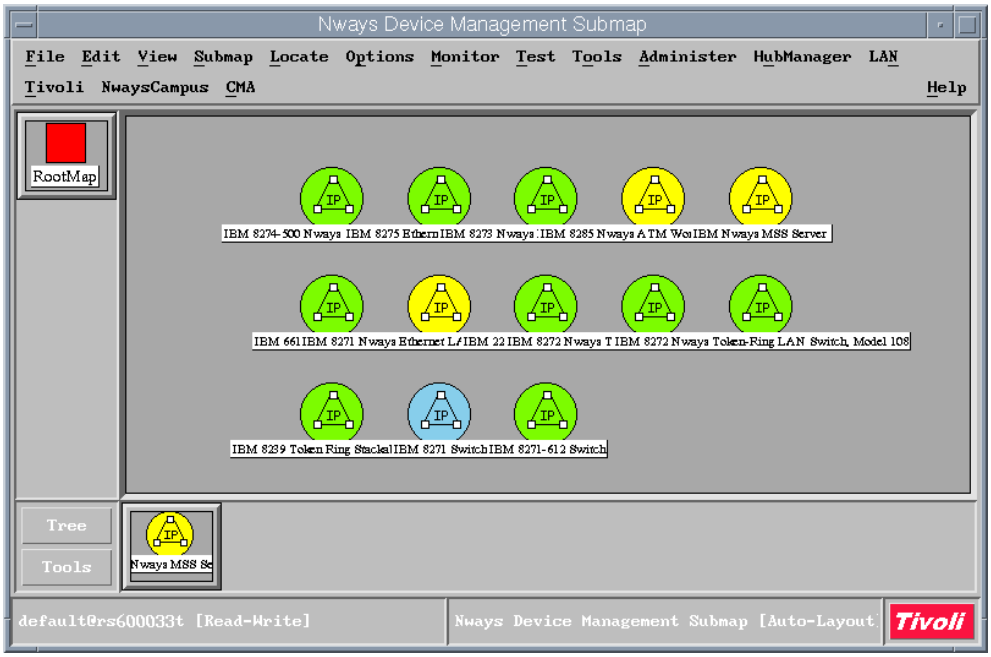


Figure 43. Nways Device Management Submap

Double-clicking on any icon in this submap will show a collection of all devices of that particular type. Figure 44 on page 84 shows an example for the MSS collection submap.

.

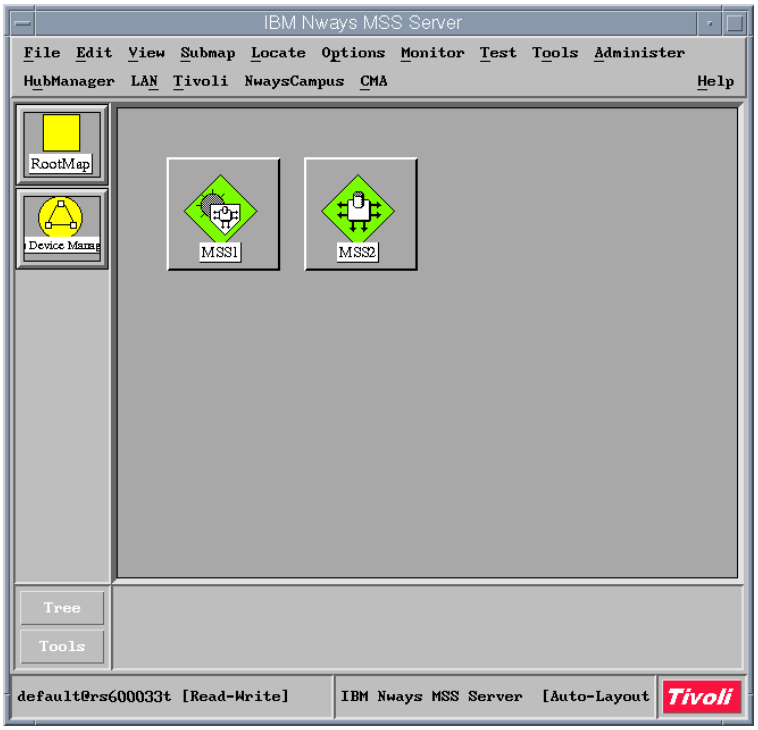


Figure 44. Nways Device Management for the MSS

We have discovered two 8210/MSS devices. By double-clicking on any of the device icons in the submap the device-specific view will be launched. For instance, the 8210 icon initiated the JMA as shown in Figure 45 on page 85.

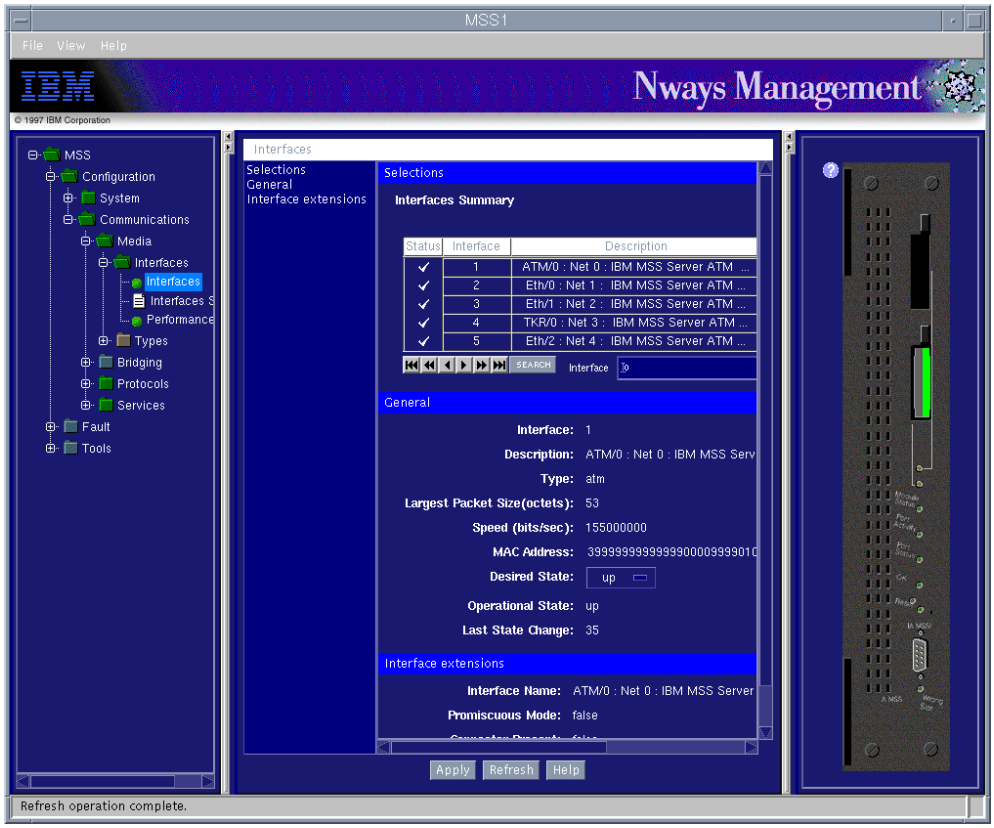


Figure 45. 8210/MSS JMA View

The JMA shows the status of the physical ports on the device graphic at the right-hand side of the window. The status can also be displayed by picking the appropriate button on the device management subtree in the left-hand window.

5.1.7 PSM Status

For the PSMs click on the 8271 accessible from the screen shown in Figure 43 on page 83 and clicking on **8271_REMOTE**.

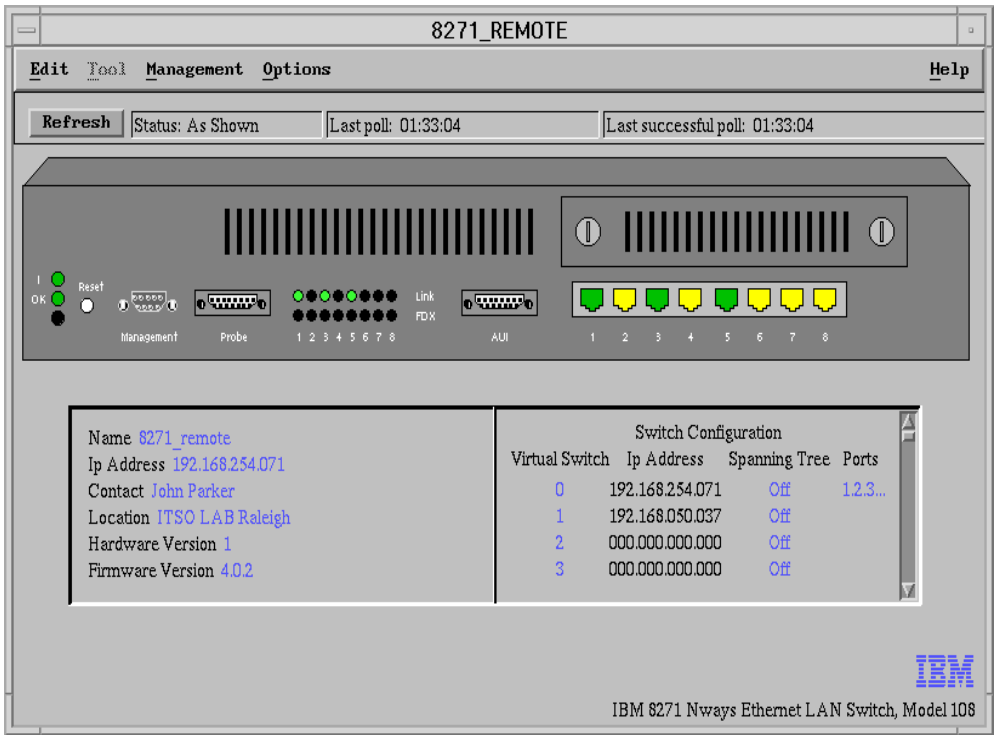


Figure 46. 8271 PSM

The right-hand side of the hub view has port icons with a color-coded status that shows the operational status of the 8271 ports, and towards the left side of the view you will find the LED status for each port. The status color interpreted for the 8271 are the following:

Green Ports is enabled and connected.
Yellow Port is enabled and not connected.
Grey Port is administratively disabled.
Red Port is operationally disabled.
Blue Status is unknown.

Our 8271 has ports 1, 3 and 5, enabled and connected. The remaining ports are enabled, but not connected.

There are hot-spots within the graphical view usually on all interfaces. Single-clicking using the left mouse button on a port, interface or device gives information on that specific item.

5.1.8 ATM Submap

Nways Campus Manager ATM provides management for ATM devices that are part of the network. The main components of Nways Campus Manager ATM are:

- ATM Manager (ATM Campus submap)
- LAN Emulation Manager (VLANS View)
- FaultBuster
- Locate/Search Function

To open Campus Manager ATM click on the **ATM Campus** icon to display the ATM topology. The ATM Campus submap shows a hierarchical view of the ATM

network topology. The ATM Campus submap contains ATM clusters, PNNI peer groups and a default group that is for devices that are not yet associated to any ATM device.

Figure 47 on page 87 displays the ATM top-level view of our scenario network.

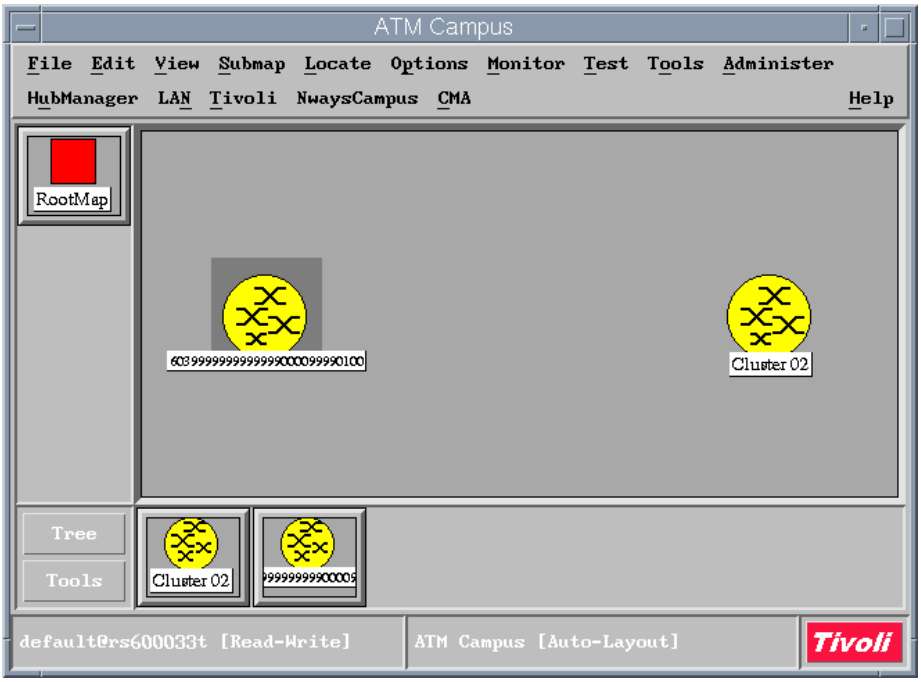


Figure 47. ATM Campus Top-Level View

The ATM cluster Cluster 02 contains all the ATM devices that have the same 12-byte network prefix, where the 12th byte is the cluster number. These are devices that do not support PNNI or are not connected to devices that do. A peer group contains all ATM devices that share the same peer group identifier. The icon is displayed with that peer group identifier as the label. The concept of the peer group applies to devices that are configured for PNNI.

Figure 48 on page 88 shows the ATM device submap for the ATM PNNI peer group we set up in our network scenario. The label on top of the panel shows the PNNI peer group identifiers that are configured in the ATM switches.

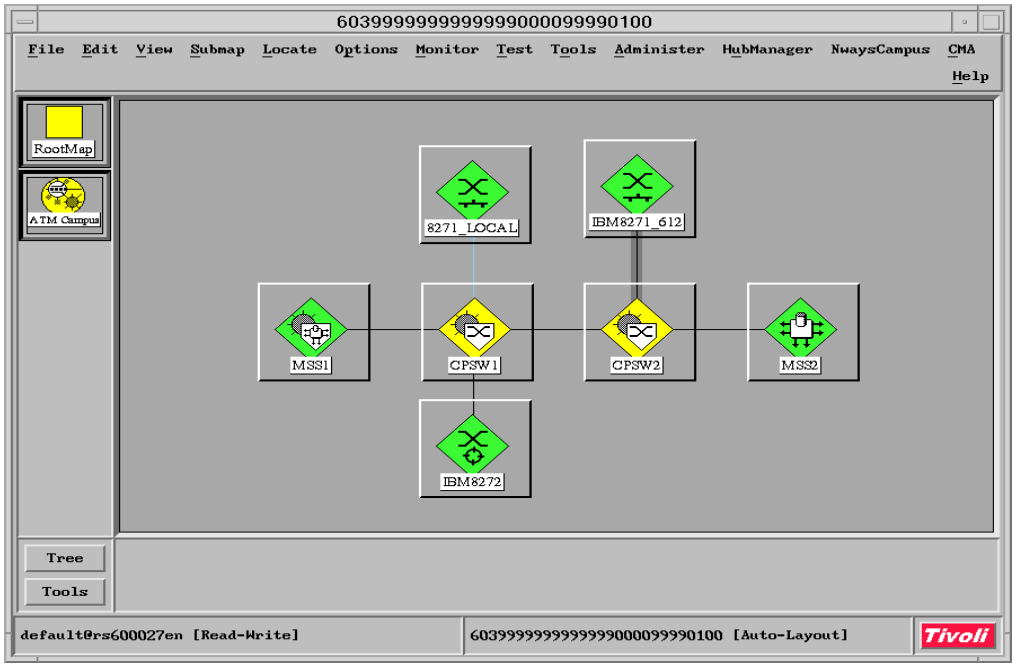


Figure 48. Device Submap: ATM Campus PNNI Group View

Here the 8260 ATM switches labelled CPSW1 and CPSW2 form the ATM backbone. Other ATM devices including ATM-to-Ethernet edge devices connected to one or both of these backbone switches shown by the connections on the map. The ATM edge devices are connected using UNI Version 3.x or 4.0, but show up in the PNNI group view as the backbone switches to which they are connected have PNNI enabled.

Note: In a large ATM network with a high number of ATM-attached devices, you may want to delete the edge devices or workstations from the ATM device submap, so as to have a clear view of the core backbone devices only.

The IBM 8273 and 8274 are not seen in this submap, as they do not currently support the standard ATM MIBs.

By double-clicking on any of the devices in the device submap view an ATM device level view will appear, as shown in Figure 49 on page 89. The ATM device level view shows the physical and logical ATM ports of the device.

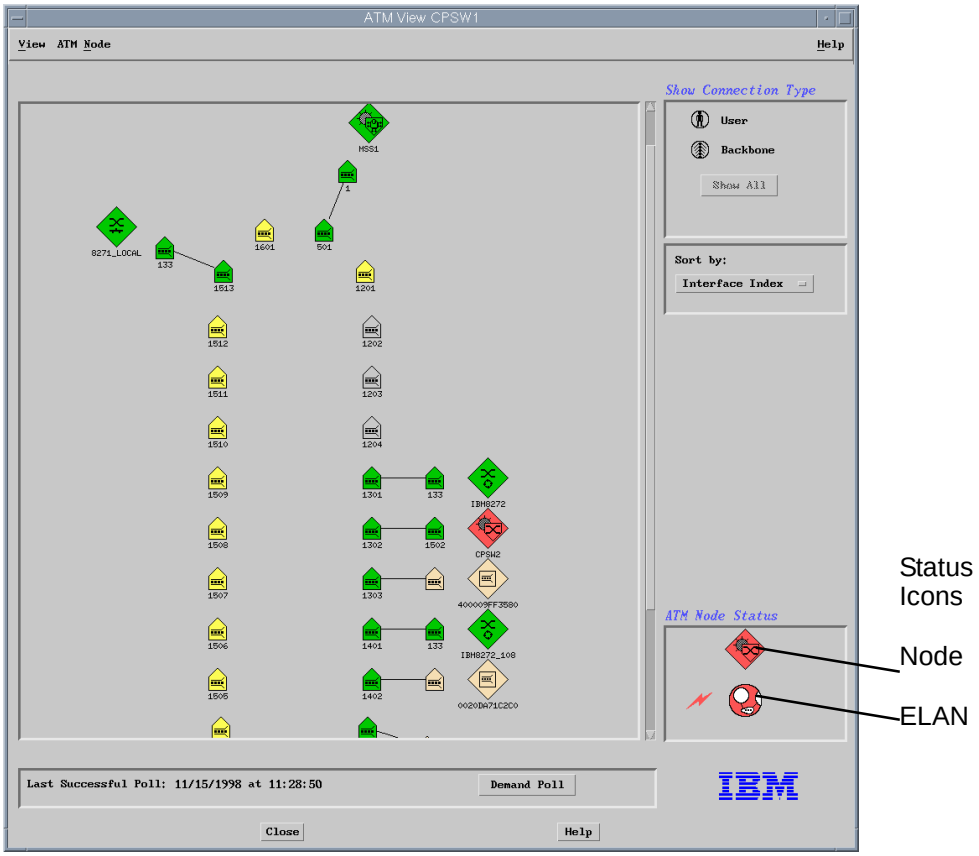


Figure 49. ATM Device View

The view above also shows the status of the devices that are connected to the ATM ports on this device. The two icons at the bottom right of the screen indicate the overall status of the ATM node and the VLANs/ELAN members that it supports. Double-clicking on the **Node** icon will open an ATM node configuration panel. Doing the same to the VLAN icon will open the ELAN Configuration panel, (see Figure 50 on page 90).

Figure 50. LAN Emulation Configuration View

Status for the ELAN members configured on the devices can be seen in this panel and configurations can be checked and modified.

5.1.9 ELAN Status Information

The VLANs icon on the NetView root submap provides ELAN management. The icon is executable and starts the LAN Emulation Manager. The domain here represents the ELAN elements that fall under a LECS instance.

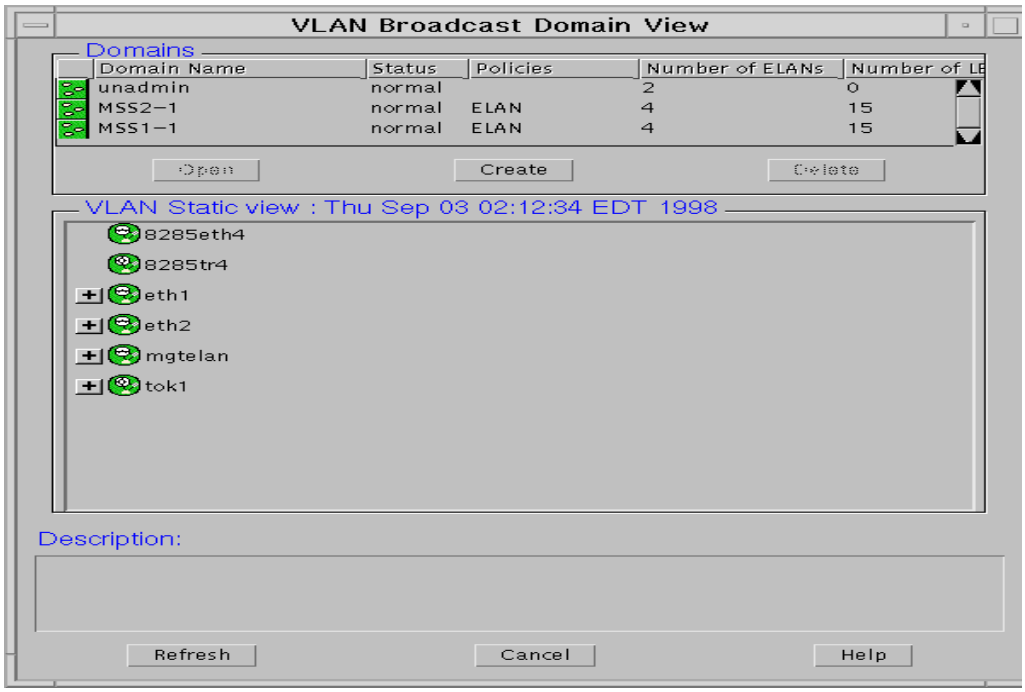


Figure 51. ATM ELAN (LECS) Domain View

As shown in Figure 51 we have three domains in our network scenario shown in the top third of the panel. The unadmin domain is a default domain created automatically and contains ELANs that are not associated with any of the other domains.

MSS1-1 and MSS2-1 are the domains reflecting our configuration, where we have two MSSs, both serving the function of the LECS, and providing redundancy in case of failure. This view is only provided for ATM Forum-compliant ELAN domains.

The area entitled VLAN static view shows the ELANs defined in the ATM network.

The + sign on an ELAN in the VLAN static view indicates that there are LECs that have registered with this ELAN, which is a tree view and that can be expanded by clicking on the + sign.

Figure 52 on page 92 shows the expanded view for the ELAN eth1, showing all the LECs that are part of this ELAN.

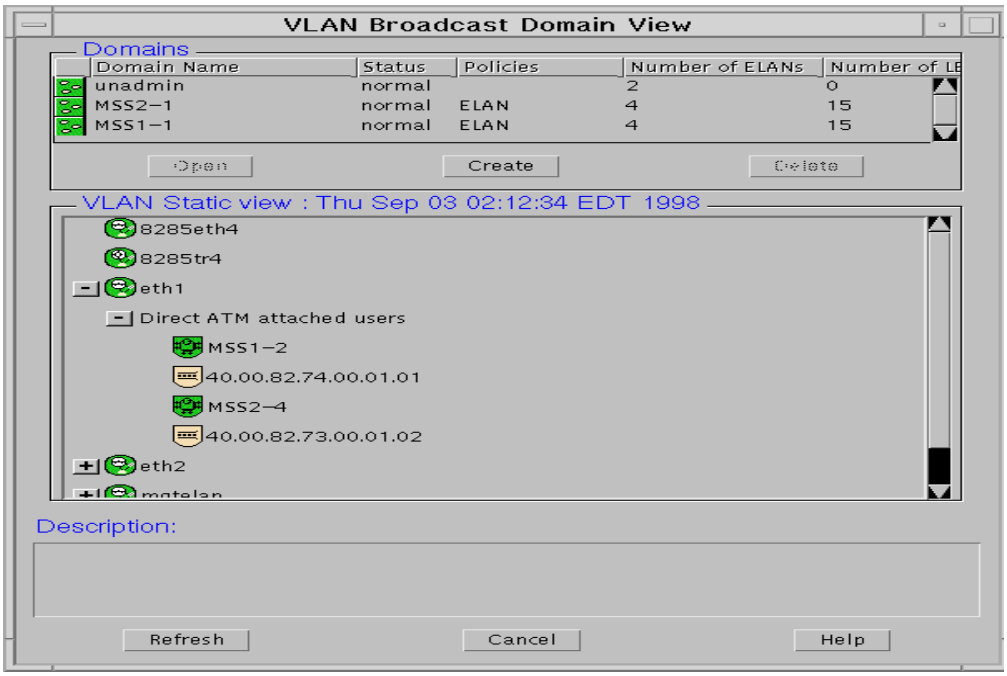


Figure 52. ATM LECs in a Specific ELAN

By selecting the Domain **MSS2-1** and selecting the **Open** button the Exploded Domain view can be accessed. This is a similar view to the main VLAN view, but only shows the information for the selected domain. This window shows the ELANs that are contained in this domain, but only as icons and not as a list of items as in the VLAN Static View panel. The view also shows the LECS that administers the domain and the ELAN policies used to control access to the domain. Double-clicking one of the ELAN icons will open the Exploded ELAN view as shown in Figure 53 on page 93.

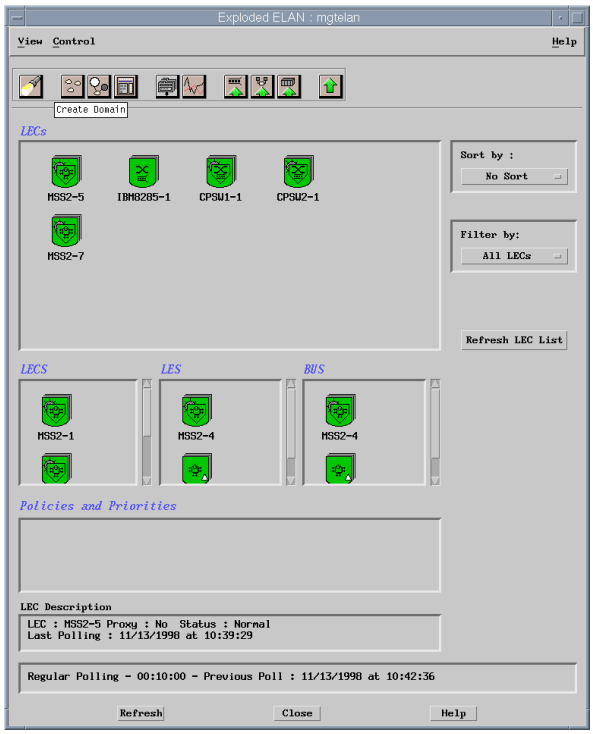


Figure 53. Exploded ELAN View from Exploded Domain View

Here we can see the status of the LECS, LES/BUS and LECs for a single ELAN.

5.1.10 Locate Function

Using the locate function can also show status. Start the locate by selecting the item **Nways Campus->Locate** from the pull-down menu. Enter the IP address of `192.168.*.*` . Here we can see the status of all devices in this subnet, including ATM devices (see Figure 54 on page 94).

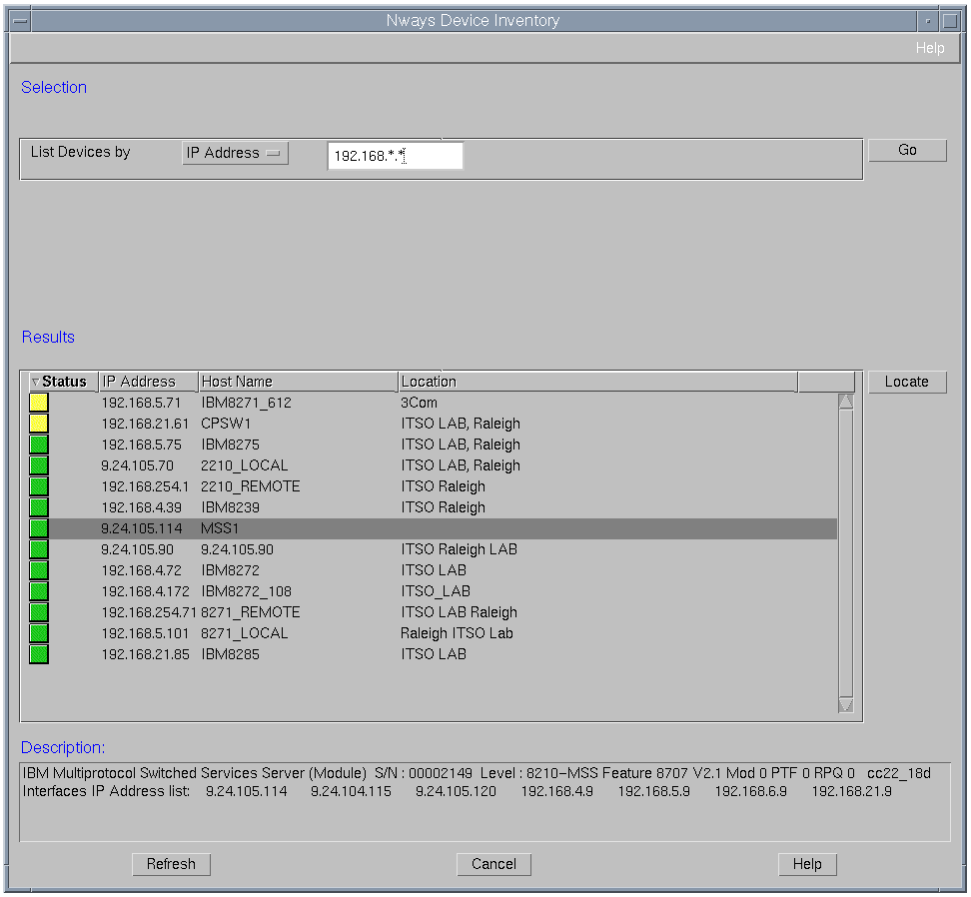


Figure 54. Locate Output Window

Status and configuration information can be seen for the ATM environment.

5.2 Using Collections

This example shows how we created a simple collection that shows our ATM devices in one submap. To start the collection editor select **Tools->Collection Editor** from the NetView pull-down menus.

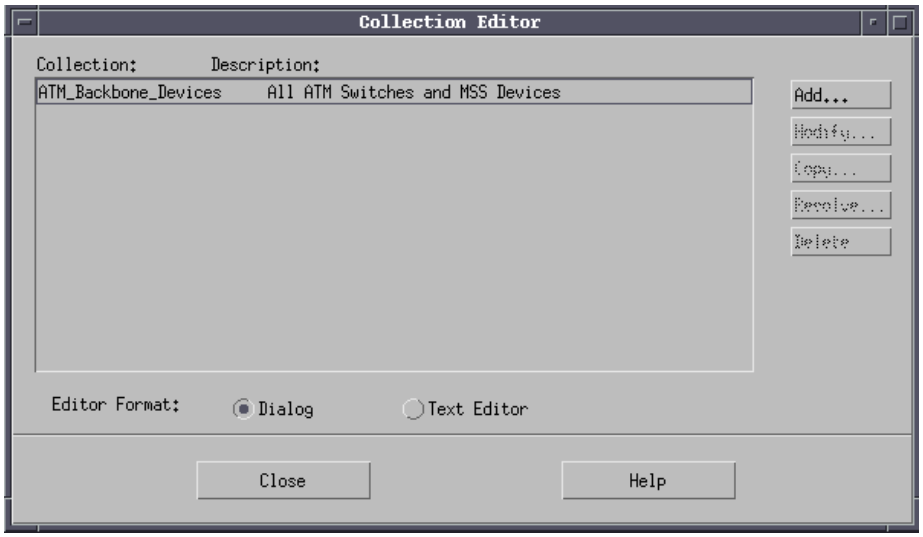


Figure 55. Collection Screen

The information used in a collection is based on the NetView database. Each device has a set of defined parameters that are set when a device is discovered. These can be viewed by selecting an object on the map and selecting **Edit->Modify/Describe->Object Attributes.** Figure 56 on page 96 shows the attributes for the CPSW.

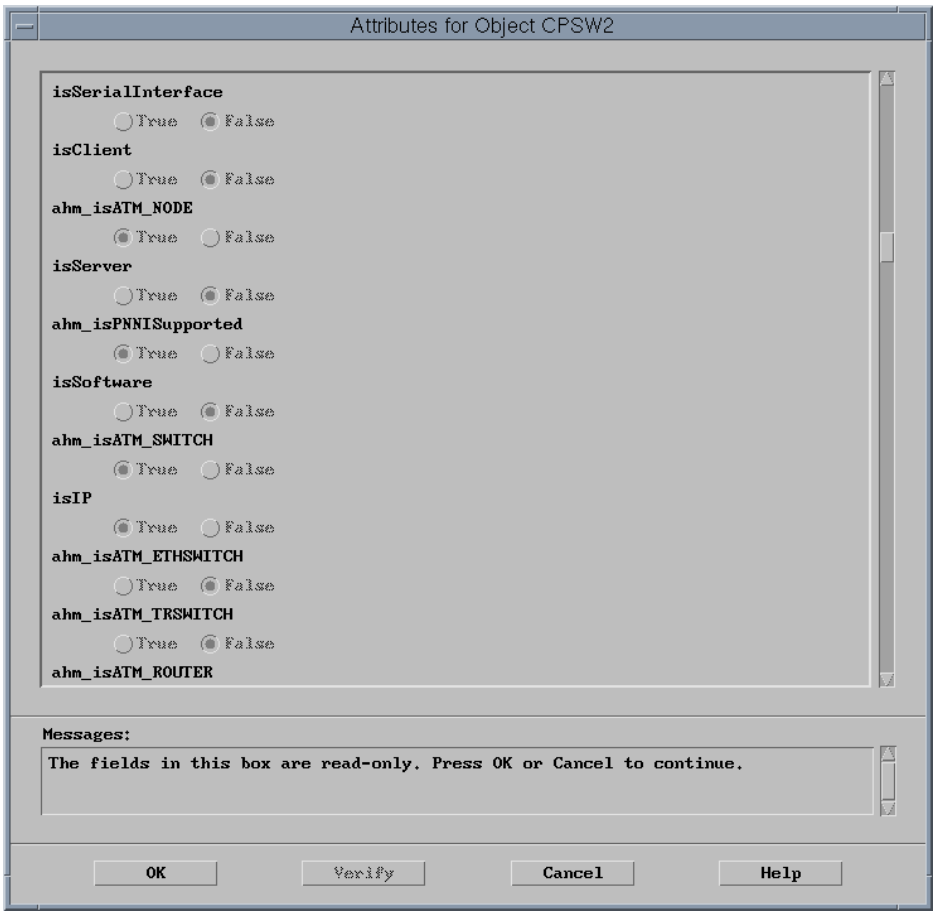


Figure 56. Device Attributes for CPSW2

We defined all the ATM nodes and ATM switches so that they will appear in one submap named ATM_Backbone_Devices. To do this, we selected the devices based on the collection rule shown below:

```
'ahm_isATM_SWITCH' = True Or 'ahm_isATM_MSS' = True
```

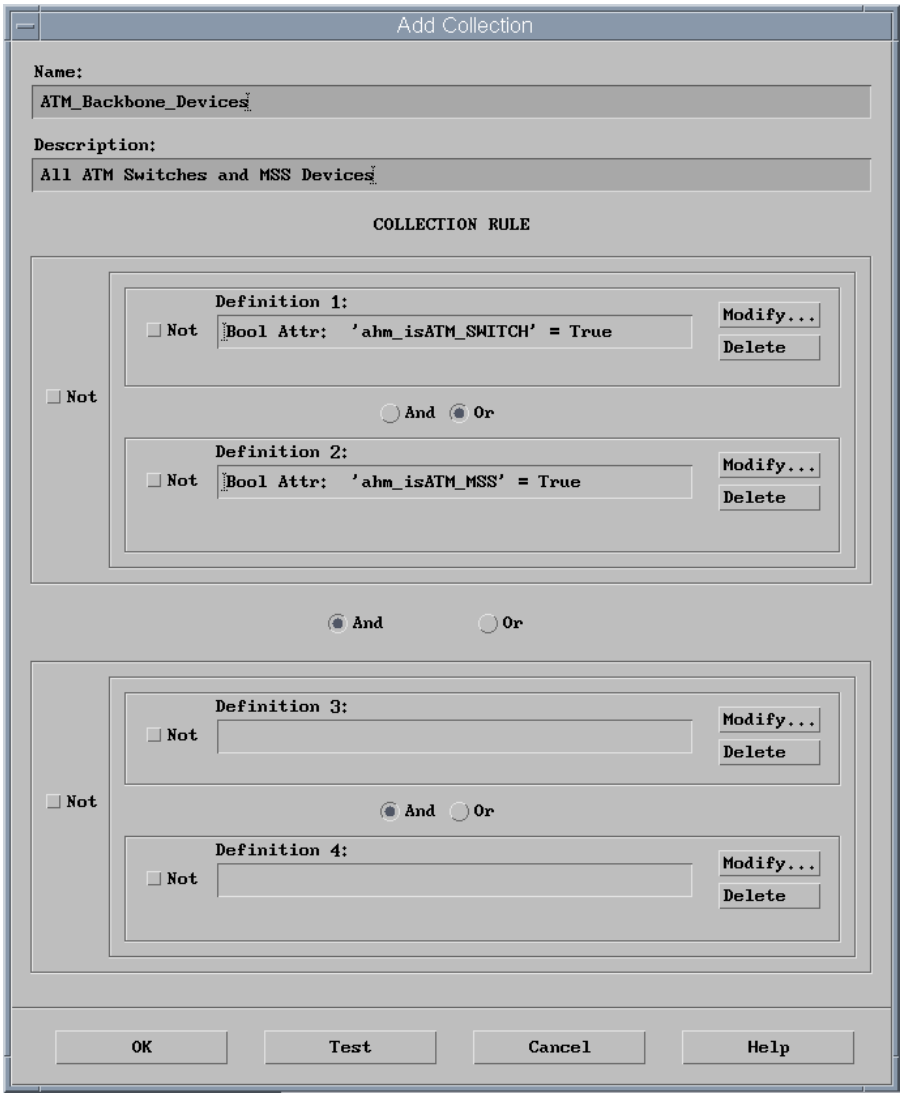


Figure 57. Add Collection Window Showing Collection Rule

Clicking on **OK** will create the collection rule and apply it to the NetView database, selecting any objects that match the rule and putting them into a collection submap called ATM_Backbone-Devices. The Collection window is located from the root submap by selecting the **Collections** submap icon, followed by the **ATM_Backbone_Devices** icon in the Collections submap.

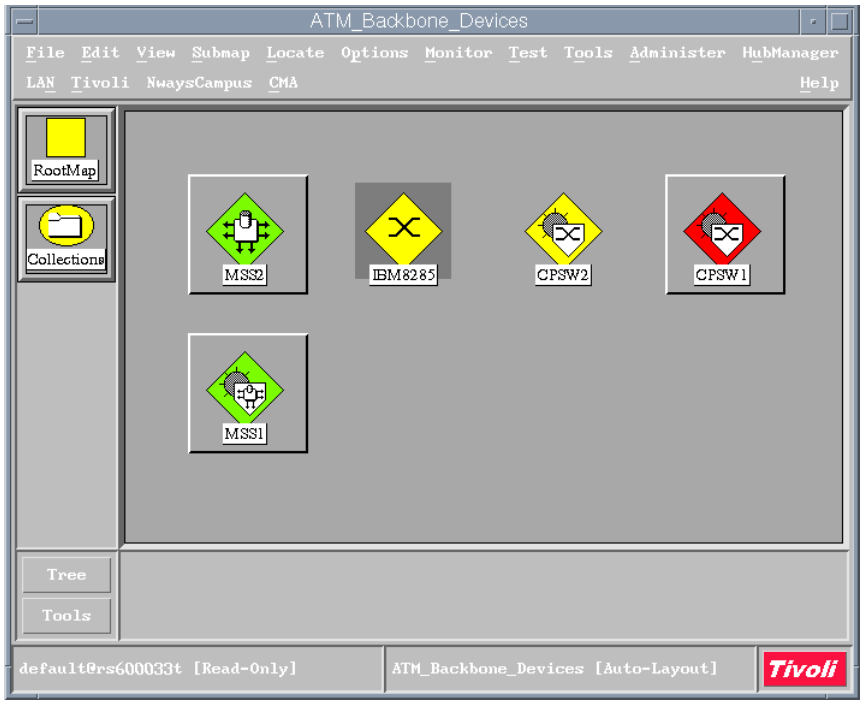


Figure 58. Collection View for ATM_Backbone_Devices

Figure 58 shows that the icons in this view are linked to objects in the NetView database, their status color will be updated by NetView.

5.3 Configuration

This section refers to the configuration and tuning required for the Nways applications. Here we show the configuration that we performed on some of the devices in our environment. Below is a list of the applications used:

- Device Managers (JMA/PSM)
- LNM
- 8210 Configuration Program
- 8260 Hub Manager
- ATM Manager
- RouteVision

IBM has a wide range of features and functions within its network management product suite. In this book, we focus on the detailed management of the devices that are part of the lab environment setup. We show one or two examples for each major category (that is, Hub Manager, PSMs, JMA and JPM).

You will notice that for some devices there are several management components or views available for managing different features and functions of the same device. The views are called protocol views. An example is an 8260 Hub with both ATM and legacy modules, (that is, Ethernet, token-ring and FDDI), where the management options available are:

- **Hub Manager**: Provides graphical device management and configuration support for legacy modules in the chassis hub.

- **ATM Campus Manager**: Provides an ATM management view and configuration support for ATM modules and topology.
- **Java Management Applications**: Modules within an 8260 such as the MSS or switching modules can be managed and configured by using JMAs. Clicking on those modules will bring up a JMA view of the module.
- I**P Internet Submap:** For looking at a device from an IP subnet view, that is from an IP topology perspective.
- **LAN Network Manage**r: Displays LAN topology and management of LAN resources at an adapter level and provides management for bridges.

With several options available on some devices, the component or view that you execute depends on from what perspective you want manage it (that is, LAN, ATM and RMON). In the following sections we cover the management options from a product component perspective.

5.3.1 Hub Manager

The Hub Manager provides management for the IBM 8250, 8260 and 8265 hubs. On the NetView Root submap, an icon can be found for IBM Hubs Topology. This submap represents a collection of 8250s, 8260s, 8265s, and any PSM or JMA's managed devices in your NetView topology database that conform to the selection criteria; namely, they have the object attribute NVOT isHub8250 set.

In this section, we show an example of managing an 8260 G-17 Multiprotocol Hub, which hosts the following:

- Ethernet switching modules
- ATM control point switch module
- ATM media modules
- MSS module
- DMM module with controller

Here the DMM is the master management module, and provides chassis management as well as management for legacy modules. The management for ATM modules is provided by the CPSW, which maintains a subset of the DMM MIB and is called the ATM management module (AMM).

Double-clicking on the icon for the 8260 hub in the IBM Hubs Topology submap explodes a hub view as shown in Figure 59 on page 100.

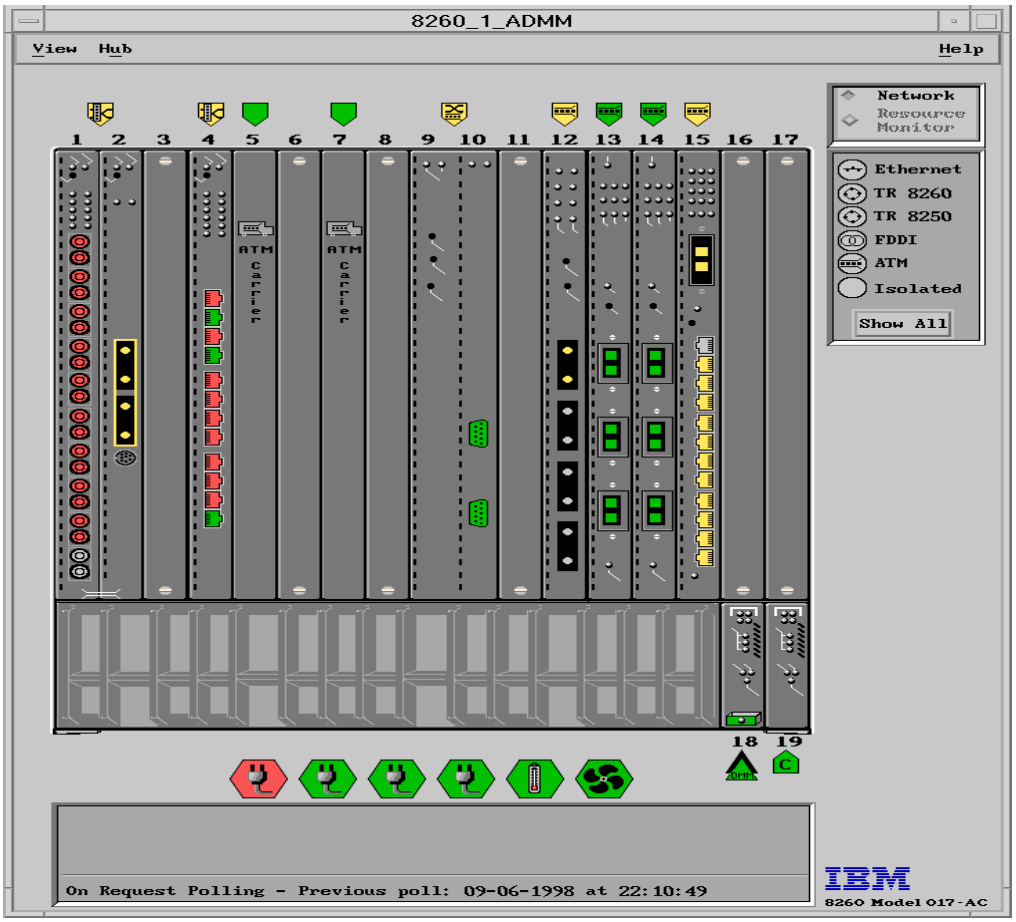


Figure 59. IBM 8260-G17 Graphical View

The Hub view is almost an exact replica of the physical hub except that the color codes are not the same. The status depends on the last poll. You may have noticed that ATM modules in slots 5 and 7 do not have a picture, and only show as an ATM Carrier.

The reasons are usually that the current DMM microcode does not recognize or support it, or that the Nways product does not recognize it. In some cases, certain modules themselves have an SNMP agent built in. In our case slots 5 and 7 contained MSS modules, which we had to enable and configure to allow SNMP management of them. The MSS base management is provided by a JMA.

At the top of each module, there is an icon representing a specific type of module media, for instance Ethernet, ATM or token-ring.

On the bottom of the graphic view there is a single icon representation for the fans and one for the temperature of the hub. There is a power supply icon for each power supply installed in the hub. All icon graphics resemble the actual item itself, or are self-explanatory.

In our scenario we had four supplies. For the purpose of showing different color codes we switched off the leftmost power supply, and its icon showed a red color in the graphical view, indicating a critical status.

Double-clicking on the icon on top of a module will show a module level view. If you single-click on the same icon, the description of the module, IP address (if it is configured), and the polling parameters for the hub are shown in the information area at the bottom of the panel.

By double-clicking on the icons for ports, fans and power supplies, new panels that show current status will appear. From here you can perform configuration.

On the top right-hand side is the network area the icons represent different LAN types as follows:

- Ethernet
- TR 8260
- TR 8250
- ATM
- Isolated networks

From here you can select a particular icon, thus only showing modules in the 8260 that are of that particular network type.

Figure 60 on page 101 shows an example of ATM native modules and appears by clicking on the **ATM** icon, and then selecting **Native**. This is useful when you need to manage modules that belong to a certain type of LAN architecture.

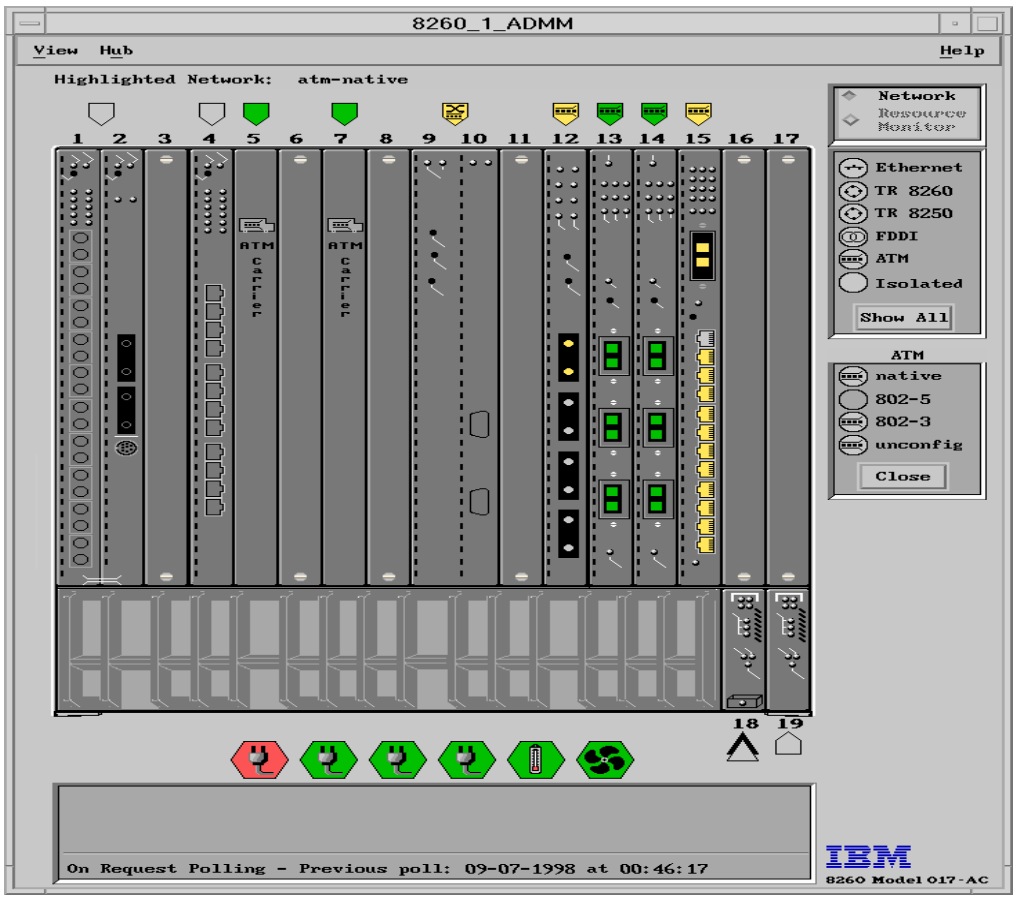


Figure 60. Example: Highlighting ATM Native Modules in an 8260

Selecting a port on the ATM module with the right mouse button brings up a context menu. From here, the port configuration can be opened, as well as the ATM configuration and profile. The profile lists the interfaces general parameters, as seen in the following screen.

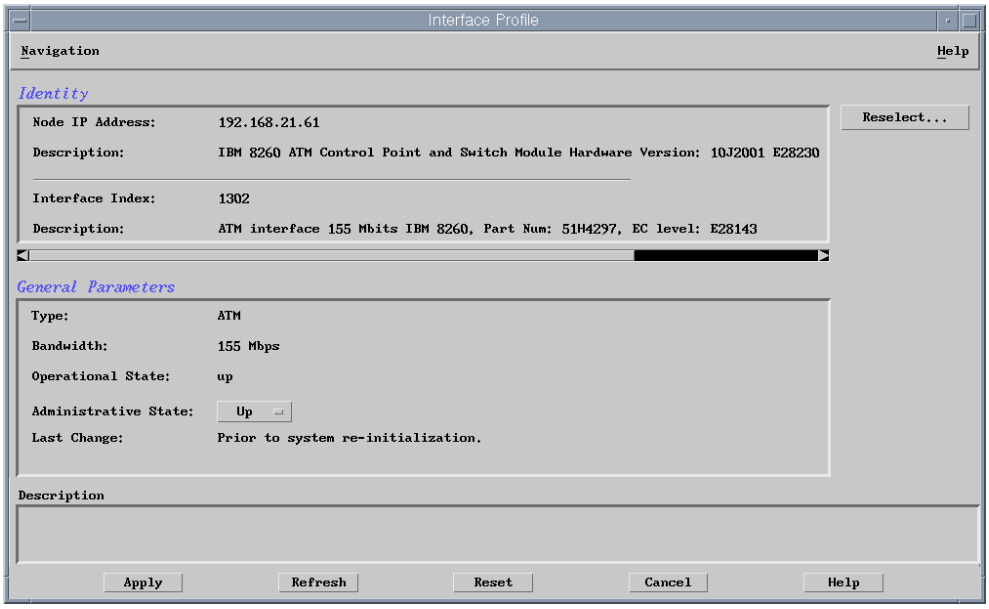


Figure 61. ATM Interface Profile for Slot 13 Port 2, Interface 1302

General hub information is also available by selecting the **Hub** pull-down menu. For instance, selecting **Hub->Show->Show Modules** will list all of the installed modules and some basic information about them.

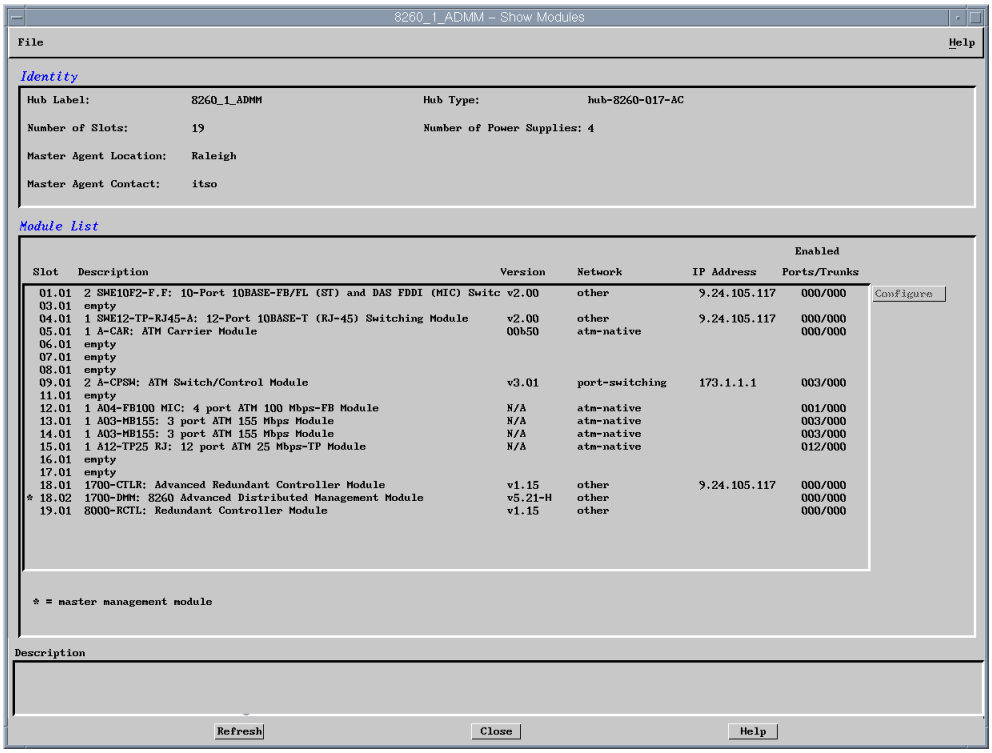


Figure 62. Hub Show Modules Output

5.3.2 Associating the Device Managers with the Devices

This section details how to associate the relevant executable application with the discovered devices. There are times when the applications do not perform this association automatically during the discovery process.

The Management Application Transporter, during the refresh cycle mentioned previously, attempts to automatically associate the device with the appropriate installed PSM or a JMA. If the Management Application Transporter (MAT) cannot find a match, a dialog box will be displayed asking if you want to use a default.

There are several situations that may cause the Nways device management applications from not correctly associating the appropriate application to a device icon and not marking it as an executable. One is a timing problem when Nways attempts to perform an SNMP GET request to retrieve a MIB variable.

The solution to the problem is different depending on whether it is PSM, JMA or hub manager.

If the device is managed with a PSM, you will need to make the icon executable using the Application Transporter pull-down menu option:

1. Add public as a read/write community name to the device configuration.
2. Associate the device with the PSM.
3. Open the subsystem.
4. From the PSM view, select **Edit-> Modify** from the menu bar and change the **General Parameters** screen to the correct community name

You may remove the public community from the device configuration.

If the device management application is either the Hub Manager or the Nways JMAs, the NetView icon must be made executable as follows:

1. Select the icon using the left mouse button.
2. With the right-most button select the **Edit-> Modify/Describe -> Symbol options.**
3. Change the behavior to **Execute.**

If the device is an 8250, 8260 or 8265, select the Application Action to be,

IBM Hub Manager: explodeHubView.

If the device is a 2210, 2216, 8210, 8273, 8274, 8229, 6611, one of the newer models of the 8271 (model numbers 524, 612, 624 or 712) or a generic JMA then set the application action to be,

IBM Nways Java Management: OpenJavaDeviceView.

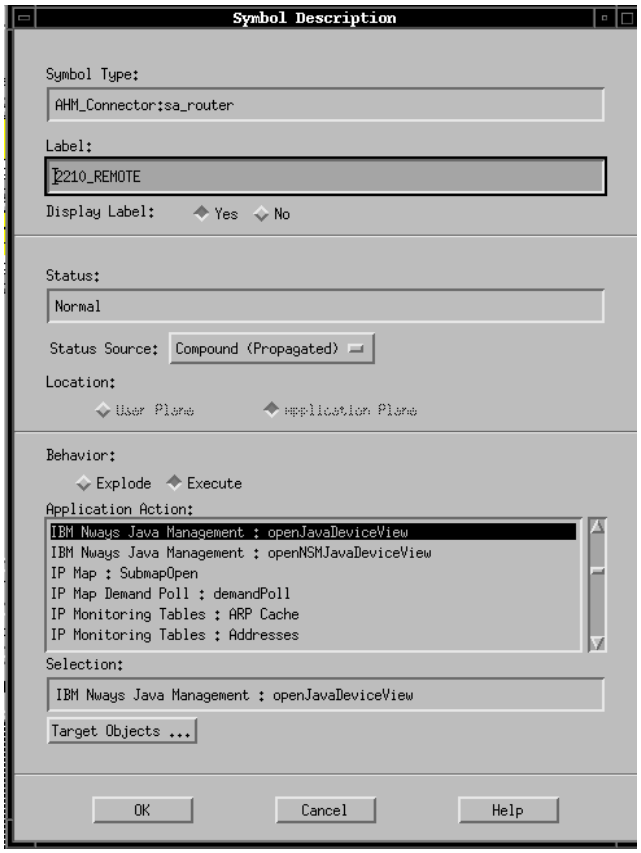


Figure 63. Symbol Description for 2210_REMOTE

Select and add the Target Object of the device you wish to make executable, and click **OK** to activate this.

5.3.3 PSM Operation

The PSM shown in Figure 64 on page 105 is accessed by the clicking on the 8271 Switch Model 108 icon in the management submap.

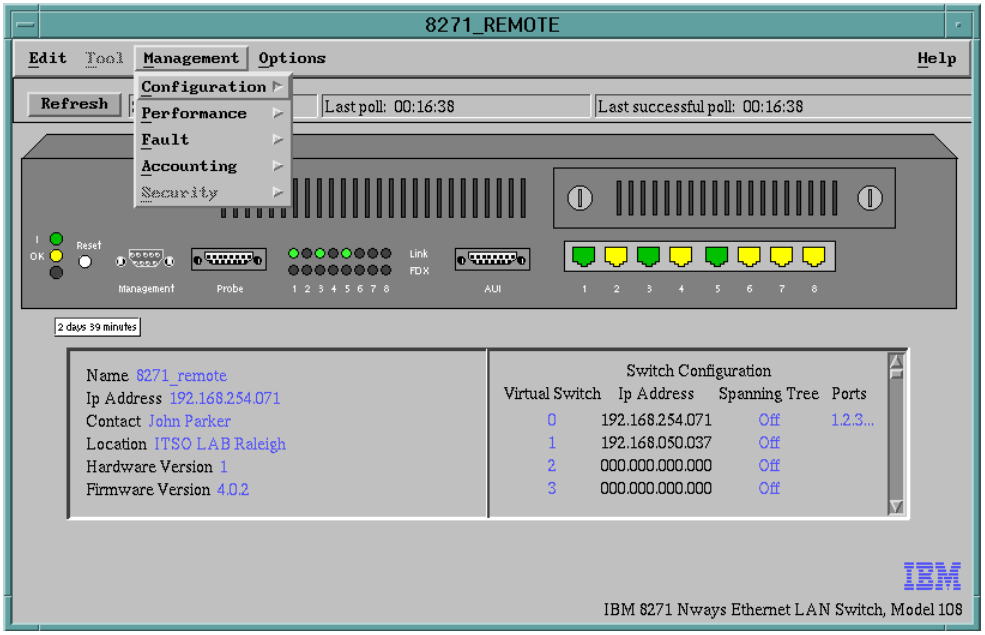


Figure 64. 8271_Remote Configuration

Similar to the Hub Manager view, the graphical view is a visual representation of the switch operational status, as per the last successful poll of the device.

Double-clicking on the hot-spots allows the configuration of the selected item. Double-clicking on the **Reset** button located on the left side of the switch view performs a reset of the switch.

5.3.3.1 IBM 8271-108 Polling Options

By default, the 8271-108 PSM polls the associated 8271 device only when the graphical view is exploded. The time of the last poll is indicated in the top of the PSM graphical view. Clicking on the **Refresh** button on the top of the PSM graphical view will activate a single manual poll of the device. If the requirement is to poll the device at a regular time interval, you can change the polling options from the menu bar by selecting **Options --> Polling Parameters**.

5.3.3.2 IBM 8271-108 PSM Management Capabilities

The overall general capabilities of the 8271-108 PSMs are as follows:

- Set basic configuration parameters such as IP address, device name and location.
- Regulate access based on MAC address by address filtering.
- Configure 8271 domains, or virtual switches, allowing segregation of ports within a switch to a domain.
- Set up Etherpipes, which allows parallel links between switches to be aggregated to allow higher bandwidth.
- Enable, disable and configure ports in 8271 switches.
- Configure spanning tree, to allow redundant paths and avoid loops.
- Set thresholds for warnings about fault conditions (trap management) and define the SNMP managers to receive the trap information.

- Retrieve performance and fault information.

The configuration management panels can be invoked in two different ways.

The total configuration options are available from the pull-down menu on the main PSM window by selecting **Management-->Configuration-->Configuration Options.** These options are shown in the diagram below.

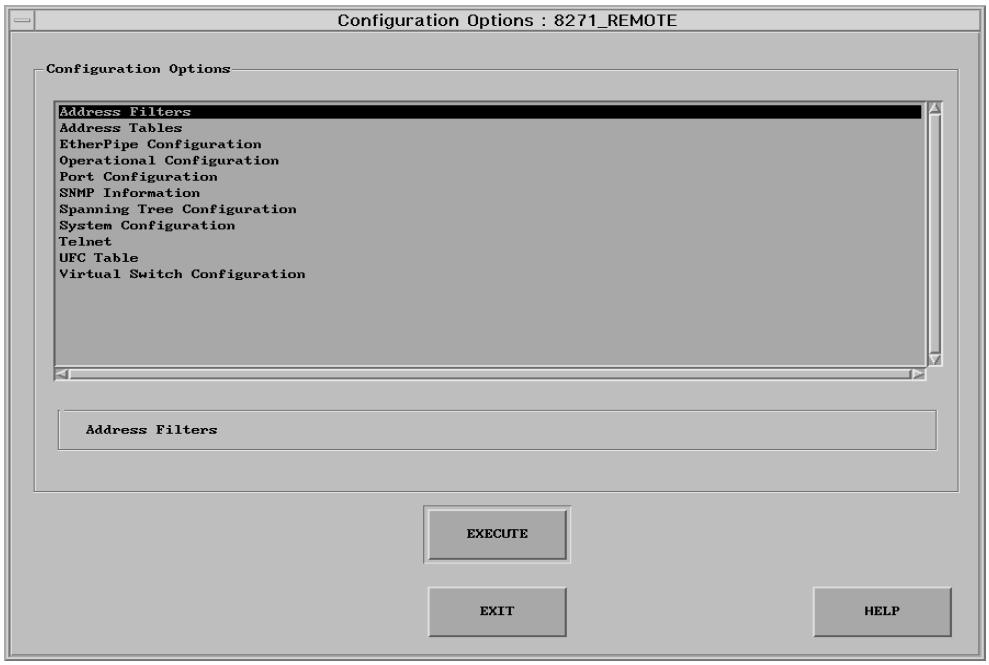


Figure 65. 8271-108 PSM Configuration Options Panel

Double-clicking on the hot-spots also brings up the configuration panel for that specific item as shown in Figure 66 on page 107. The Configuration options available through double-clicking a hot-spot are a specific subset of the configuration options that are available by using the pull-down menu. The port configuration options are shown in Figure 66 on page 107.

Figure 66. Configuration Options - Port Configuration

From here we can change the following parameters:

Address Filters - Allows blocking or passing data frames based on source or destination MAC addresses. These filter rules can be applied at a port level.

Address Tables - Displays the address table for a virtual switch and allows the setting of address aging time and address aging % level. The switch acts as a learning bridge, and builds up a dynamic address table based on MAC addresses that are seen in frames switched through the switch ports.

EtherPipe Configuration - Allows parallel links between switches to be aggregated to allow higher bandwidth.

Other options include:

- Operational Configuration
- SNMP Information
- Spanning tree configuration
- System Configuration
- Telnet
- UFC Configuration
- Virtual Switch Configuration

5.3.4 Java Management Applications

There may be two minor configurations required for the JMAs. The JPM is a sub-function of JMA, and can only be launched from a JMA view that is opened.

The JPM configuration is covered in Chapter 7, “Nways Java/Web Management Applications” on page 211.

.The JMA configuration that may be required is listed below:

- Make the JMA executable. If for any reason it is not correctly associated to the correct application. Associate devices with an application action or execution as discussed earlier.
- The JMA help information is stored as HTML Web pages. When help is selected from a JMA window a Web browser is launched automatically to display the appropriate HTML help pages. You will need to change the variable WebBrowser.path to the full path of the Netscape program directory. In our environment we set it to the following:

  ```
  WebBrowser.path=/usr/netscape/netscape
  ```

The example we show is for the 8239. Using the JMA, configuration options are located via the menu, or navigation tree, as shown in Figure 67 on page 108.

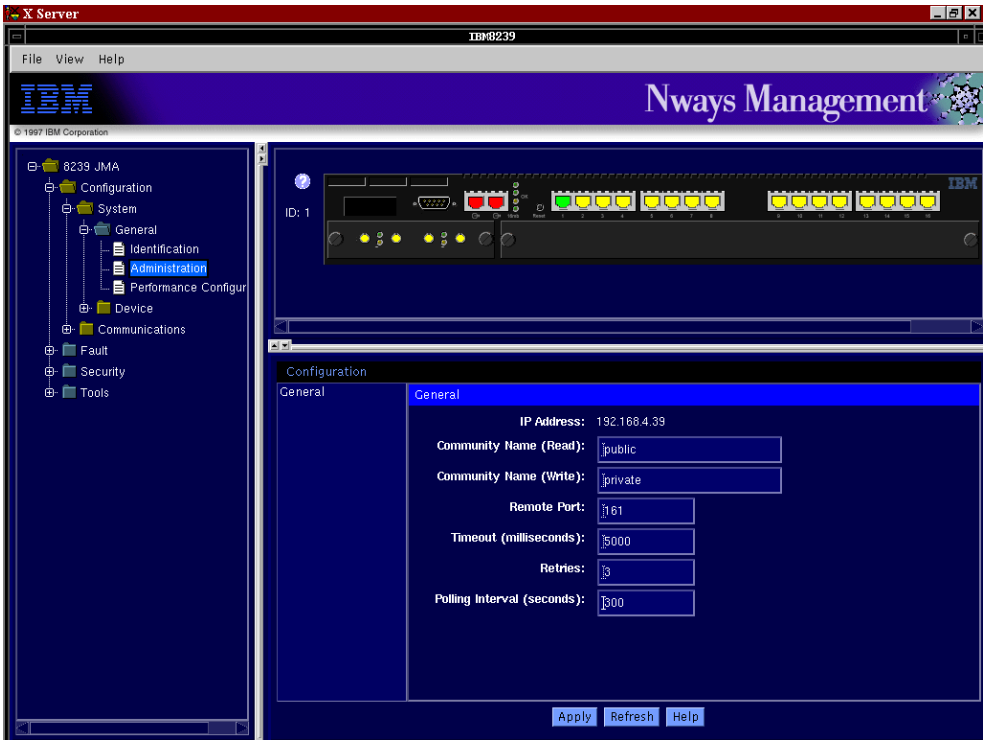


Figure 67. JMA Window for IBM8239 Showing System Administration Configuration

The navigation tree on the left lists all the elements of the JMA. Selecting an element will open it in the bottom section of the JMA window. From here, it will be possible to change configuration details for this device. Once any parameter has been changed you must click on **Apply** to update the device configuration, as long as the SNMP access is set to read/write.

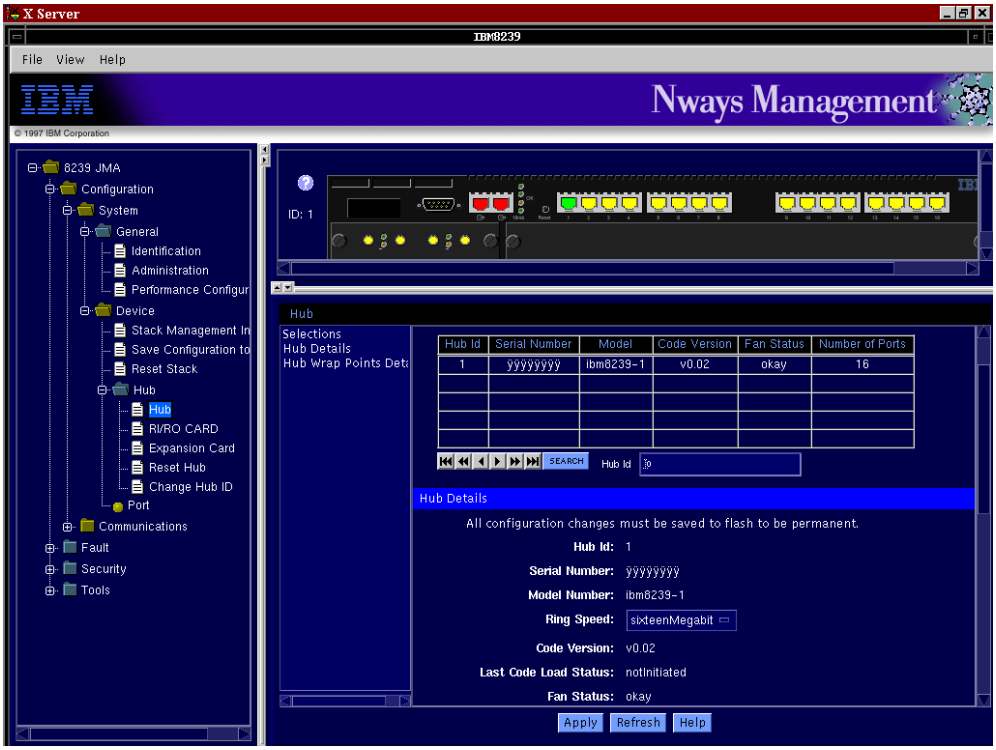


Figure 68. Hub Configuration Details in JMA

In the above view, the hub details are shown. These are the basic hub configuration details similar to the ones that can be entered from a console attached to the hub.

The JMA has all of the configuration support that the PSMs provided in previous versions of the Nways applications. In addition the JMA has built-in MIB browser with direct links to the JPM.

The graphic view of the device contains hot spots for instance, by clicking on a port the configuration details will appear and can be modified. This action produces the same results as if the Port button on the navigation tree had been selected.

Figure 69. Port Details for IBM8239

Figure 69 on page 110 shows the port details for port 1 on the 8239.

5.4 ATM Configuration

The ATM Campus submap contains ATM clusters and peer groups within which you will find devices with ATM interfaces (see Figure 70 on page 111).

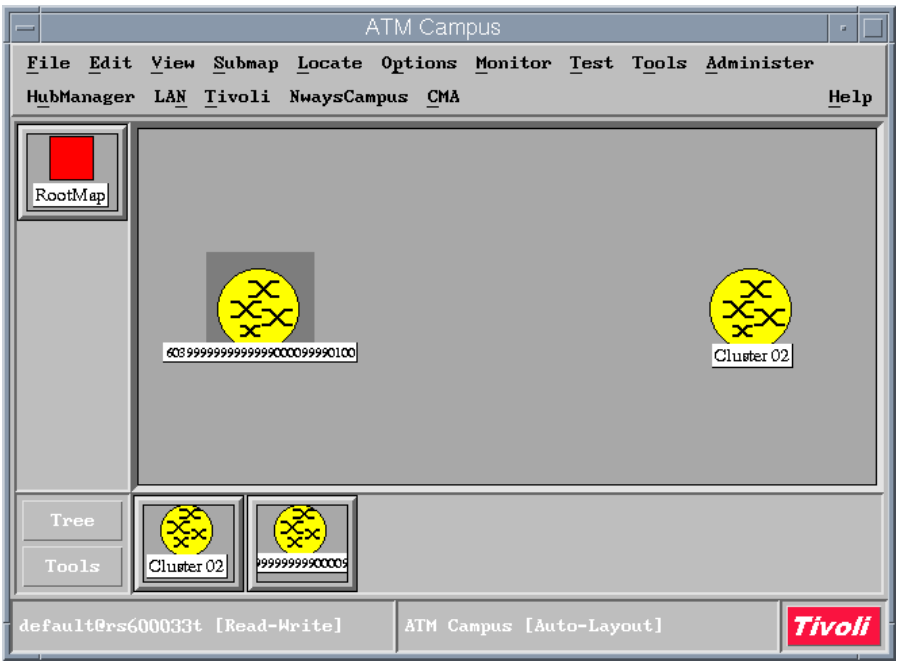


Figure 70. ATM Campus Default View

You can customize the labels of clusters, peer groups and ATM devices by selecting the device and then choosing **CMA->Change Label** from the menu bar.

The default node label for ATM devices is the IP address. You can change this to ATM Extended System Identifier (ESI). From the pull-down menu select:

Administer -->Campus Manager SMIT -->Configure -->Campus Manager - ATM Configuration and set the default format for node label.

The ATM Campus View can be exploded to show the devices in each PNNI group (see Figure 71 on page 112).

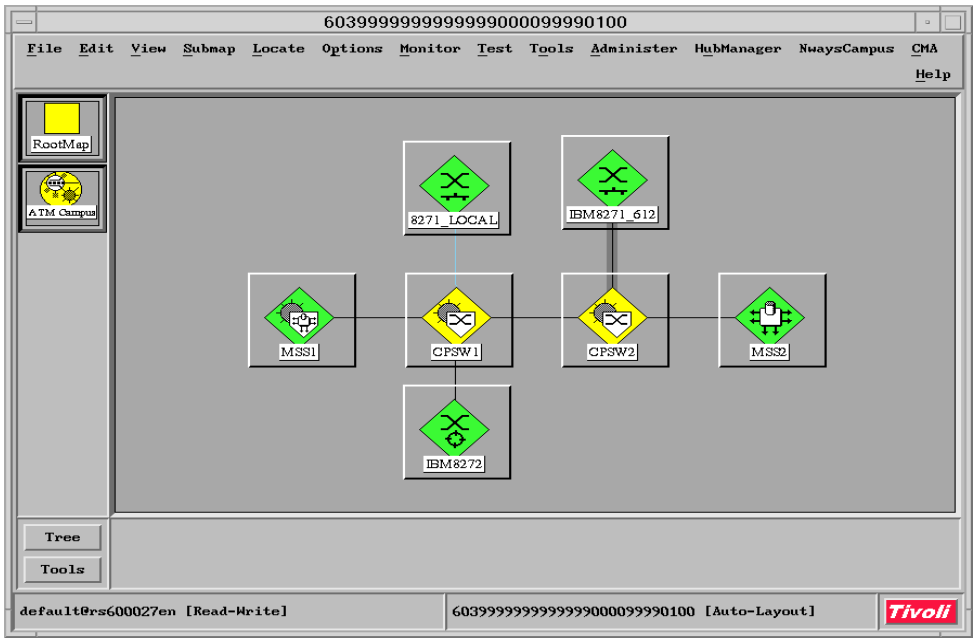


Figure 71. PNNI Group View from ATM Campus Submap

Selecting one of the icons from this view, such as CPSW1 will open the ATM view of the device, showing the ATM ports and connections to other devices.

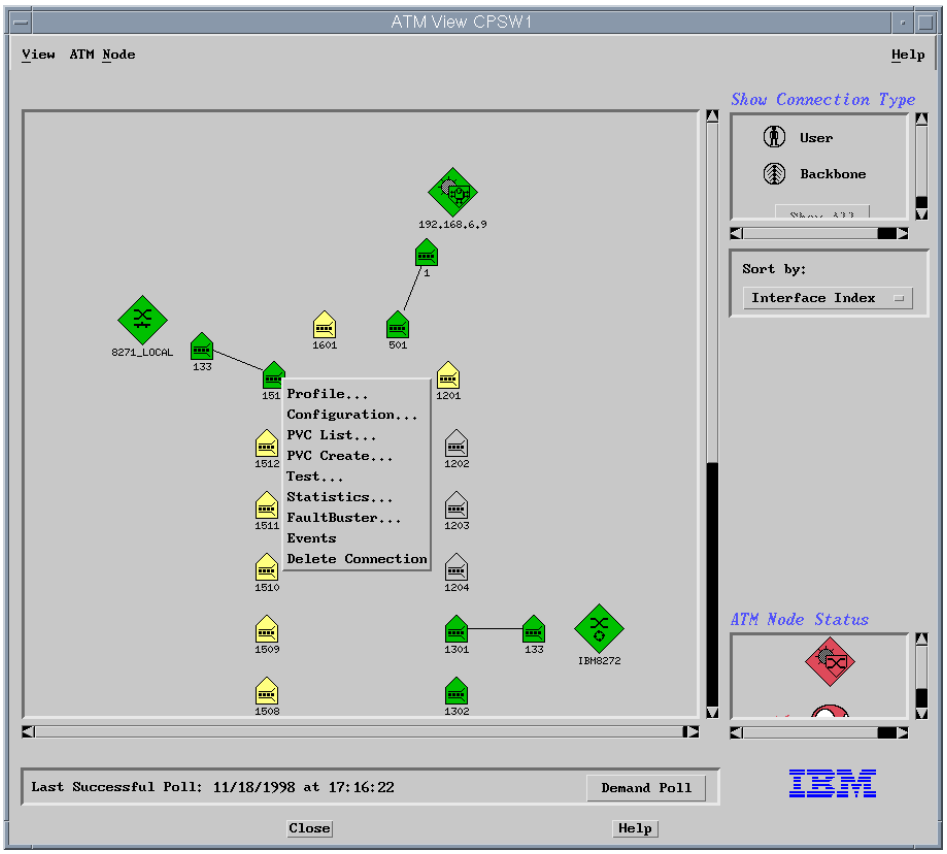


Figure 72. ATM View of CPSW1

All of the information in the view is gathered from the CPSW blade in the hub by retrieving the information from the ATM MIBs that are built into the firmware.

To view the configuration of the CPSW itself, either double-click on the switch icon at the bottom right of the screen or select **ATMNode->Configuration** from the pull-down menu. This opens the configuration panel for the ATM part of the CPSW.

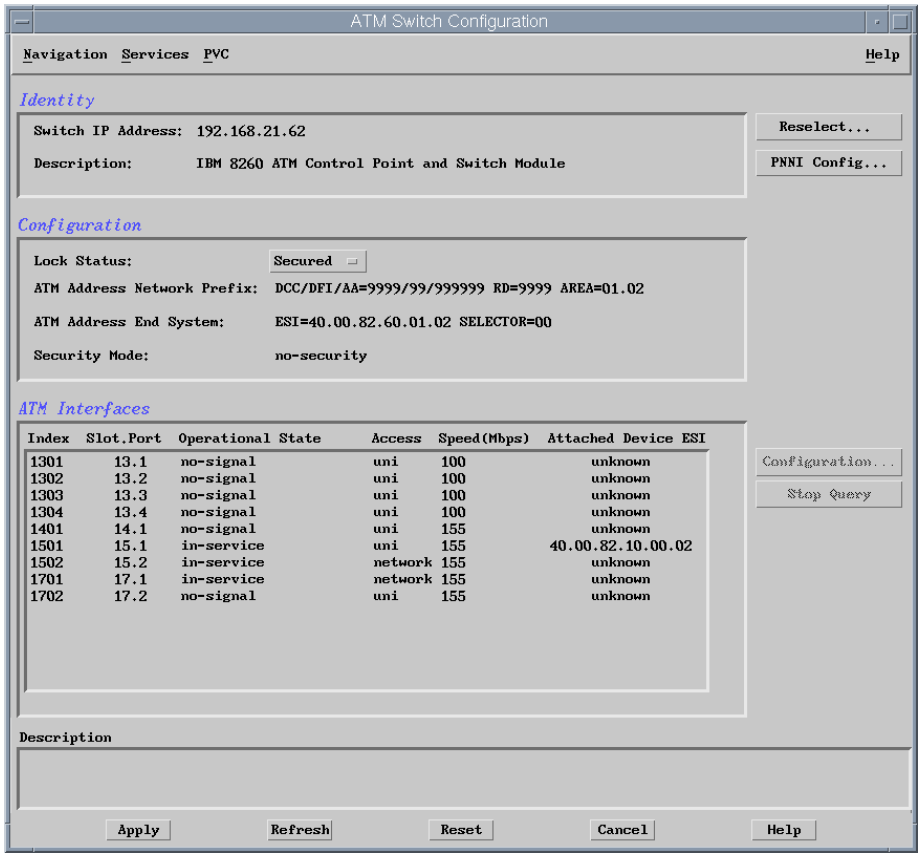


Figure 73. ATM Switch Configuration Panel for CPSW1

From this panel, the individual interface configurations and profiles can be viewed and modified. Either select an interface from the above panel and select the **Configuration** button or select an interface from the main ATM view of the device and use the right-hand mouse button to open the context menu then select the configuration option in that menu.

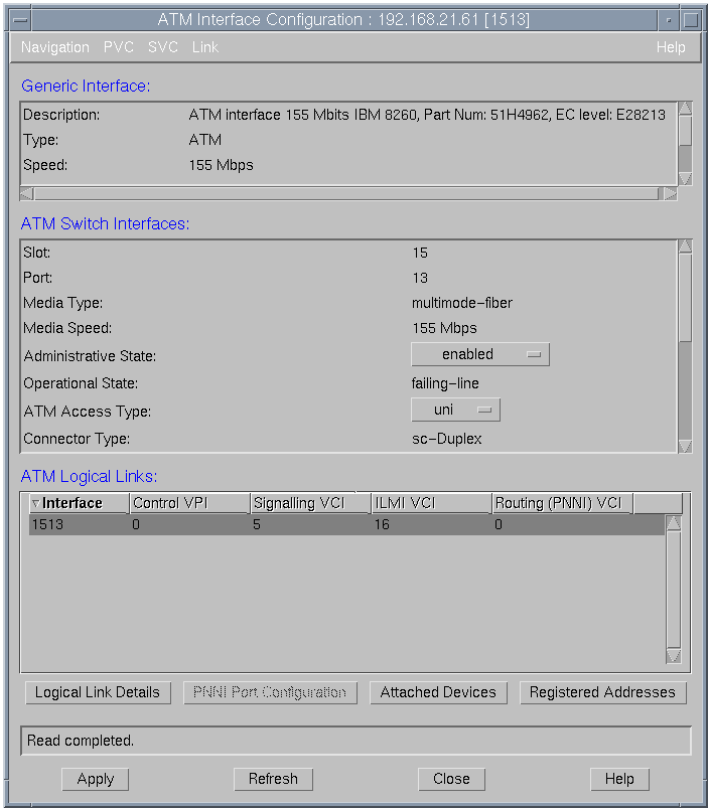


Figure 74. ATM Interface Configuration for Interface 1513 on Node CPSW1

The configuration screen for the interface allows modification of the physical port speed, as well viewing and working with the logical links that flow through that interface, (see Figure 75 on page 114).

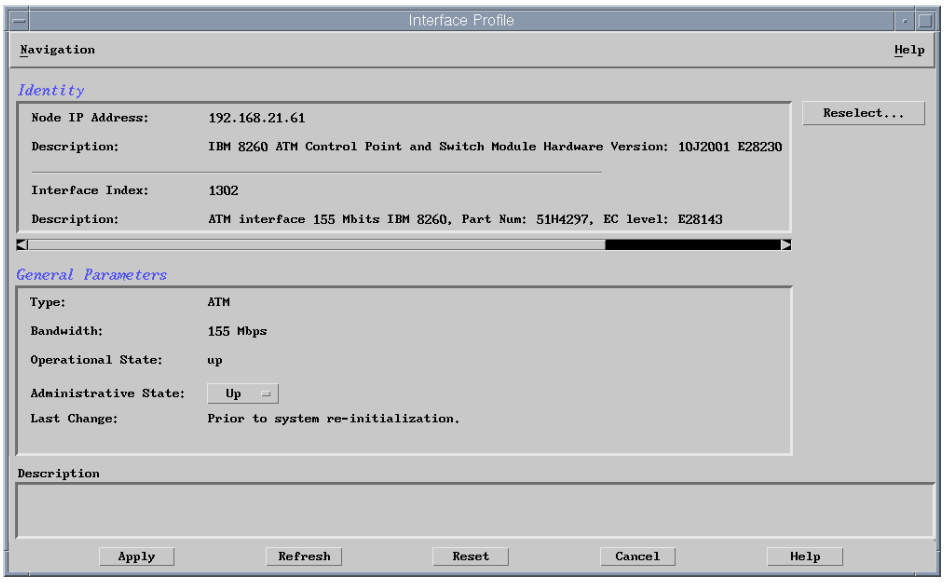


Figure 75. Interface Profile for Interface 1302 on CPSW1

It is also possible to show the attached devices on an interface in the following panel.

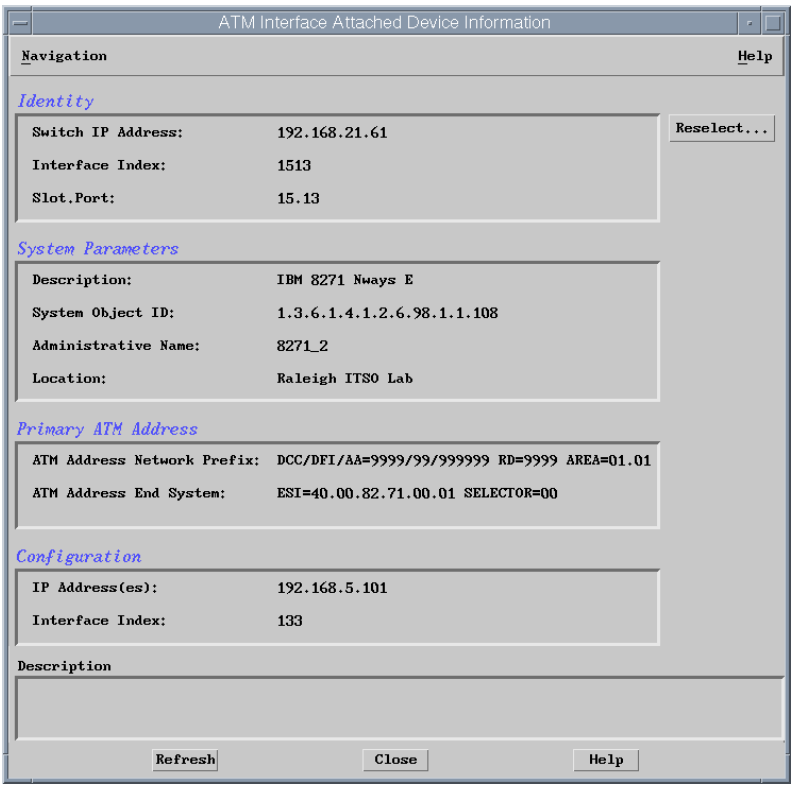


Figure 76. Attached Devices List for Interface 1513

5.4.1 VLANS

To view the total VLAN/ELAN network configuration, the LAN Emulation Manager function within Nways Manager must be used. This provides the ELAN management function through the VLAN icon and related submaps. The view is only provided for ATM Forum-compliant ELAN domains.

There are two configuration parameters for LAN Emulation:

- **LAN Emulation Polling Policy** - The options are either Regular (automatic) as per the polling interval or On Request. The default is Regular.
- **Polling Interval** - This controls the default polling interval. The default is 10 minutes.

As well as the physical ATM information, it is also possible to look at the logical links on an ATM node from the ATM View window. This is possible by either selecting the pull-down item **ATM Node->LAN Emulation,** or by double-clicking on the VLAN icon at the bottom right of the ATM View window. This will open a textual view of the LAN Emulation entities configured for this switch.

Figure 77. ATM/ELAN Configuration

From here we can see the LECS and click on **Configuration**.

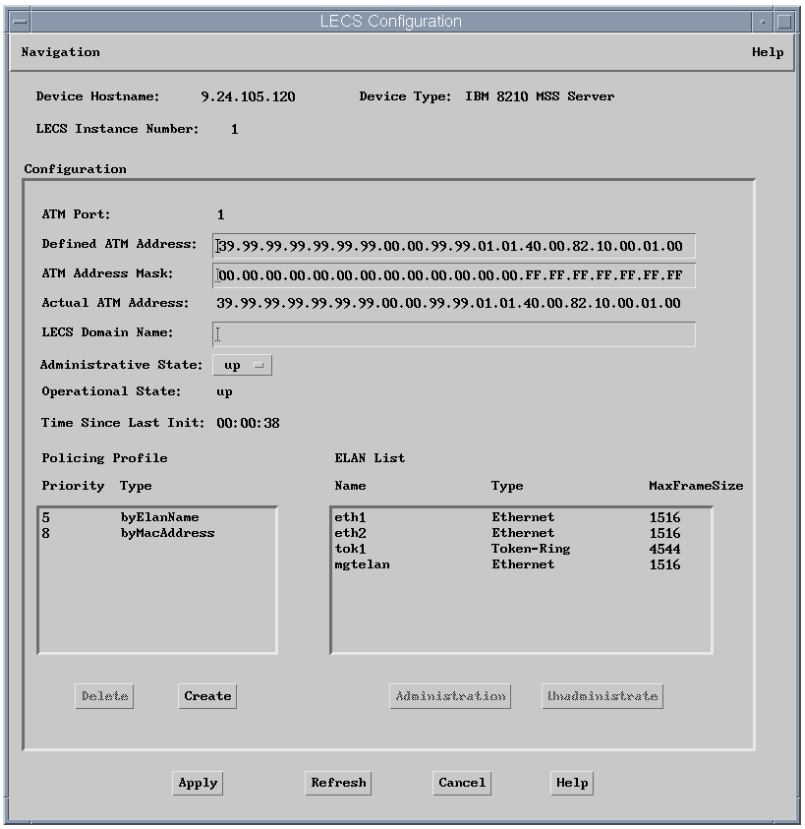


Figure 78. LECS Configuration Screen for the MSS

If we select an LES and click on Configuration we can see the LES settings as shown in Figure 79 on page 117.

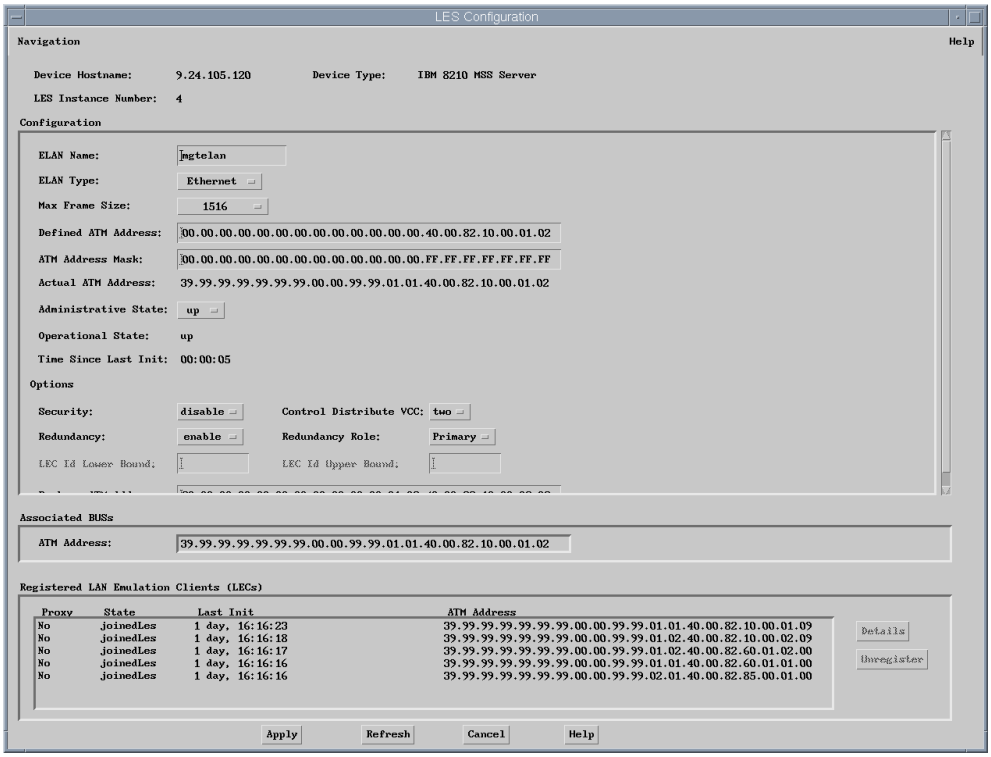


Figure 79. LES Configuration

Finally by selecting a LEC we can see the settings for the clients attached to the ELAN, (see Figure 80 on page 118).

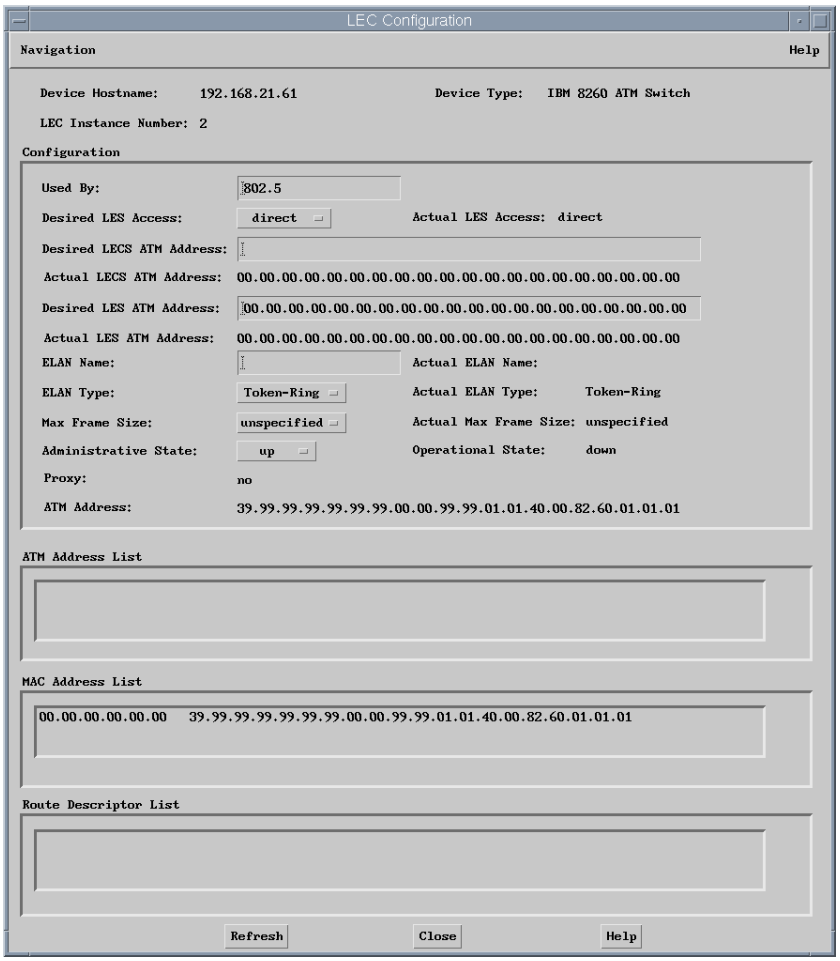


Figure 80. LEC Configuration

To view the logical topology double-click on the VLAN icon on the root submap to see Figure 81.

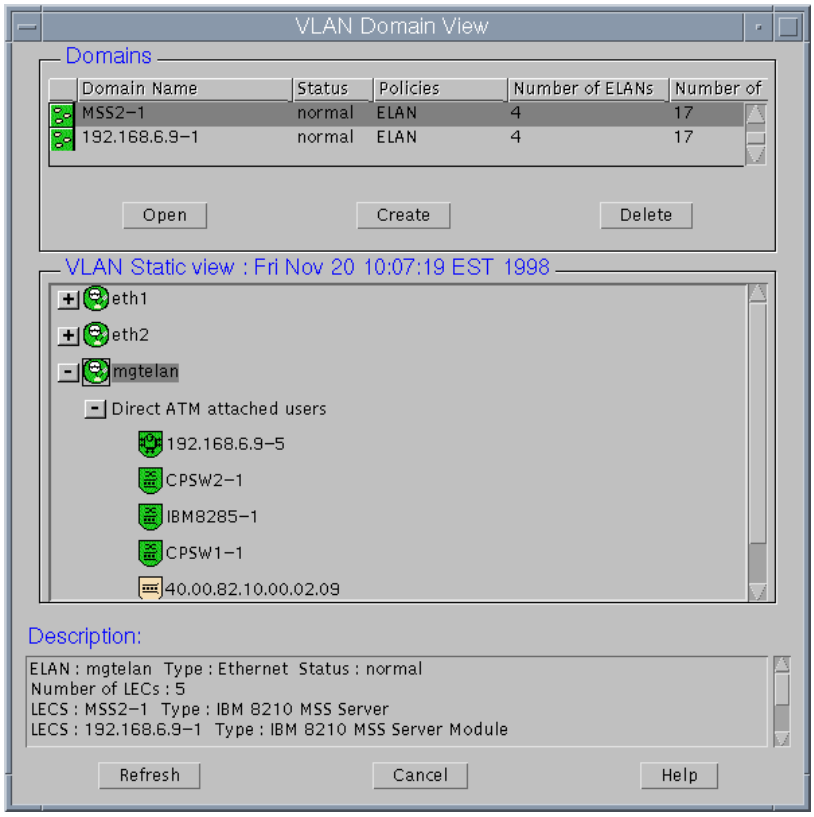


Figure 81. VLAN Domain View from Exploding VLANs Icon

If a domain in the top panel is selected, then the ELANs in that domain are listed. The ELANs can be expanded to list all of the entities within them. This panel supports the creation and deletion of domains as well as the administration of the existing domains. LECs can be moved by using drag and drop actions from one ELAN to another.

Clicking on a domain and selecting **Open** will present a graphical view of that domain, showing the ELANs and the LECS that administers it.

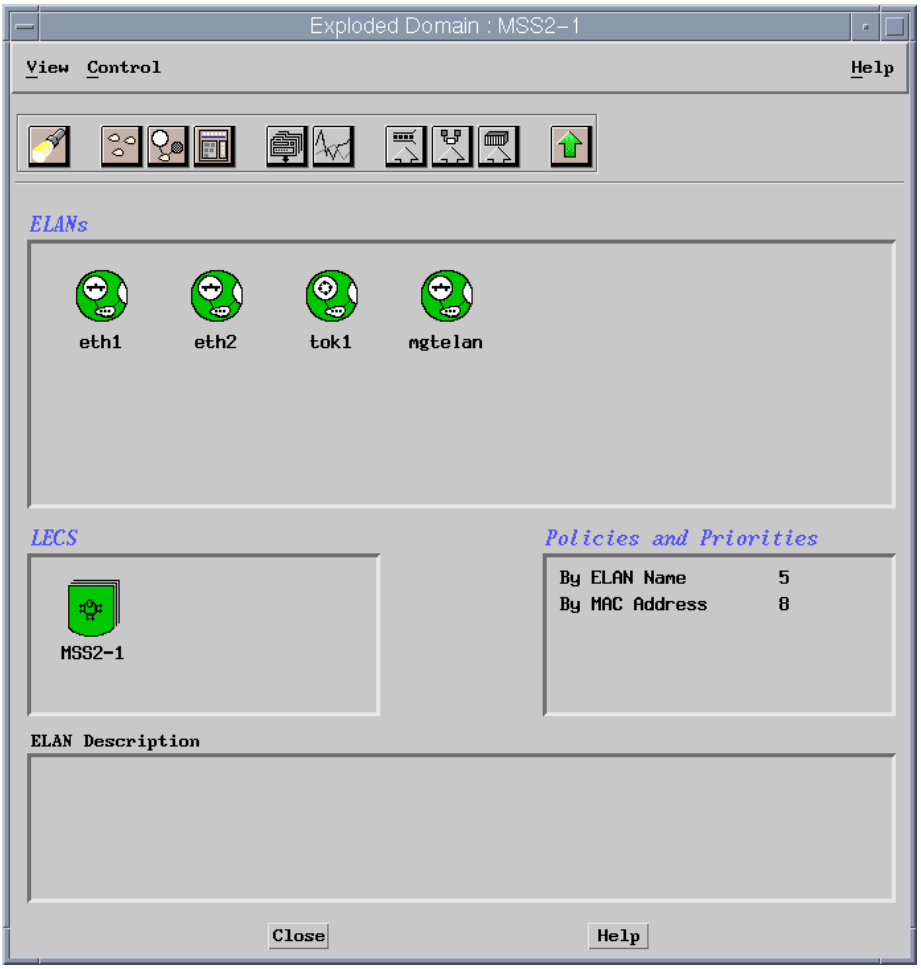


Figure 82. Exploded Domain View for Domain MSS2-1

Double-click on the **LECS** icon to see the LECS configuration panel. From here the LECS can be re-configured.

Double-clicking on any of the ELAN icons in the Exploded Domain view will open the ELAN view and display all of the ELAN entities.

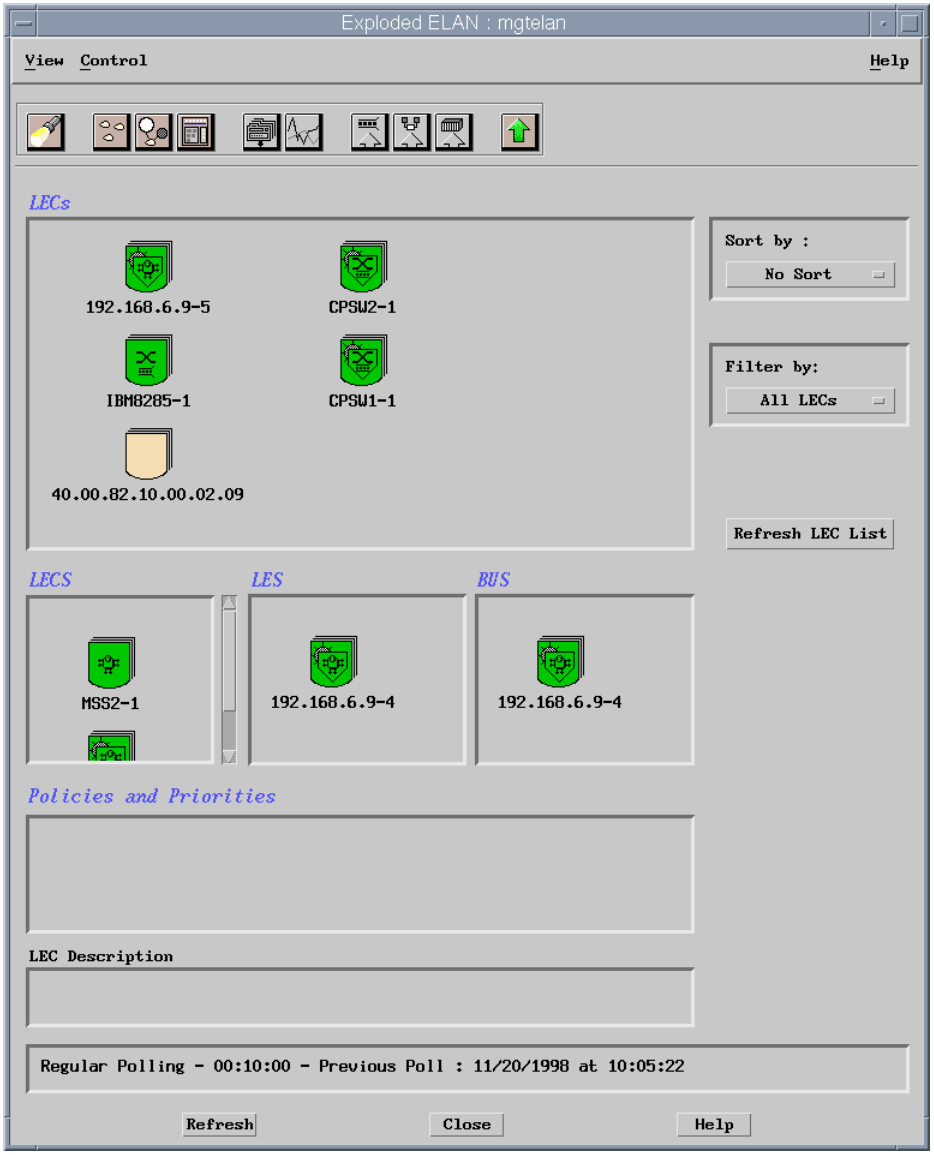


Figure 83. Exploded ELAN mgtelan

In Figure 83 the icons represent the ELAN entities. Double-clicking on any of then will open the specific configuration panel, whether the device is a LECS, LES/BUS or LEC. These screens can be used to modify the attributes of the ELAN entities.

5.5 IBM 2210, 2216 and 8210 Configuration Programs

The 2210, 2216 and 8210 devices provide configuration programs that correspond to the microcode level of the device, which are used for total configuration for these devices. You can launch these configuration programs from the Java-based device managers when using the manager workstation's local interface, provided that you have installed the respective configuration programs on the Nways for AIX management station.

By default, Nways determines the microcode level on the above devices, and associates the corresponding default configuration program directory. For example, the MSS 2.1 associates the default config program as /usr/mss210. There may be cases when there is a new microcode version, that Nways cannot determine the associated the relevant config program, so it will select the default configuration program as stated in the file:

`/usr/CML/JMA/java/websvr/properties/Cfg.txt.`

To see the associated directory for a particular device (that is, 2210, 2216 or 8210), launch the JMA view of the device and drill down the navigation tree to **MSS -> Configuration -> Configuration Tool** as shown in the Figure 84.

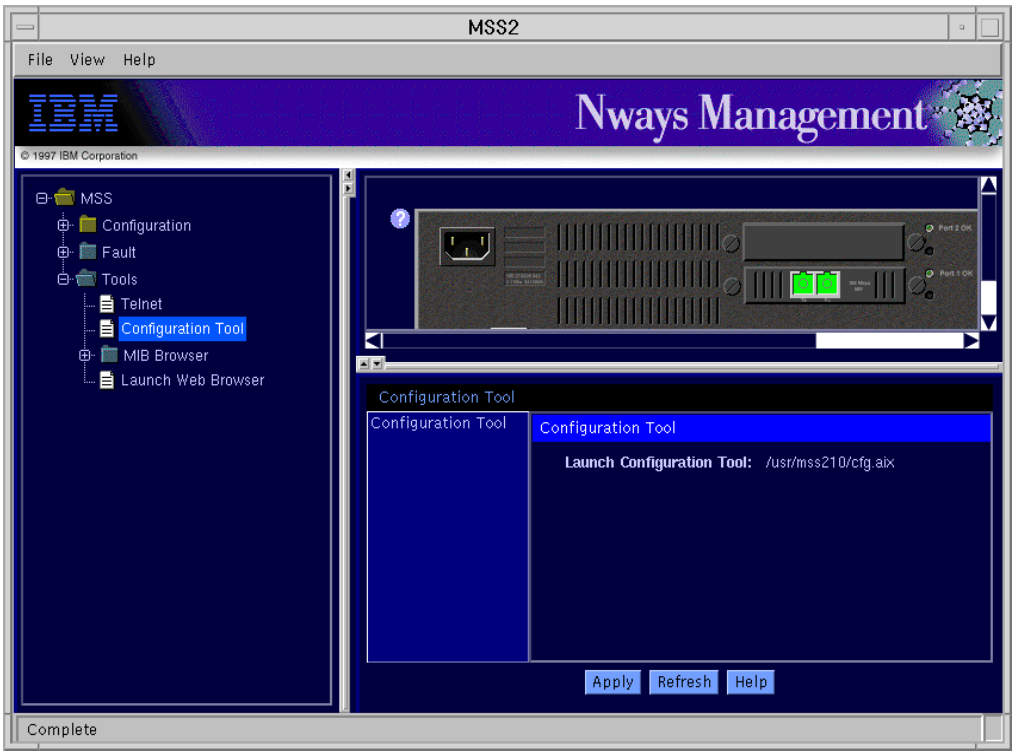


Figure 84. MSS Configuration Tool Directory

The configuration tool is launched by clicking on **Apply**. The main screen for the 8210 configuration program is shown in Figure 85 on page 123.

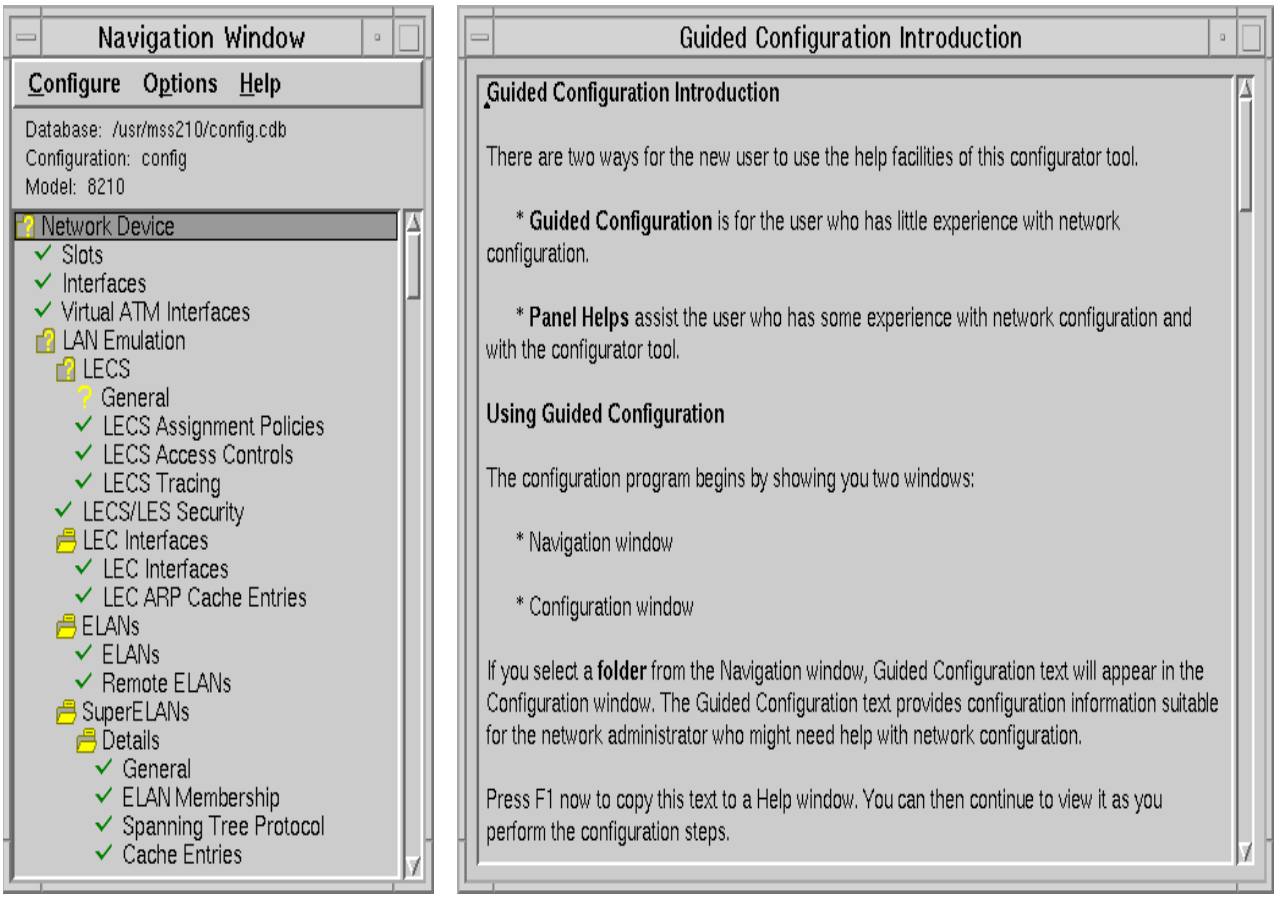


Figure 85. MSS Server Configuration Program

The MSS configuration program has two windows. On the left side is the Navigation Window. On the right side is the configuration window

5.6 IBM MSS Configuration Program for AIX

The MSS configuration program is the recommended way of doing end-to-end configuration for a MSS server, while other options such as RS232 console, telnet and Web browser exist. The ELAN manager under Nways ATM Campus manager provides management from an ELAN perspective including the LES/BUS and LECs but does not allow total configuration for the MSS.

The MSS configuration program is a stand-alone program that runs on Windows, OS/2 and AIX. It can be downloaded from the Web at `http://www.networking.ibm.com/820/820prod.html`.

The MSS configuration program version should correspond to the version of the MSS code version in the MSS server. More information on compatibility can be found in the previously mentioned Web site.

The configuration program also does not necessarily require direct IP connectivity. If all the user requires is to create a configuration file and save to hard disk for future use. There may be cases where a administrator or a

configuration specialist at a central office creates a configuration for all MSS servers, and then ships it electronically to regional offices for download.

The Navigation Window displays a navigation tree consisting of the various components and features of the MSS. To configure a particular component or feature of the MSS, click the left mouse button on the particular item. The configuration window will now display the configuration panel for the selected item. There may be multiple configuration screens per component. Help is available for each field within a panel. You can access the help by pressing PF1.

To send a configuration back to the MSS, IP connectivity should exist between the workstation and the MSS server, along with a read-write SNMP community name. The initial configuration of the MSS is done via the serial connection in order to set the IP address and SNMP community.

In our example below, the initial configuration was done to establish IP connectivity with the MSS over the network. In order to have connectivity to the MSS. We also had to configure an ELAN prior to having IP connectivity established.

Instead of repeating the initial configuration while doing the full configuration, we used the configuration program to retrieve the initial configuration from the MSS over the network. The retrieval is done by selecting from the pull-down menu bar **Configure -->Communications -->Single network device**.

In order to retrieve the configuration an IP address of the MSS and the community name should be entered as shown in Figure 86 on page 124. We used a community of private; which had read and write authority.

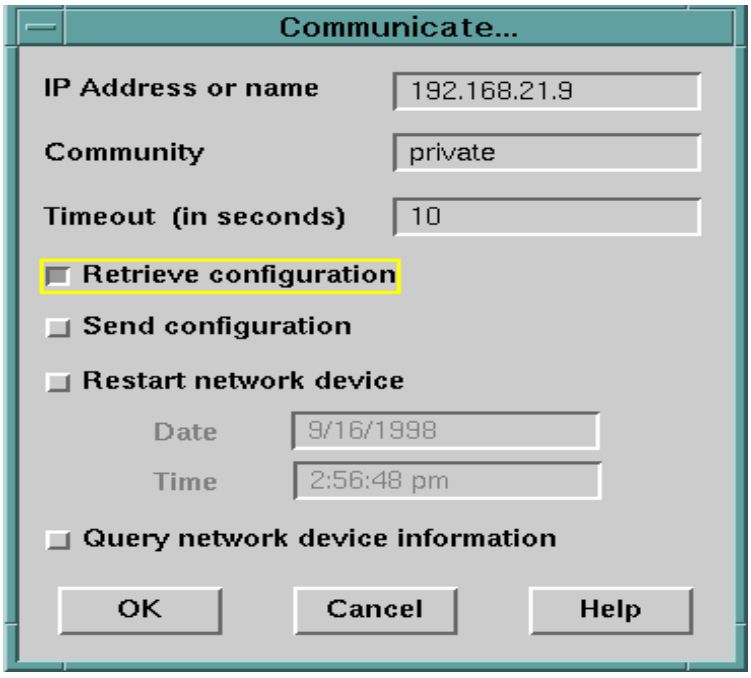


Figure 86. Retrieving the Current Configuration From the MSS

Select the retrieve option and click on **OK** to start retrieving the current configuration from the MSS server.

Once we had retrieved the configuration into the MSS configuration program we made the required additions to make the total configuration.

There were several steps involved in configuring the MSS for our scenario that consisted of four ELANs. Here we show an example of configuring a single ELAN.

5.6.1 Creating an ELAN Instance

Here, we show the steps to define a new Ethernet ELAN called eth1.

From the navigation tree select **ELANs**. The configuration window will show the ELAN details. At the top of the list is the ELAN mgtelan that was already created as part of the initial configuration done using an RS-232 console connection . In the ELAN Details page, we entered the following:

- An ELAN Name of eth1
- An ELAN Type of Ethernet
- The Max Frame Size to 1516

Ensure that the **Enable LAN** button is selected.

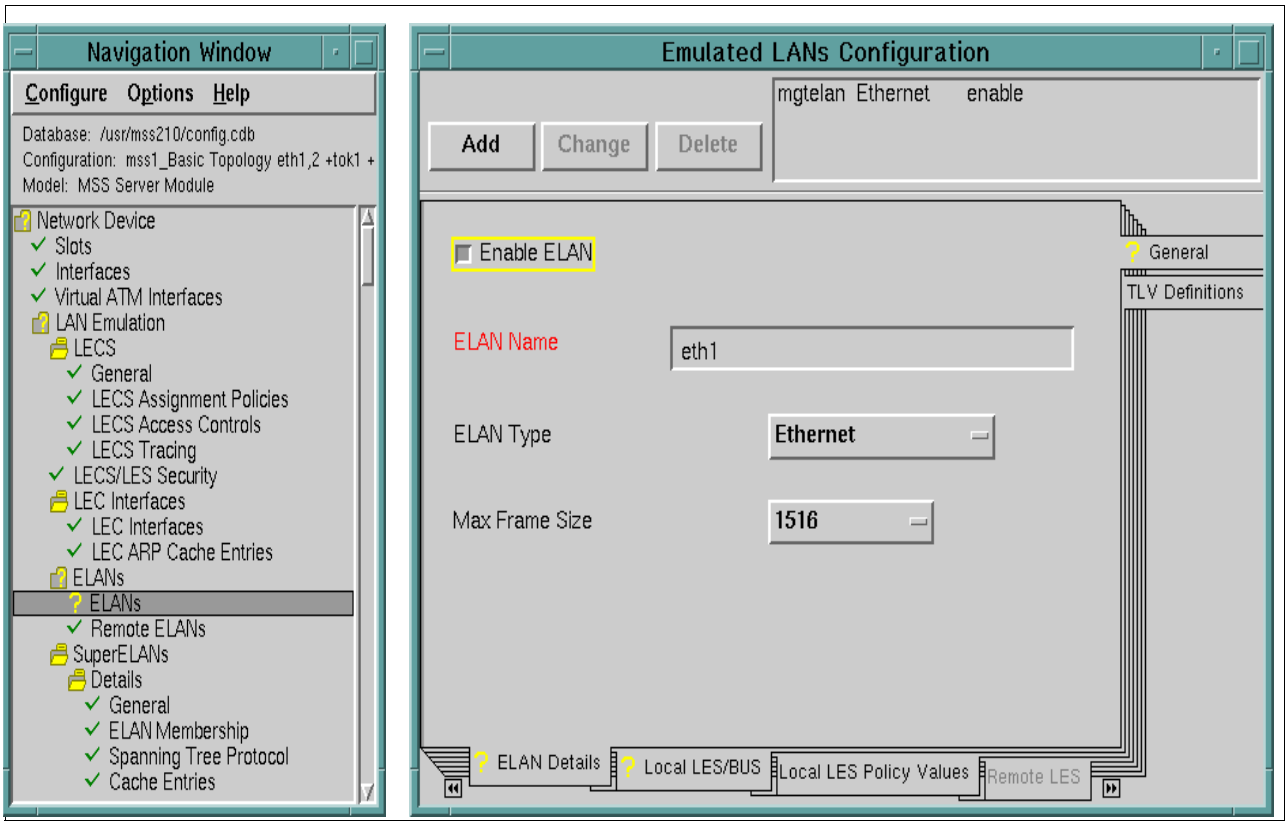


Figure 87. MSS ELAN Configuration - ELAN Details Page

Next we selected **Local LES/BUS**. Figure 88 on page 126 shows the Local LES/BUS Configuration.

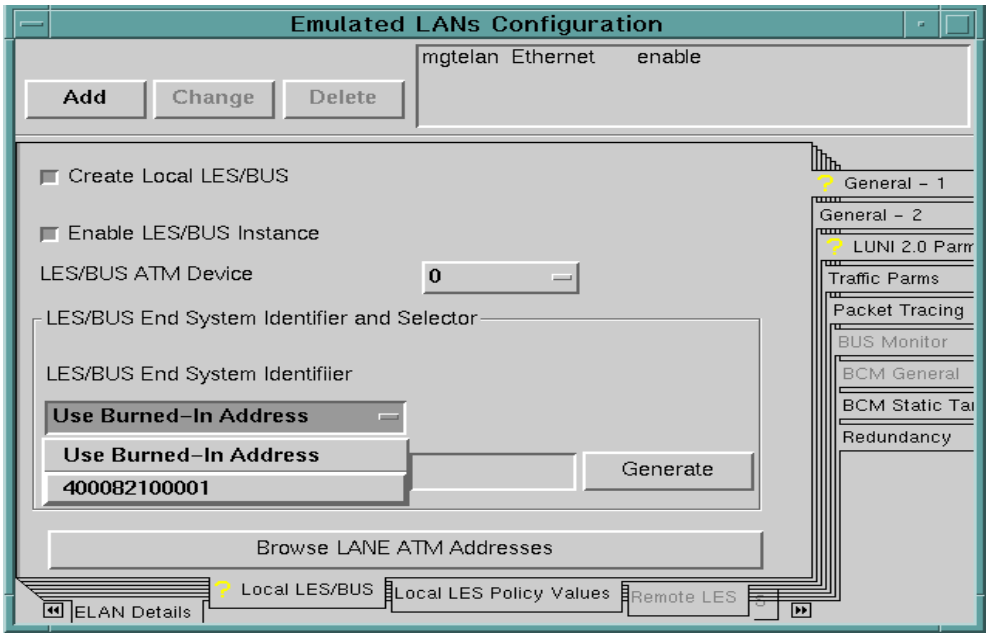


Figure 88. Selecting the ESI Value

For the LES/BUS ATM device parameter select the ATM physical interface to which the LES/BUS instance is bound from the drop-down list. In our case it was 0 as we only had a single ATM physical interface. Instead of using the burned-in address as an ESI which is ambiguous, we defined an ESI value of 400082100001 and selected that from the drop-down list. For the selector byte, we let the configuration program generate a free one automatically by clicking with the mouse on the **Generate** button.

Figure 89 on page 126 shows the final values for the parameters in the Local LES/BUS General page 1.

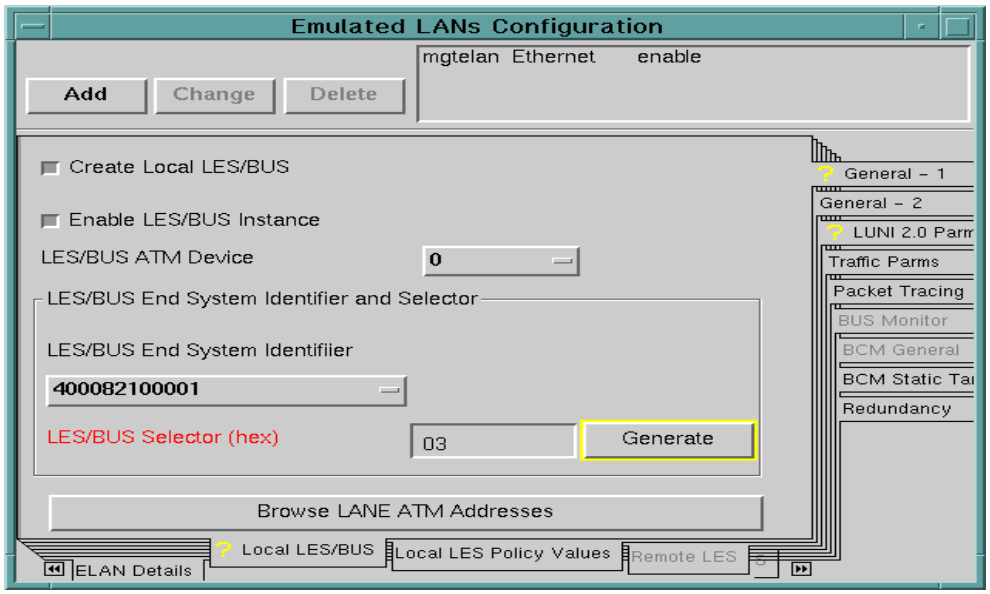


Figure 89. ELAN Configuration - Local LES/BUS

Select the label **LUNI 2.0 Parms,** then select a value of 2 as the ELAN identifier. This must be a unique number.

The next step was to set the policy values for this ELAN. Select **Local LES/BUS Policy Values** followed by **ELAN Name page**. For the ELAN Name parameter, we selected eth1 as the ELAN name policy value to be part of this ELAN.

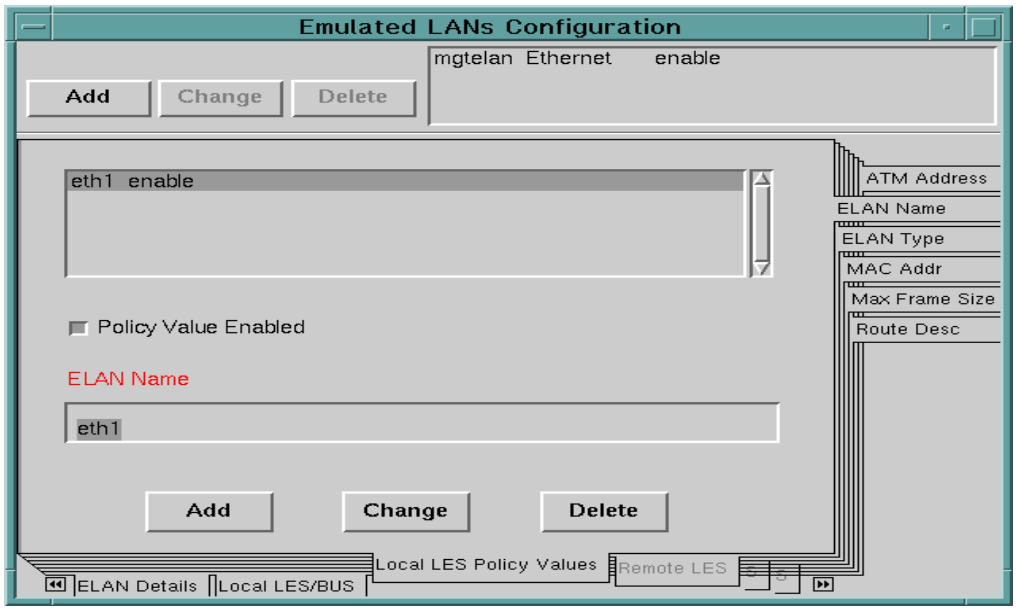


Figure 90. Policy Values: ELAN Name

Click on the **Add** button on top of the screen, to add this ELAN to the configuration. Figure 91 on page 127 shows the results of this action.

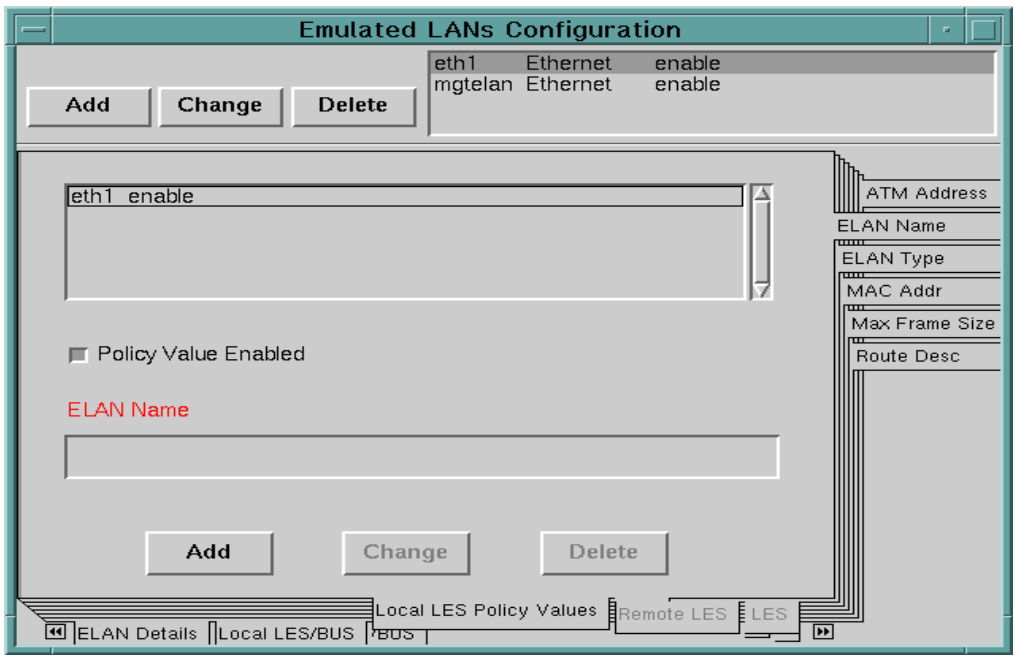


Figure 91. Adding an ELAN

This completed the configuration for the ELAN eth1 example. As part of our Nways scenario requirement, we executed further configuration steps in creating additional ELANs, LECS configuration, IP addresses and redundancy.

5.6.2 Downloading the Configuration to the MSS

Once we completed the additional configuration we were ready to download the configuration to the MSS. Before downloading the configuration, we saved the configuration to the hard disk, serving as a backup in case the configuration for the MSS is lost.

To send the new configuration to the MSS server, select **Configure--> Communications --> Single network device,** (see Figure 92).

Figure 92. Communicate Settings

Enter the IP address and the community name, select **Send Configuration** and **Restart network device.**

Click on the **OK** button to send the configuration into the MSS server, and then restart the MSS server. The restart performs a reload operation and is disruptive to the operations of the MSS. The Date and Time parameters are for doing a restart at a scheduled date and time automatically.

5.7 2210 Nways MRS Configuration Program

The JMA for 2210 router provides basic configuration options for the device. If total configuration for the router is required, the recommended method would be to use the 2210 router configuration program. Some of the other options for the total configuration are the RS232 console, XMODEM and TFTP.

In this section, we briefly cover the IBM 2210 MRS configuration program. The 2210 MRS configuration has the exact look and feel of the MSS configuration

program. The 2210 MRS configuration program is shipped along with the 2210 router. Newer versions of code can be downloaded from the following Web:

```
http://www.networking.ibm.com/220/220prod.html
```

The 2210 MRS configuration program version should correspond to the version of the MRS code on the router. Otherwise, unpredictable results can occur. More information of version compatibilities can be found in the previously mentioned Web site.

The MRS configuration can be launched either from a JMA view of the 2210 or from the command line. It is also possible to add it to the NetView menu. To launch from the JMA view, select **Tools->Configuration Tool.**

Again in our scenario, we did the initial configuration using the RS232 console to establish IP connectivity to the 2210 routers and define SNMP community.

Once we had IP connectivity established, we used the retrieve feature from the pull-down menu to retrieve the existing configuration on the 2210 router as shown in Figure 93 on page 129.

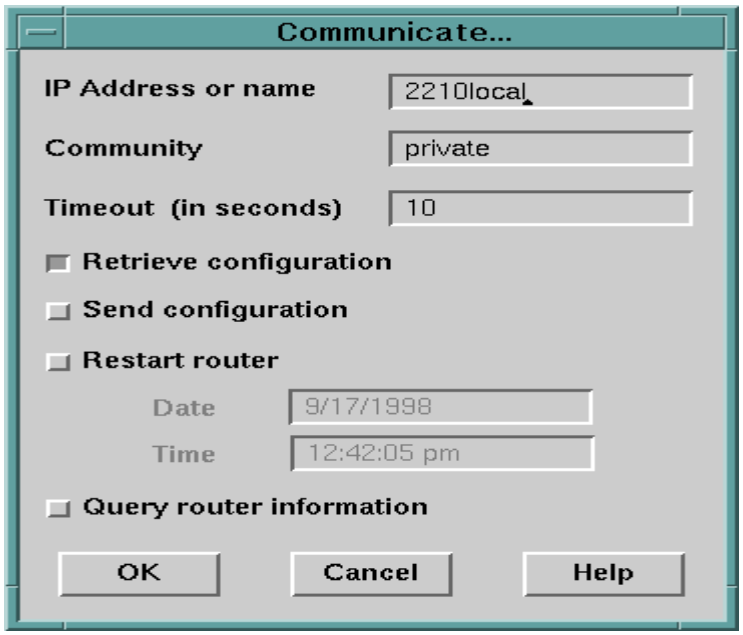


Figure 93. Retrieving the Configuration from the 2210 Router

Once we had retrieved the current configuration from the NVRAM of the 2210 router into the configuration program, we made the full configuration required for our scenario. The next step was to send this configuration to the 2210 using **Configure --> Communicate --> Single Router** from the pull-down menu in the navigation window, as shown in Figure 94 on page 130.

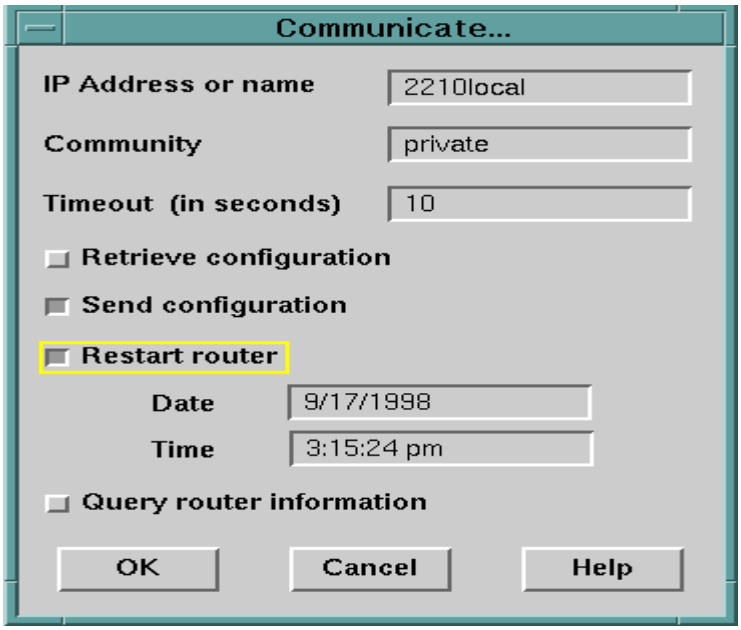


Figure 94. Sending the Configuration to the Router

We selected both the **Send Configuration** and **Restart router** options, so that once the configuration is updated on the router, the routers will perform a restart to activate the new configuration.

Note

Configuration changes should be done first on devices farthest from the configuration station in order to avoid losing connectivity to devices.

For example, if RTR B's IP address on the interface to RTR C is changed and restarted using the configuration program, all devices to the left including RTR B will lose IP connectivity to RTR C.

5.7.1 IBM 2216 MAS Configuration Program

The IBM 2216 MAS configuration is very similar in look and feel to the MSS and IBM 2210 MRS configuration programs. Also, these devices have a common code implementation, thus the configuration of the common features for the above mentioned devices are the same. We do not cover the details of this program in this book.

More information on the 2216 MAS configuration programs can be found at the following URL:

`http://www.networking.ibm.com/216/216prod.html`

5.8 Example Using Status and Configuration

This example shows how to view the status and configuration when a cable is removed from a switch connected to the ATM network via an uplink. Figure 95 on page 131 shows the ATM network running.

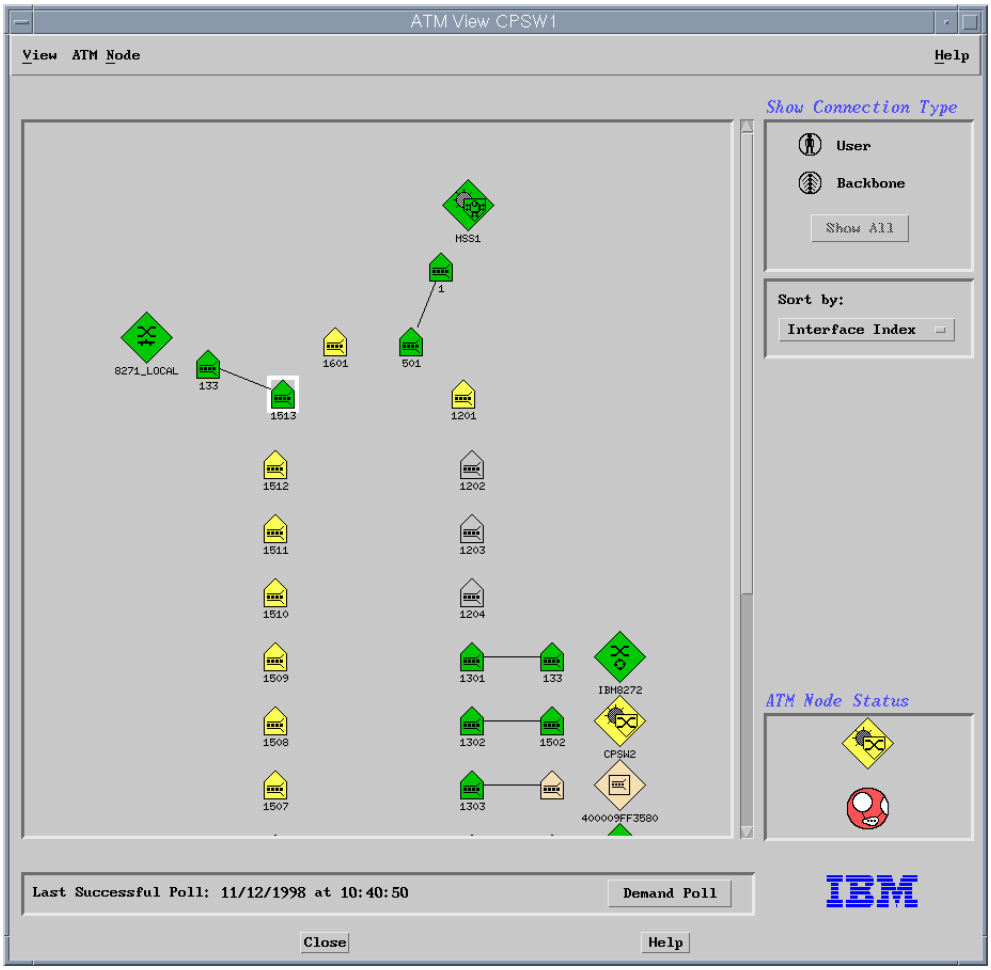


Figure 95. ATM Network from CPSW

The 8271 is connected at port 1513. The connection information for the 8271 is shown in Figure 96 on page 132.

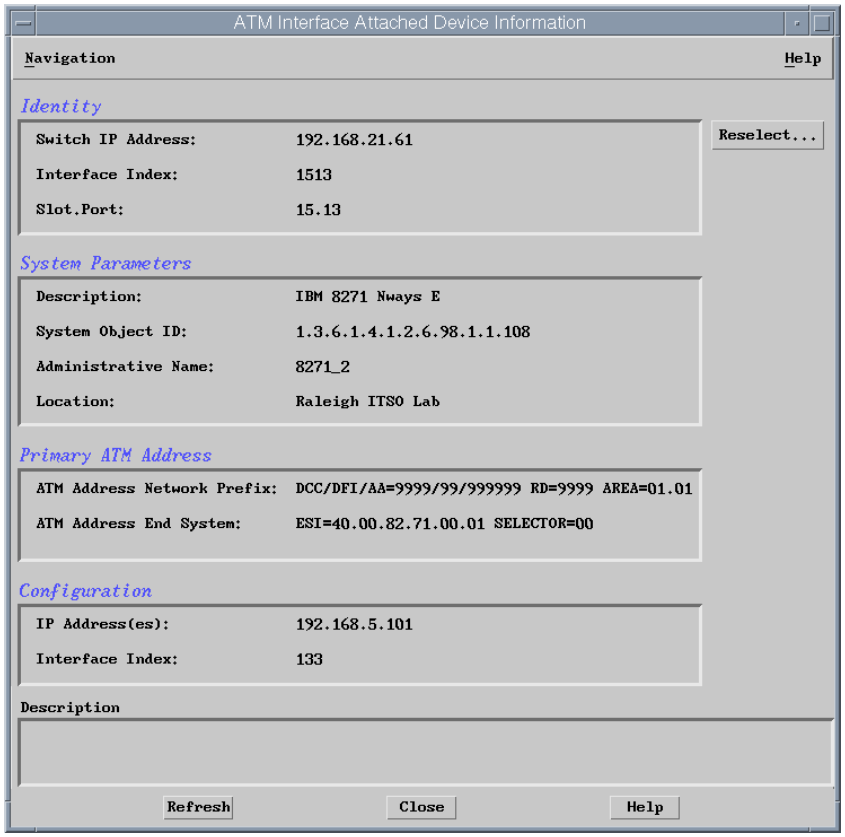


Figure 96. Connected Device Details

The ATM submap shows the 8271 from an IP perspective (see Figure 97 on page 133).

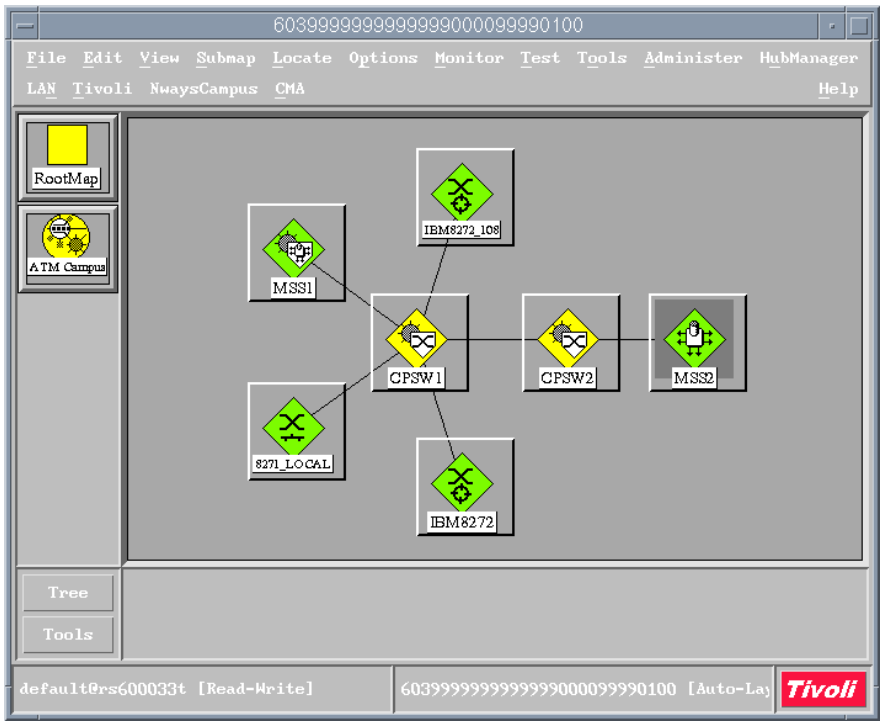


Figure 97. IP View of the 8271 Connection

From here we can see that the 8271 is also in the same subnet as the switch module. When we disconnected the cable we received the trap shown in Figure 98 on page 133.

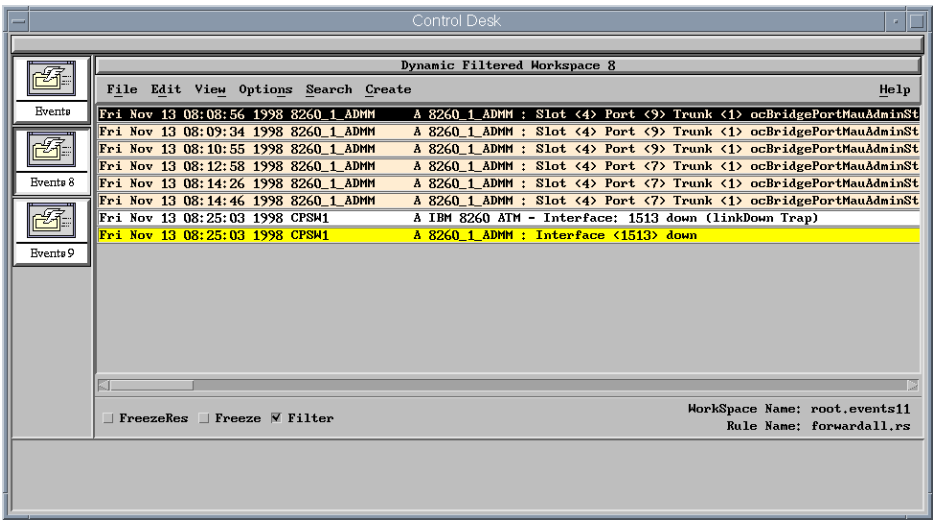


Figure 98. Interface Down Trap

From the ATM submap we can see the 8271 has been disconnected from the subnet.

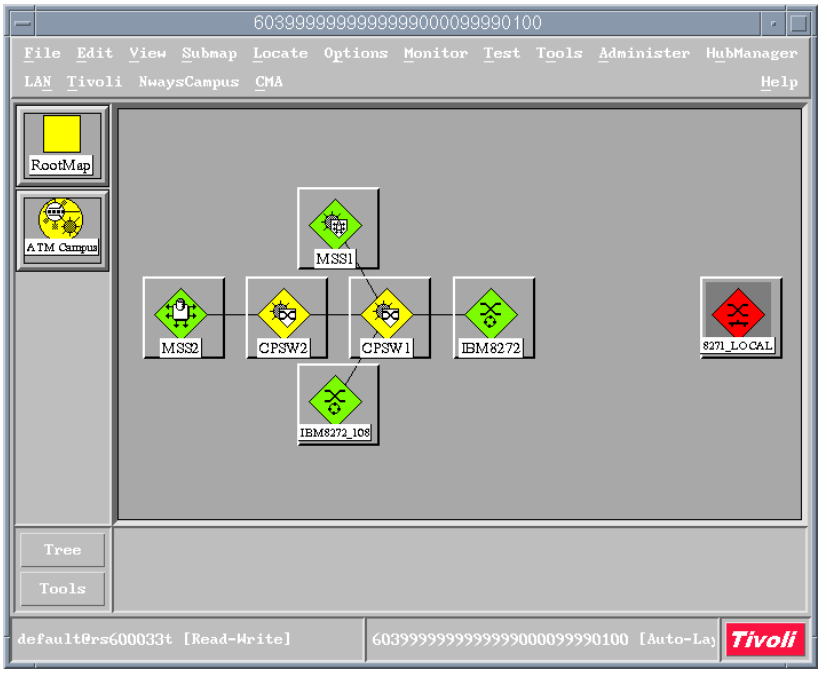


Figure 99. IP View of Disconnected 8271

When the trap arrived we initiated the fault buster application by selecting **FaultBuster** from the context menu of the CPSW. This will show the screen as shown in Figure 100 on page 135.

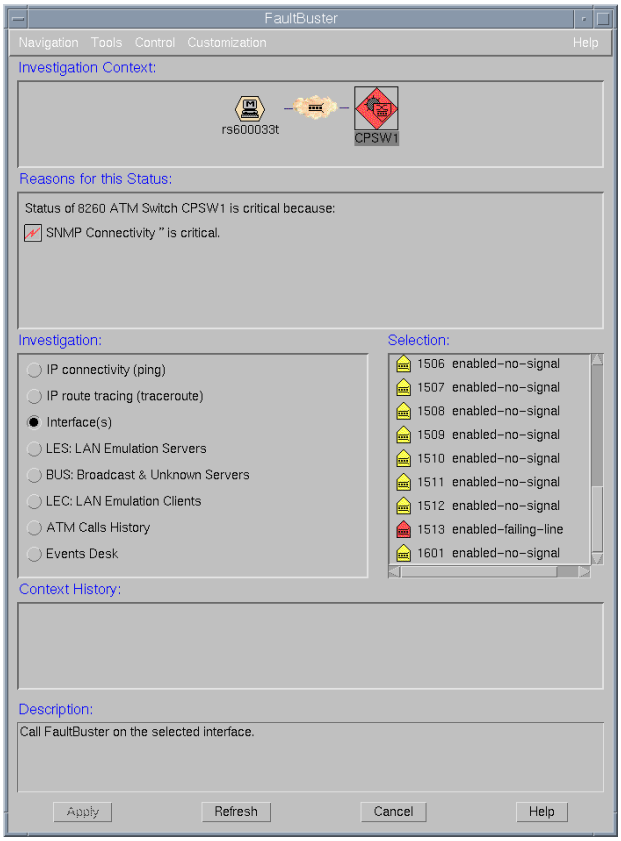


Figure 100. FaultBuster Screen for the CPSW

By selecting interfaces we can see the port that is currently down. The view from the CPSW shows the port is reporting a failing line (see Figure 101 on page 136).

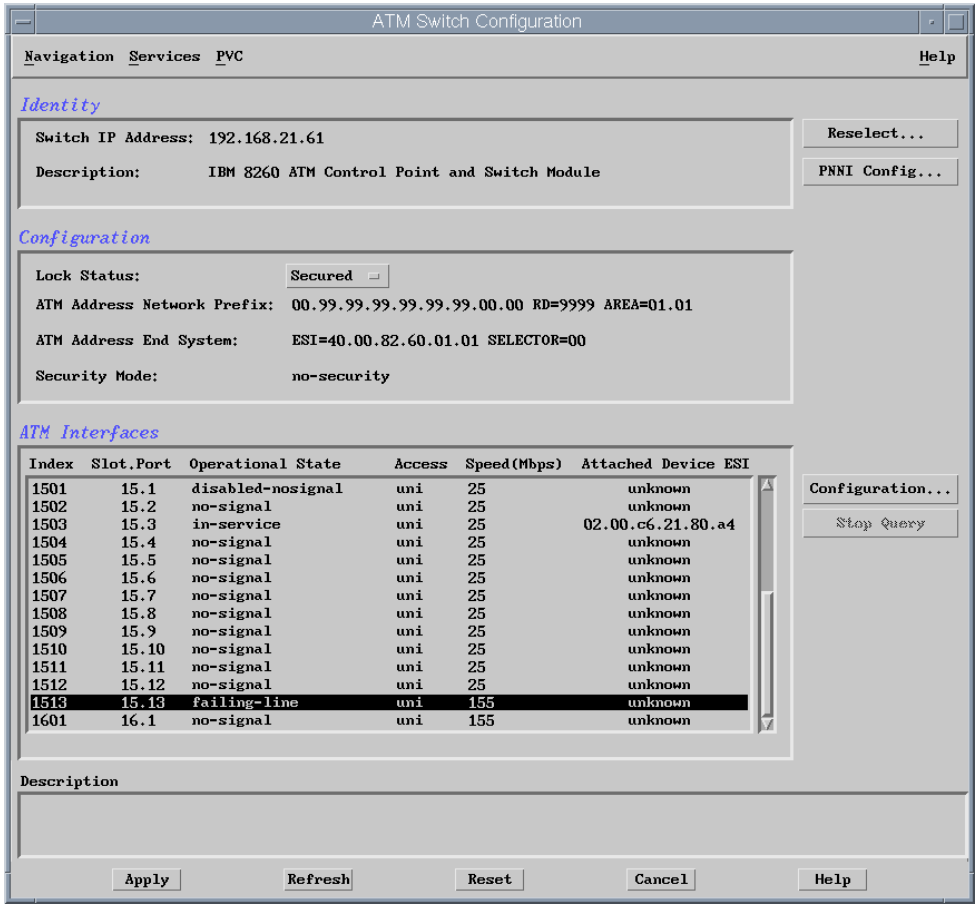


Figure 101. Failing Line Error

From the ATM switch configuration screen we can see that the 8271 has disappeared from the screen and port 1513 is now red. (See Figure 102 on page 137).

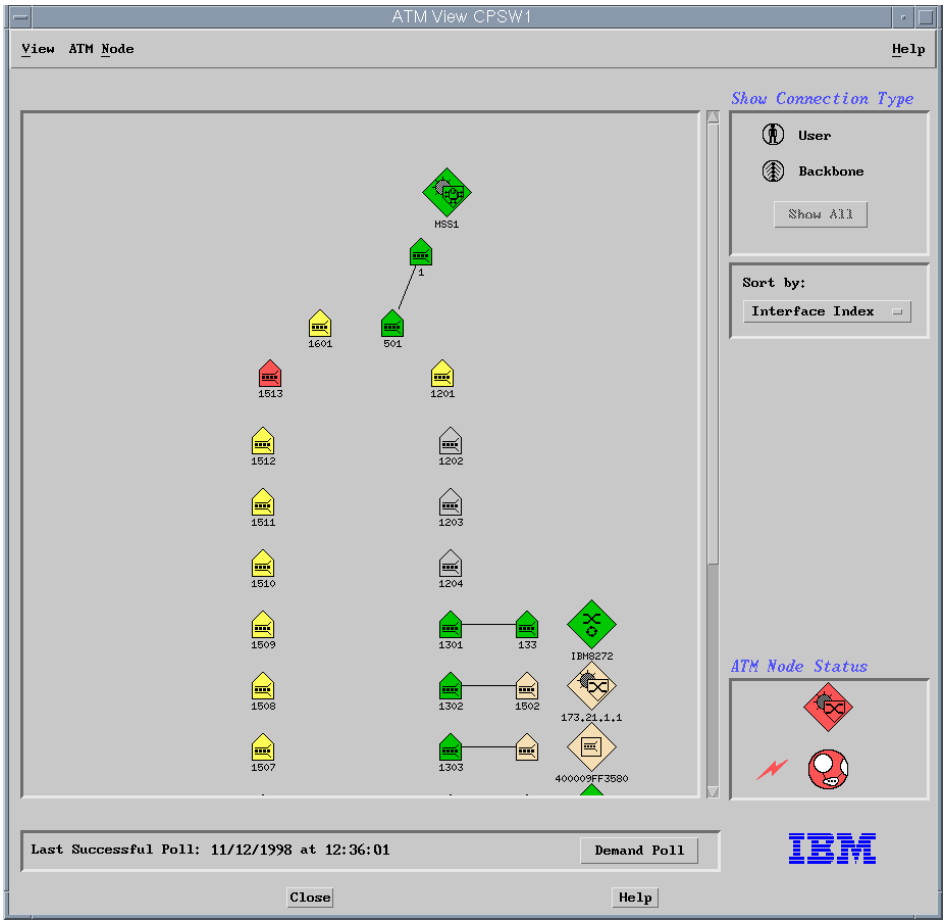


Figure 102. ATM View during Disconnect

When the cable was re-connected to the 8271 we received the event shown in Figure 103 on page 137 showing the interface was back up again.

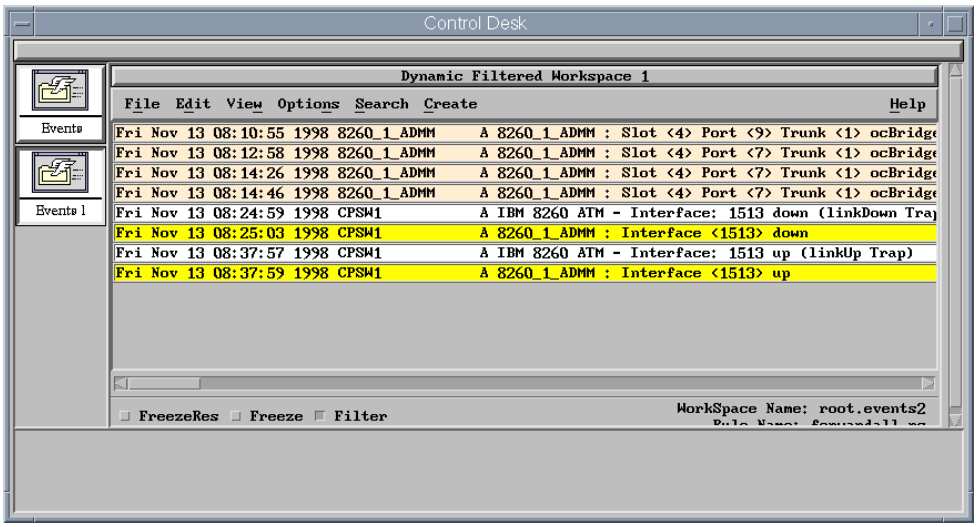


Figure 103. Interface UP Event

5.9 Reporting on Configuration

A new NetView command provided with Version 5.1 allows the capability to interrogate the NetView database and produce an text output of the data in tabular form.

The example below shows how to list the ATM switch nodes in our database. We created a text file called ATM.format. The line SELECTRULE says that any device that matches the criteria of ATM_SWITCH is to be reported on.

```
SELECTRULE:ahm_isATM_SWITCH=TRUE
SELECTFIELD:1:Object ID
SELECTFIELD:2:Selection Name
HEADER:ATM Switch Report:
HEADER:-------------
OUTPUT:Object ${1} (${2}) is a node.
FOOTER:Total Objects in Database  :  ${TOTAL_OBJECTS}
FOOTER:Number that match criteria :  ${NUMMATCH}
FOOTER:Number that fail criteria  :  ${NUMFAIL}
FOOTER:End Nodes Report.
```

Figure 104. ATM .format File

We ran the command shown below:

```
nvdbformat -f ATM.format
```

The output is a list of the switches contained in our database.

```
Object 460 (IBM8285) is a node.
Object 462 (CPSW2) is a node.
Object 464 (CPSW1) is a node.

Total Objects in Database  :  1380
Number that match criteria :  3
Number that fail criteria  :  1377
End Nodes Report.
End Nodes Report.
```

Figure 105. Output from nvdbformat Command

Chapter 6. Event and Performance Management

This chapter focuses on the events that are generated in our managed environment, either from devices, performance monitoring applications or directly from the management software. We show the operation of the fault management tools that are available to the network management user. In the performance section we take a look at what is available in the software and also provide a section on setting up RMON.

6.1 Event Management

The applications associated with event management are as follows:

- NetView Event Desk
- NetView Rulesets
- ATM Manager
- Device Managers
- JPM/JMA (discussed in Chapter 7, “Nways Java/Web Management Applications” on page 211)
- RouteVision (discussed in Chapter 8, “RouteVision Suite” on page 269)

This section contains the details of the review of SNMP MIBs and associated traps for the IBM Nways networking hardware. The objective was to list all the potential events that can be generated and sort through these to filter out the unwanted events. When we have decided on what events we want to see we then work through what actions need to be performed on reception of these events including identifying correlation where appropriate.

We assembled all the Abstract Syntax Notation (ASN) for the Nways networking hardware from various sources. This process is time-consuming but will provide a good event management system if you can eliminate all the insectary events that are generated in such an environment. These events can also be used in NetView rulesets or automated actions.

We can use the JMAs and PSMs to assist in defining the events.

6.1.1 Event Configuration Using PSMs

The fault management options available from the PSM menu are:

- Trap Configuration where traps can be enabled and assigned severity levels.
- Trap Receiver Tables where the IP address or addresses are defined for the network management stations that will receive the traps.

The Fault Options panel can be opened from the PSM menu bar by selecting **Management --> Fault --> Fault Options**. Figure 106 on page 140 shows the screen for the 8271.

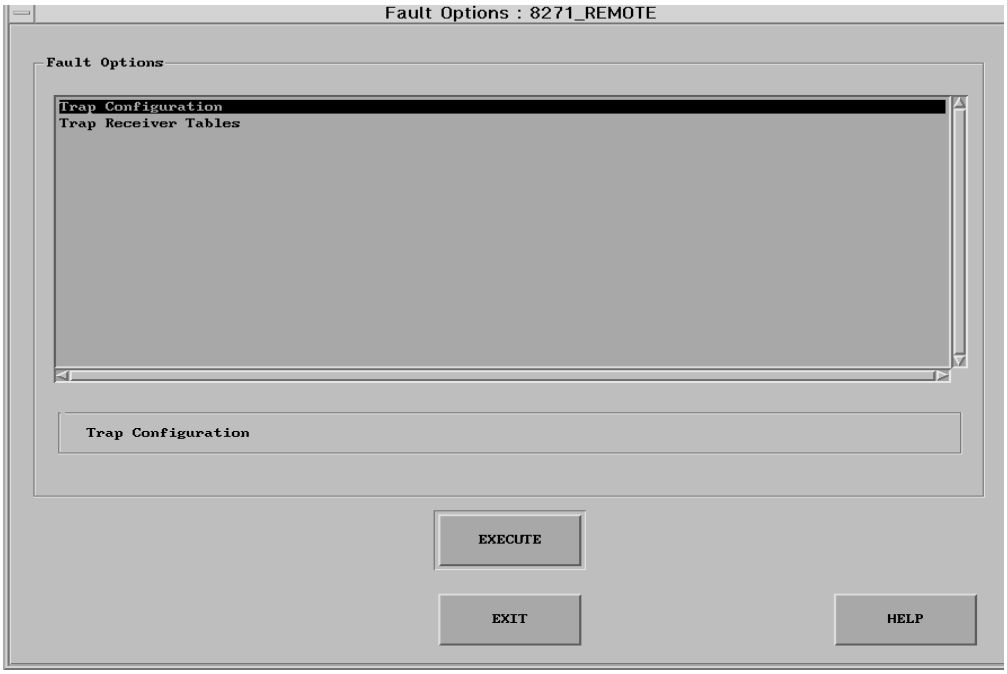


Figure 106. 8271-108 PSM Fault Management Options

The 8271 supports the following traps:

- Cold Start
- Warm Start
- Link Up (port up)
- Link Down (port down)
- Authentication Failure
- Spanning Tree New Root
- Spanning Tree Topology Change
- Switching Mode Change
- Temperature Change
- Etherpipe Failure

Clicking on **Execute** will list all of traps for the 8271.

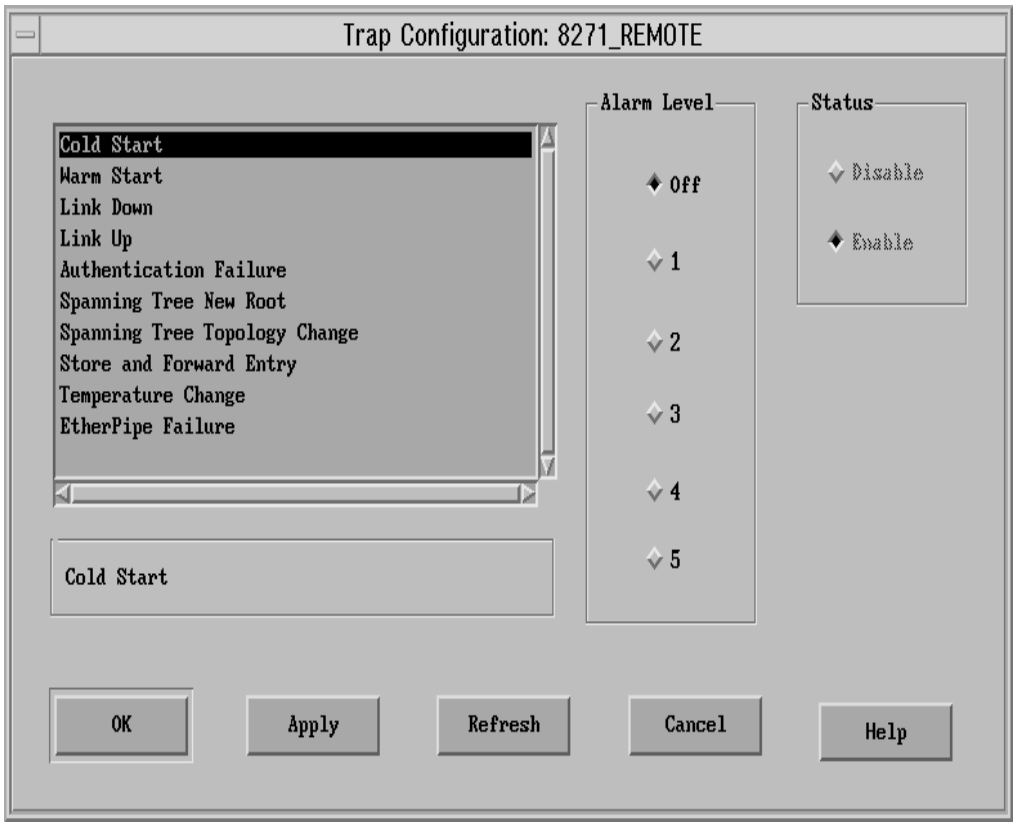


Figure 107. 8271-108 PSM Trap Configuration

The status can be enabled or disabled. A trap that is enabled generates a trap if a corresponding fault condition occurs. The trap generated also has an alarm level, which indicates the sensitivity or severity for the trap generated. The possible values are Off and 1 through 5, with 5 being the most sensitive or severe. A trap can be ignored when the alarm value is off, although the trap is enabled.

The Alarm value and status can be changed by selecting each trap and modifying the values.

Note

All the 8271 traps except the Authentication Failure trap are enabled by default and cannot be disabled, but the alarm level is set to off. Setting the alarm level to off lets the trap be ignored. For a trap to be generated and displayed in the NetView Events display, the alarm level should be a value other than off, and the status should be enabled.

Here, we explain how the trap is processed by NetView and Nways PSM. When NetView receives a trap from a device, the following takes place:

1. The trap is received and processed by the trapd daemon and logged in the event log by NetView. If the trap configuration for the trap is not set to LOGONLY, the trap will appear in the event log.
2. The trap is then passed to the Nways Manager PSM for the device. If under the trap management panel the alarm level is anything other than OFF, then the PSM formats the trap and forwards the trap to the management

application transporter (MAT), which puts the formatted trap into the event log.

For example, we enabled the traps for authentication failure and link-down/link-up, and set the alarm levels so that traps can be generated (see Figure 108 on page 142).

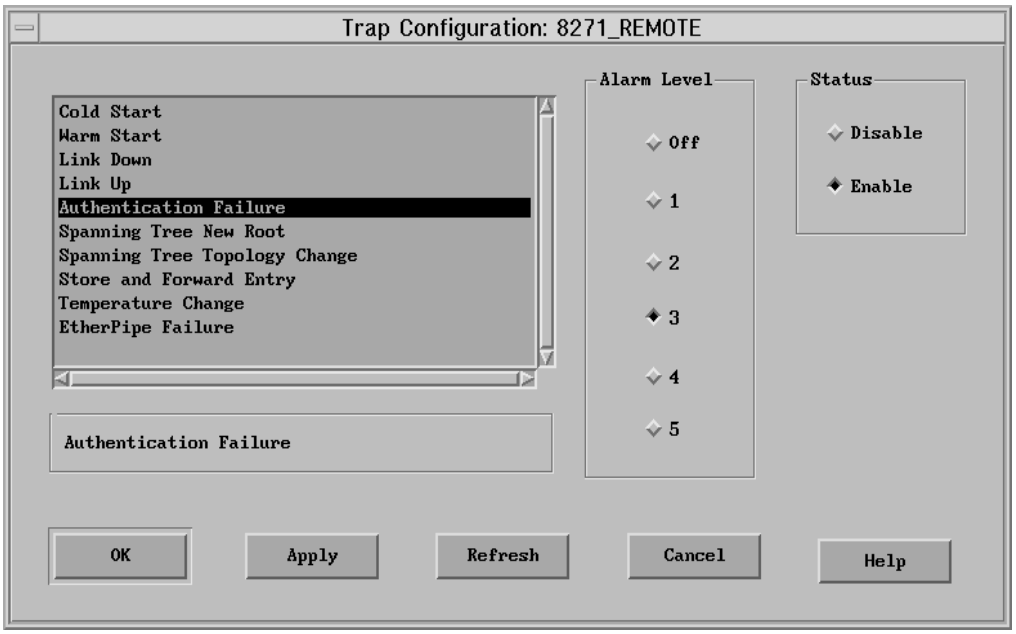


Figure 108. Trap Configuration

Click on **OK** when complete.

6.1.2 Trap Receiver Tables

Once the required traps for the management environment are enabled, and the alarm levels are set, the Trap Receiver table has to be configured. The Trap Receiver table contains an entry for each SNMP manager (that is, management station) to which a trap is to be forwarded. Each entry also has a corresponding community name that the management should use to receive traps, and also a virtual switch number through which the management station can be contacted.

Figure 109 on page 143 shows the trap receivers for our management scenario with the IP address of the management station set and a community name of public.

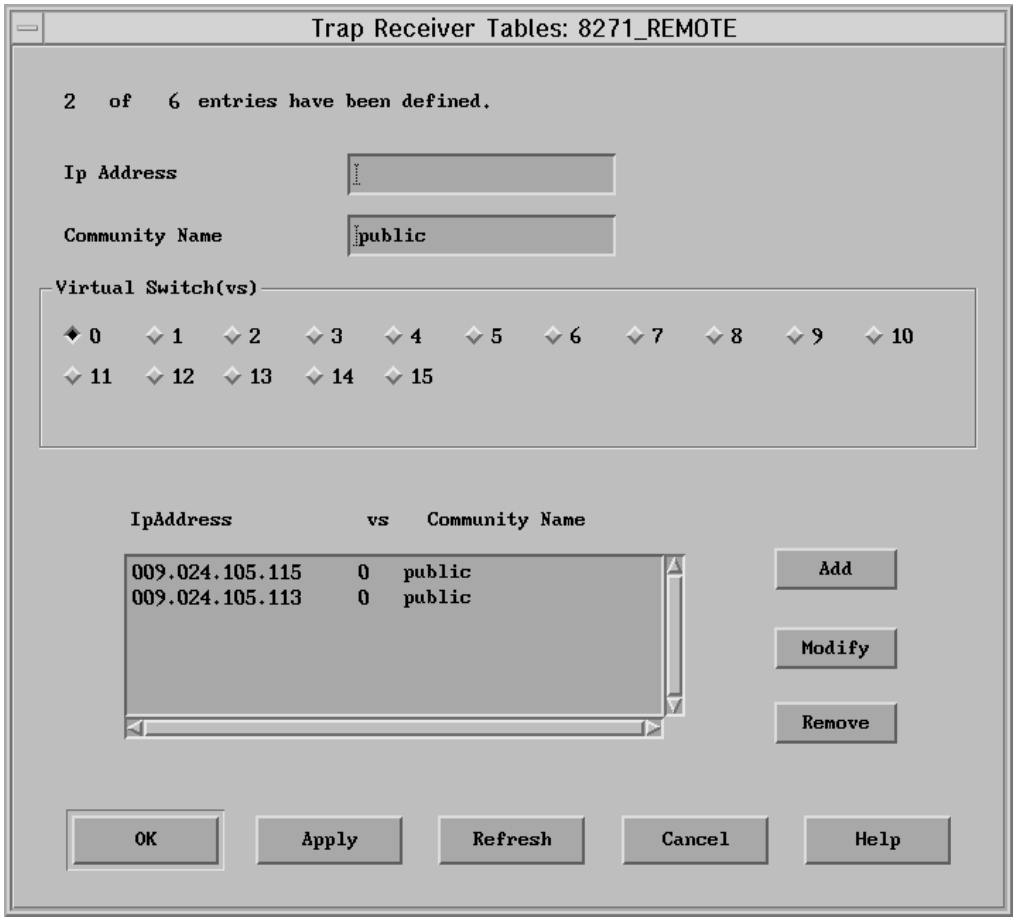


Figure 109. 8271-108 PSM Trap Receiver Table Configuration

We made the required changes to enable traps for Authentication Failure, Link Down and Link Up.

Figure 110 on page 144 shows how the PSM events appear on the NetView events window.

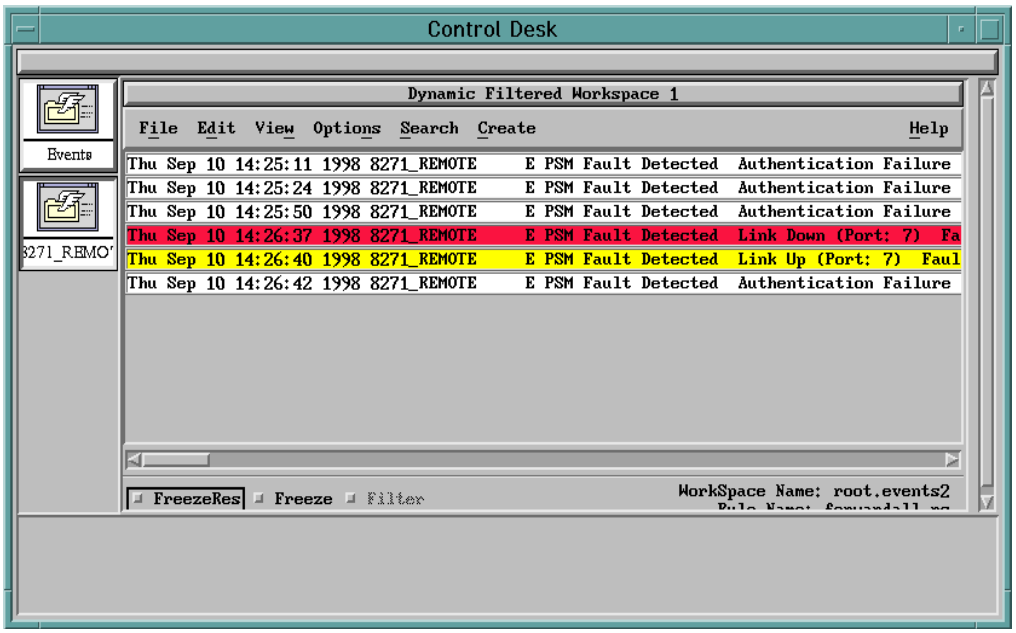


Figure 110. NetView Events Display for 8271-108: 8271_REMOTE

This screen shows a series of Authentication Failure traps, Link Down and Link Up events. The color code of the event depends on the fault level set by PSM trap configuration. A fault level of 4 for the Link Down trap shows up in red.

6.1.3 Using JMAs

Examples of setting up the events using JMA is shown in Figure 111 on page 145. Using the JMA the trap settings are performed using the Fault panel.

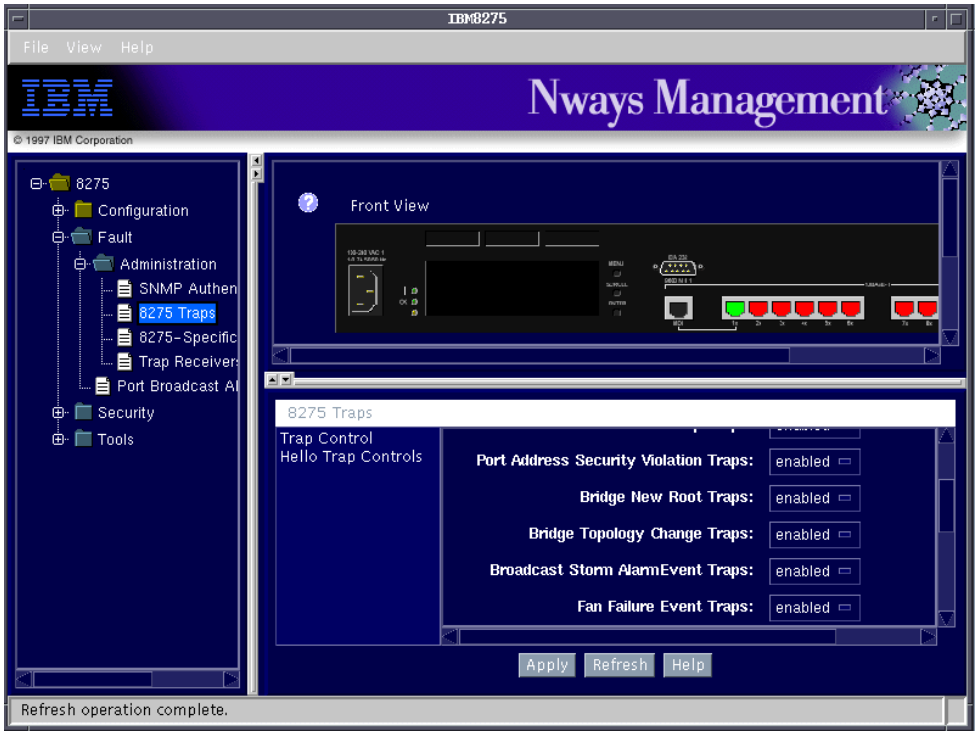


Figure 111. 8275 JMA Showing Fault Control

Select **8275 Traps** from the navigation window, then enable or disable the traps where appropriate. Finally click on the **Apply** button.

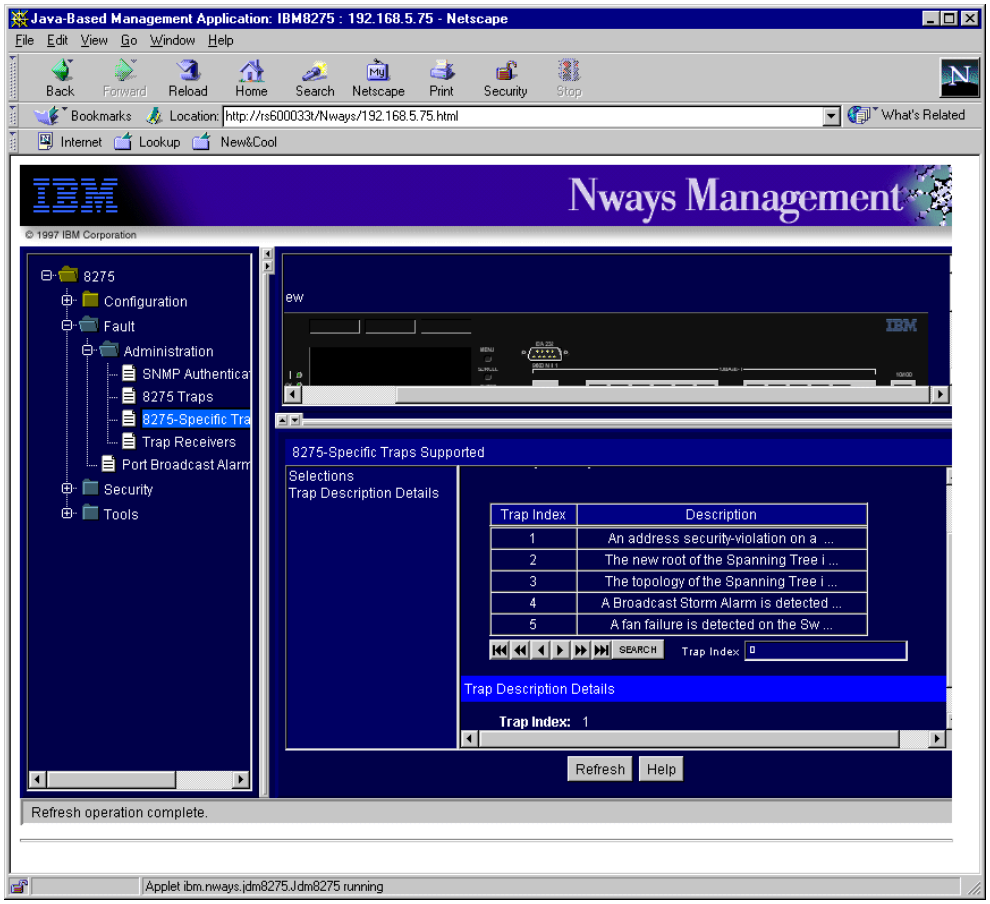


Figure 112. Trap Description

Figure 112 shows the description for each of the trap definitions for the 8275.

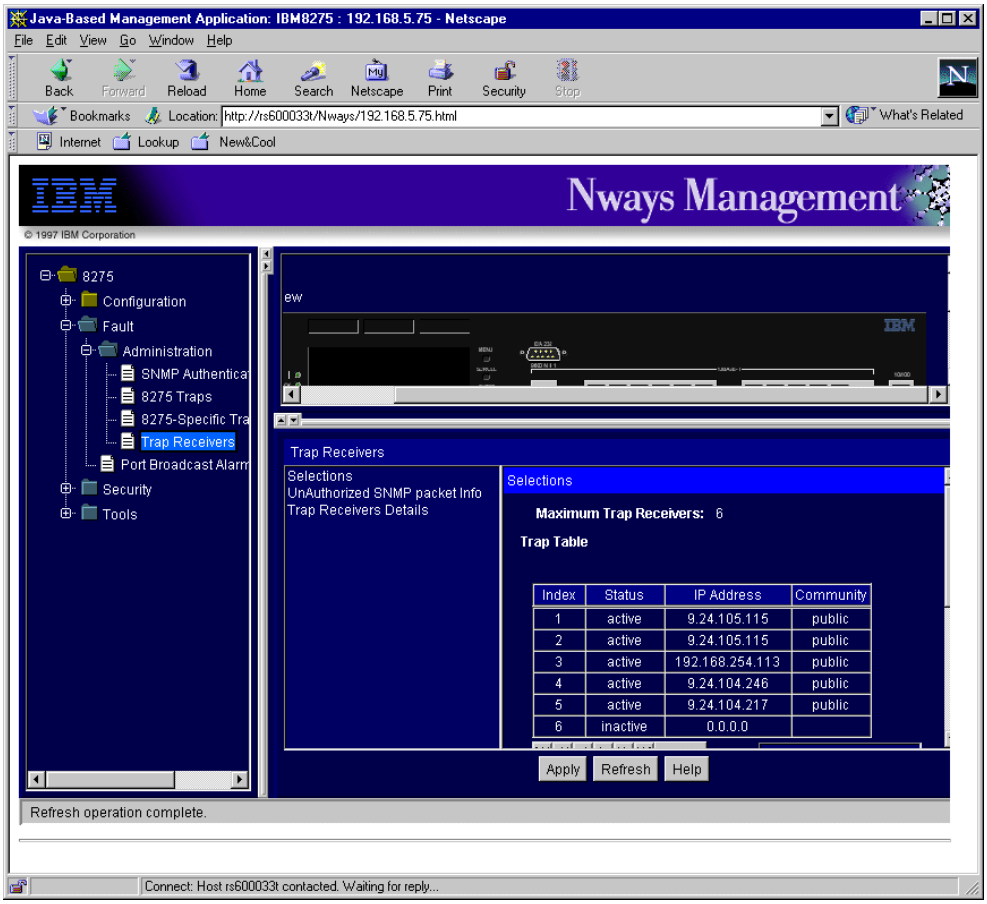


Figure 113. SNMP Trap Receivers

The trap receivers can also be entered and activated.

6.1.4 8260 and CPSW

For the 8260 hub, there is no trap customization available through the hub manager program. Trap settings can only be changed from a console connected to the management module on the hub. Further trap customization is handled by NetView at the management station. However, the 8260 carries blades that are managed by PSMs and JMAs, such as the 8271 and the MSS blades, so traps can be customized on these sub-devices.

To configure the SNMP and trap configuration for the 8260/65 use the commands show community and set alert.

```
8260> set alert change trap display

8260> set alert

Possible completions:
        authentication
        bridge_port
        change
        console_display
        hello
        new-environment
        port_up_down
        script

8260> set alert port_up_down

Possible completions:
        disable
        enable
        filter

8260> set alert port_up_down enable
8260> save all
```

Figure 114. 8260 Trap Settings

Figure 114 shows the commands to set the 8260 and CPSW traps. Here we enabled the port_up_down trap.

6.1.5 IBM 8210 Traps

The base traps for the 8210 are activated using the command set community. We activated the traps as shown in Figure 115 on page 148.

```
MSS1 SNMP Config>list community traps

         Community Name                  Enabled Traps
--------------------------  -------------------------------
private                     None
public                      Cold Restart, Warm Restart,
                            Link Down, Link Up,
                            Authentication Failure,
                            EGP Neighbor Loss, Enterprise Specific
```

Figure 115. 8210 SNMP Base Traps

In addition to the base traps the 8210 allows the ability to send the event logging system(ELS) events from the 8210 to NetView in the form of an SNMP trap.

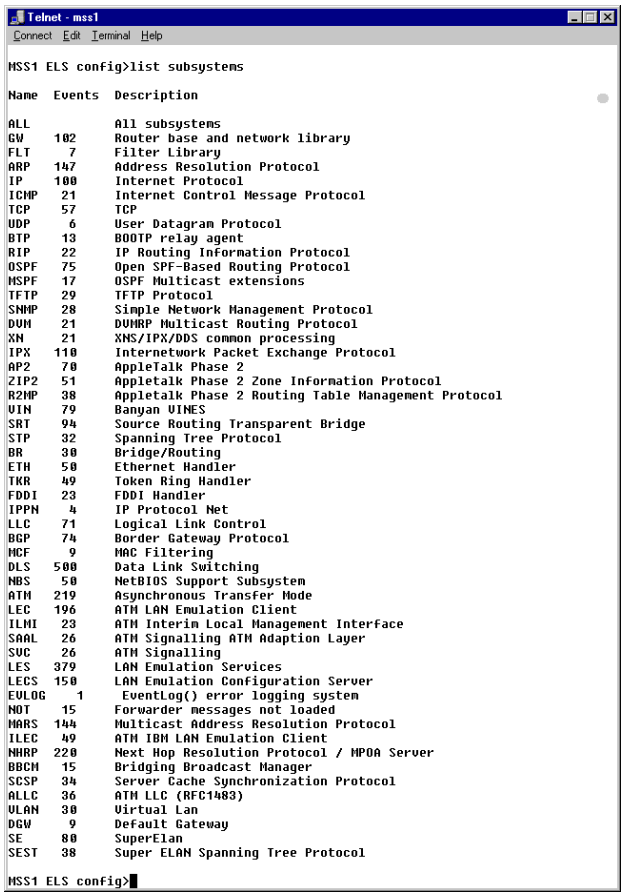


Figure 116. Activating the MSS Events

Figure 116 on page 149 shows the commands to activate these events. These groups can create a large number of events. Although time-consuming, it may be worth identifying individual events to send. This is done by using the talk 5 command `show active events`.

.

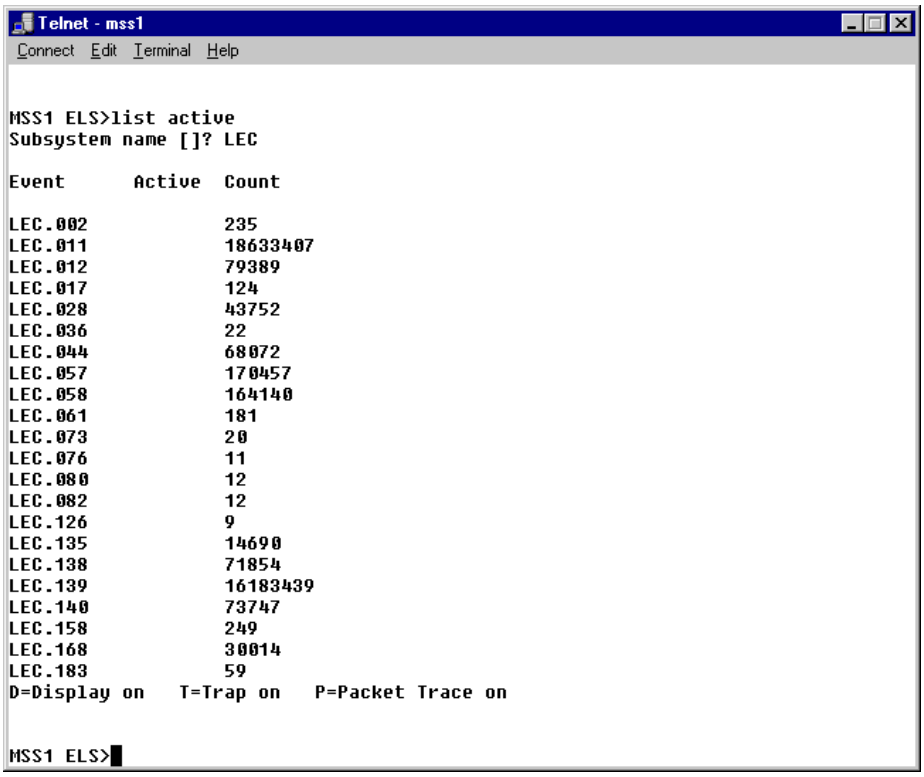


Figure 117. List Active Traps

Also use the command stat to show the current event settings and the number of times this particular event has been generated.

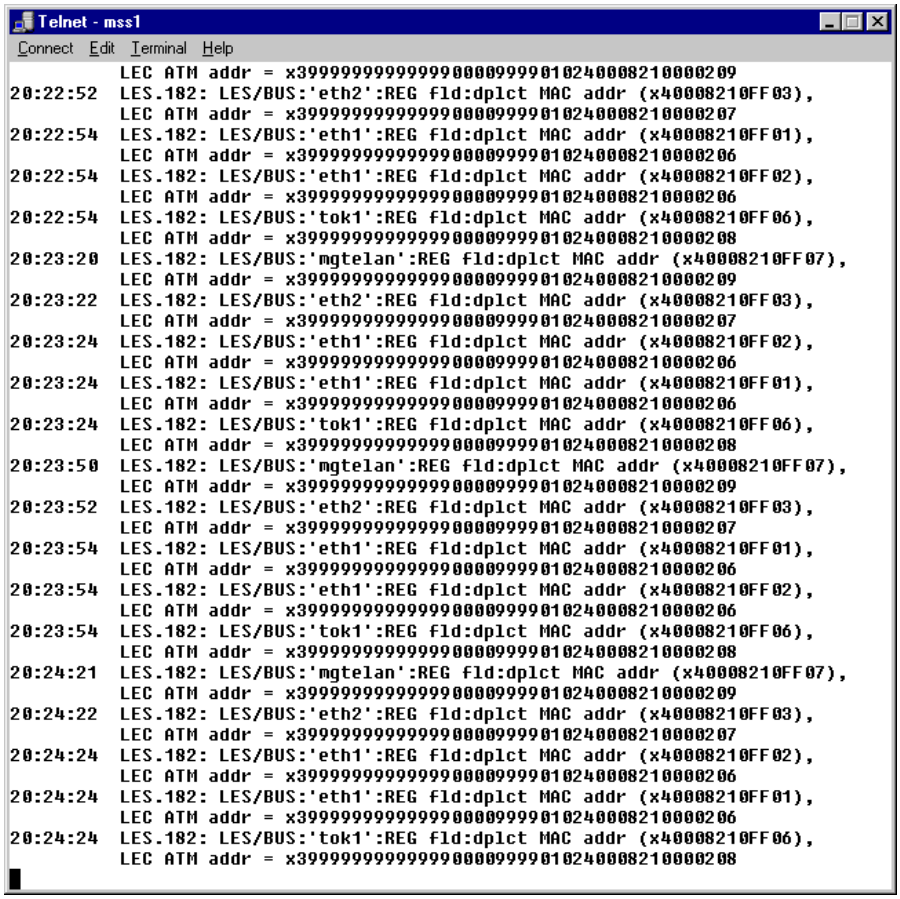


Figure 118. Talk 2 Error Display

Use display subsystem LEC Error, then verify how many events arrive when the display is activated using talk 2.

The trap can be activated using the talk 6 command as follows:

```
trap subsystem lec error
```

The trap will appear in the events window as shown in Figure 119 on page 152.

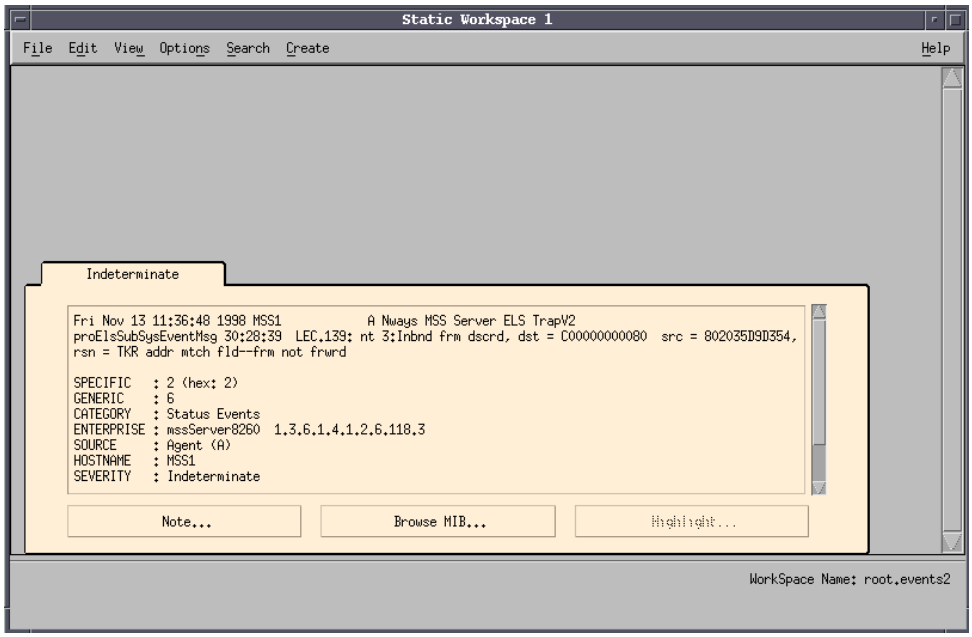


Figure 119. MSS ELS Trap

6.1.6 8273 and 8274 Traps

The 8274 fault settings can be changed using RouteVision. The same applies to the 8273, although the JMA can be used for some of the 8273 events.

6.2 Filtering from NetView

This section shows how we used NetView to filter out the unwanted events that cannot be filtered at the device level. To set the traps to log only in NetView select **Options->Event Configuration->Trap Customization** from the NetView pull-down menu. Figure 120 on page 153 will appear.

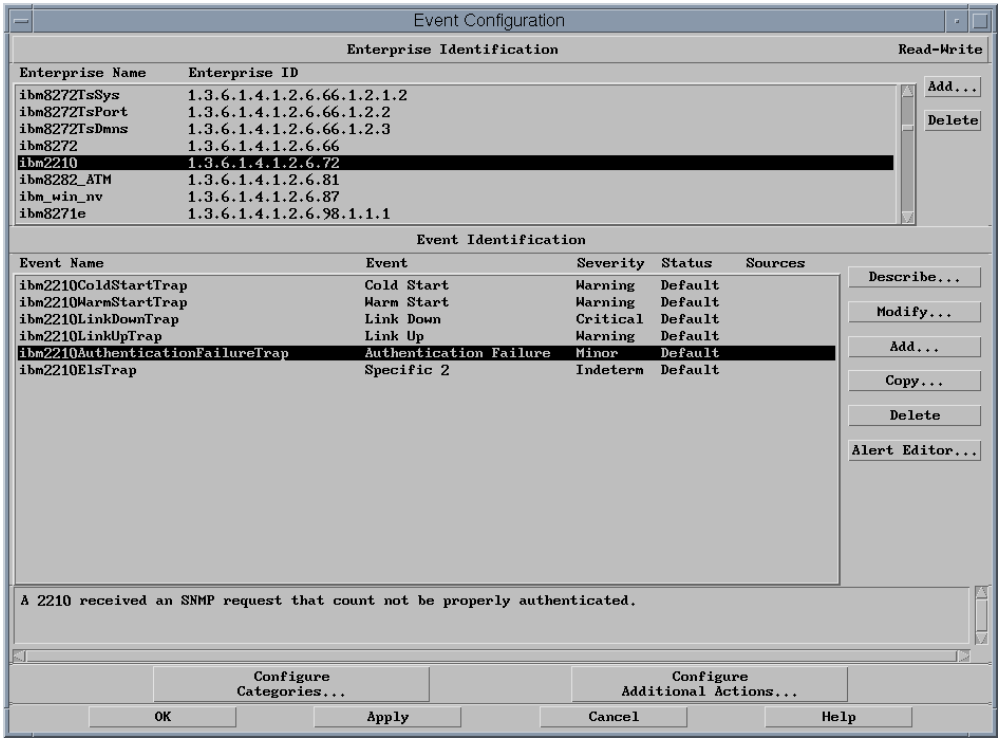


Figure 120. NetView Trap Configuration

For the 2210 we are receiving a number of authentication traps. We decided to filter these as we do not want the operators to see these events. To do this select **Modify**.

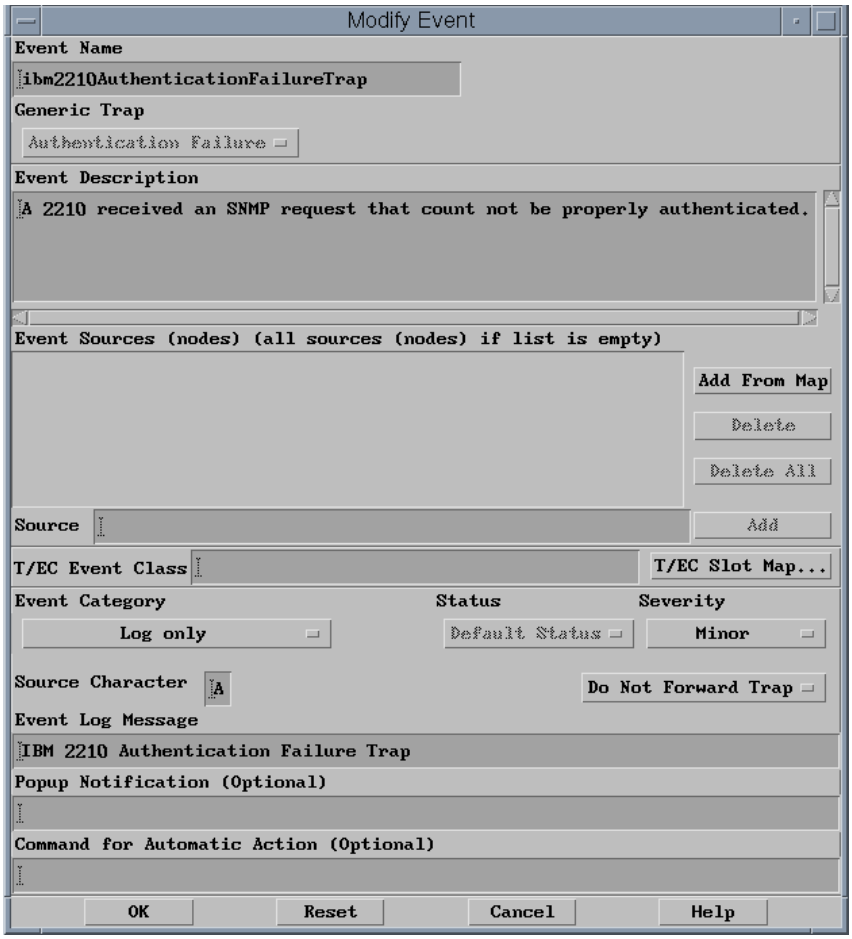


Figure 121. Modify an Event

Change the value for Event Category from Status Event to Log Only. This event will no longer appear in the event window. The next example shows how we defined a filter to show events sent from the 8260 and CPSW only.

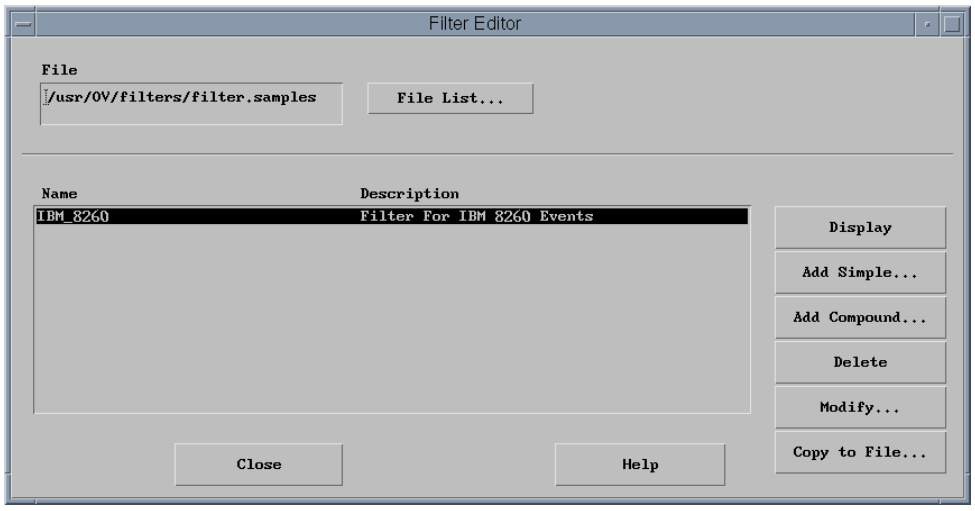


Figure 122. Filter Editor

The filter is initially added using the Add Simple option. Here we show the filter created for the 8260 traps.

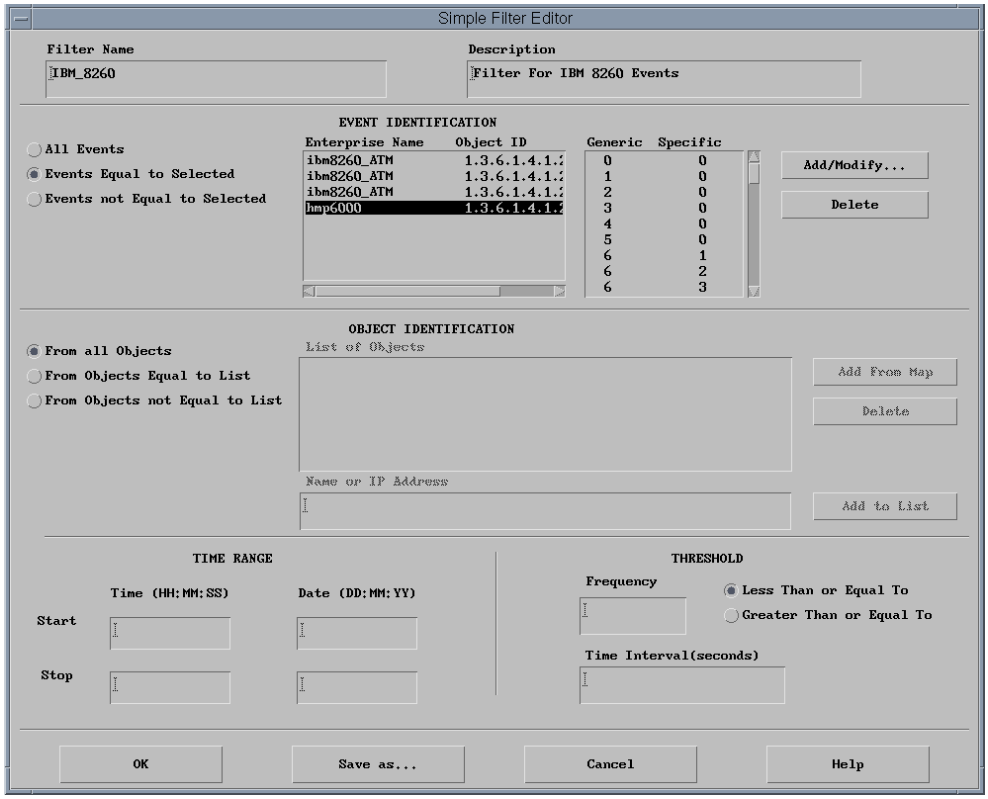


Figure 123. Selecting Events to be Filtered

All the traps not sent from the 8260 will be filtered.

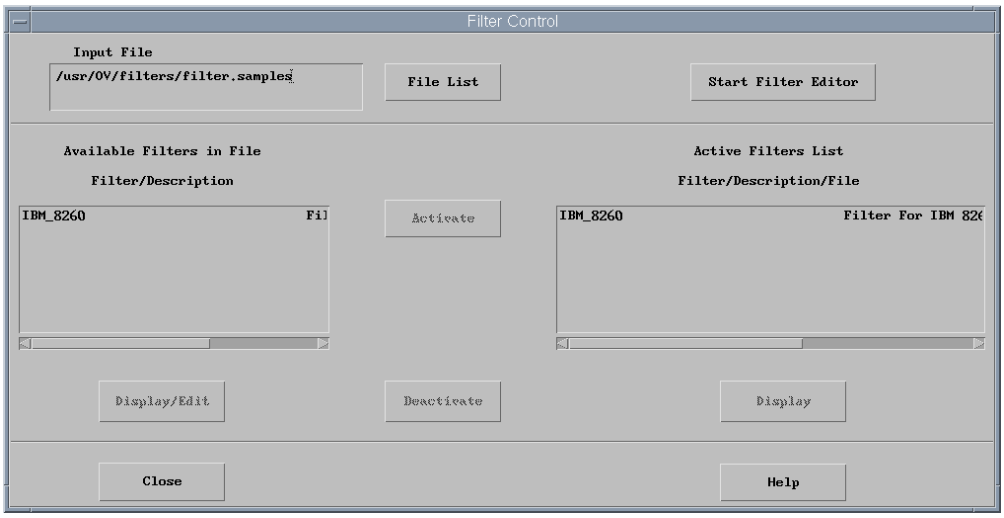


Figure 124. Filter Activation

To activate the filter from the events desk, select the **Activate** button shown in Figure 124.

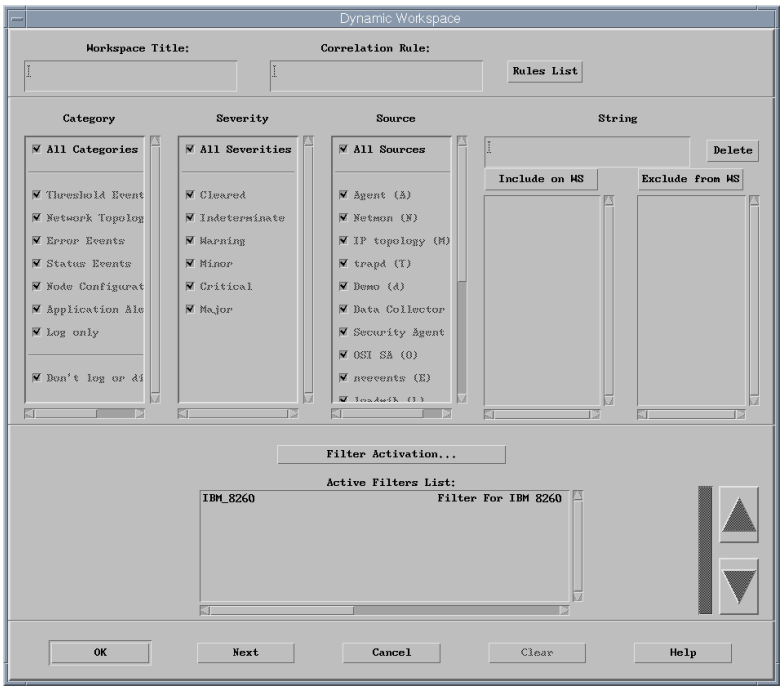


Figure 125. Activating the Filter

Click on **OK** to activate the filter. To activate the filters each time you start NetView select **File->Save as** from the NetView events desk.

6.3 Rulesets

Although we have narrowed down the number of events that will appear in the event window we can perform the following actions to provide a ruleset that will show icons representing the ATM nodes that appear in a collection. These nodes will only appear in the collection if the management station has received a link down event.

The first thing we need to do is add a field to the NetView database that we can change when an event arrives from the ATM nodes.

Using vi, we created a file called atmstat.fields. This file must be located in the directory /usr/OV/fields/C.

```
Field "ATMCRITICAL"  {
Type StringType;
Flags Locate, General;
}
Field "ATMSTATUS" {
Type StringType;
Flags Locate, General
}
```

Figure 126. ATM Critical File

To configure the fields within NetView run the command:

```
ovw -fields
```

We added the ruleset to the ESE.automatic file. This is done so the ruleset will be active at all times. Next we need to set the ATMSTATUS field to ON for all our nodes nominated as critical. This is done so that the ruleset will only be active for events sent from the selected nodes and not all nodes that are managed by NetView.

For this we used the NetView command nvdbimport. First using vi we created a file shown in Figure 127 on page 157.

```
IP Hostname, ATMSTATUS,ATMCRITICAL
IBM8285,ON,FALSE
CPSW1,ON,FALSE
CPSW2,ON
MSS1,ON
MSS2,ON
IBM8274,ON
```

Figure 127. ATM.import file

The command to set the fields is nvdbimport -f ATM.import.

The new NetView fields will now have the new fields set. To verify this we ran the command ovobjprint -s IBM8285 | grep ATM.

Next we need to define the NetView ruleset.

6.3.1 Creating the Ruleset

The ruleset will listen for events for the switch that are either link up or link down. When we receive these events the ruleset will first check that the device has the ATM_STATUS field set to ON. If this is set, the field ATM_CRITICAL will be set to TRUE for a link down. This will then activate the collection to show this node. When a link done trap arrives the ATM_CRITICAL status will be set to FALSE. This will remove the node from the collection.

From the NetView main screen select **Tools->Ruleset Editor.**

NetView rulesets are covered in the redbook *Integration Examples Using NetView 5.1*, SG24-5285. We show the settings for each of the templates. However each new node is created using the new pull-down menu. The main ruleset window is shown in Figure 128 on page 158.

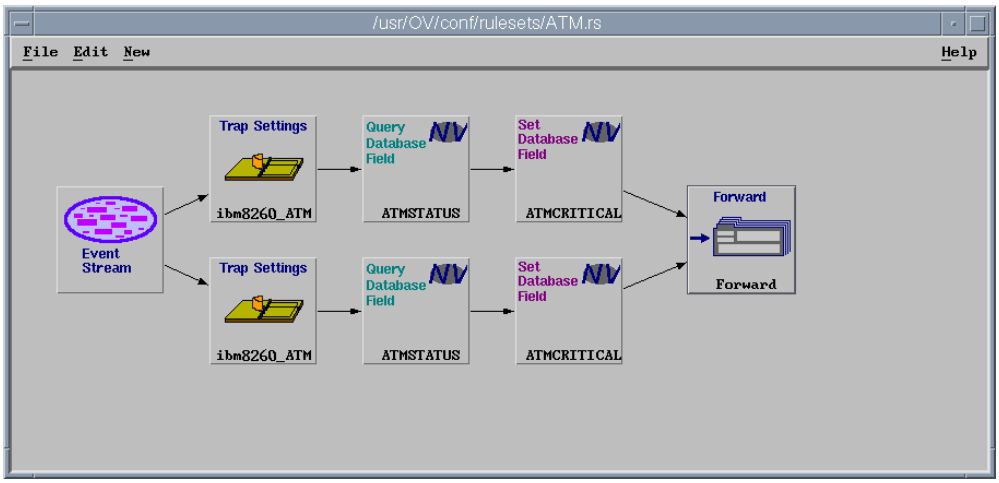


Figure 128. Ruleset Template Window

The trap settings, accessed by double-clicking on the Trap template, shown in Figure 129 on page 158.

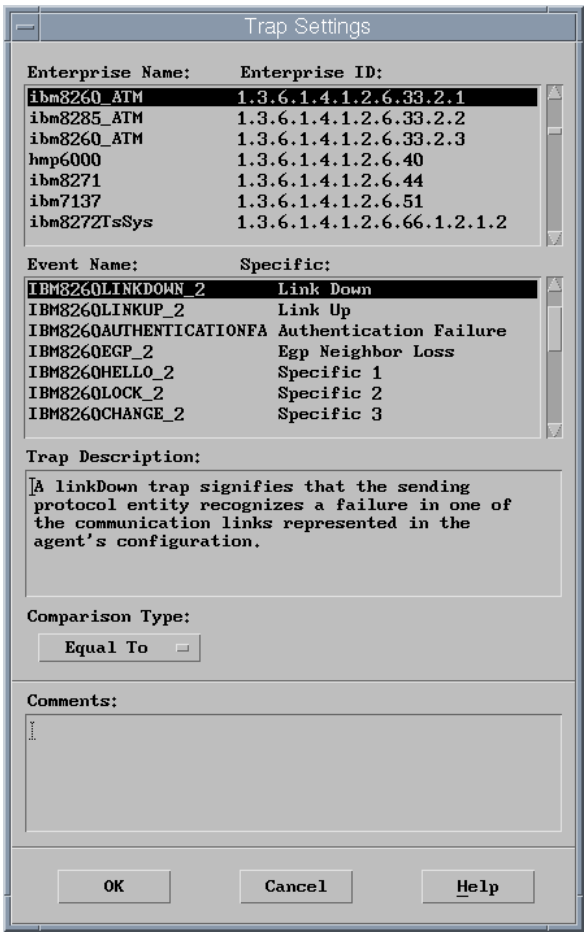


Figure 129. Trap Settings

Here we defined the 8260 traps that we considered critical. If one of these traps is sent, we have to check if the node is one of the nodes we assigned as STATUS. To query the Database field we have to create a template as shown in Figure 130 on page 159.

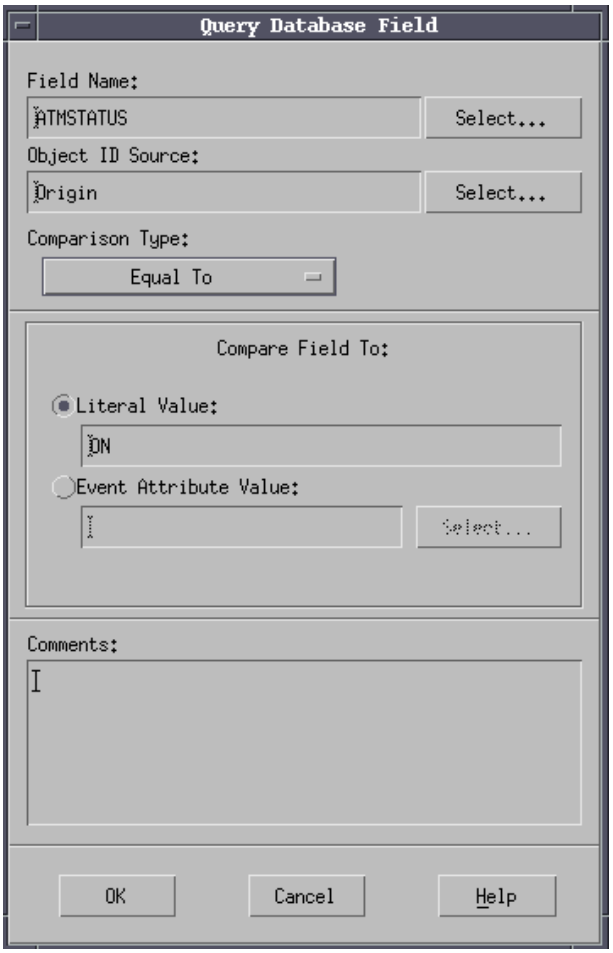


Figure 130. Query the Database

If this criteria is met the next action is to change the value of the field ATMSTATUS. The following screen shows the parameters required to set the NetView object field to ON.

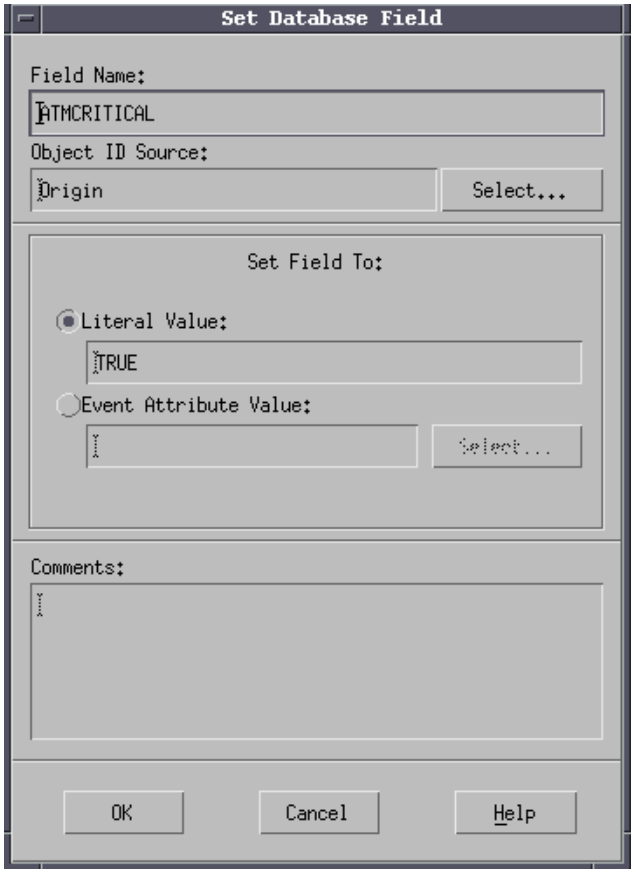


Figure 131. Set the Database

Next we add our new collection that will show only our nodes that we have assigned as critical and that have an error.

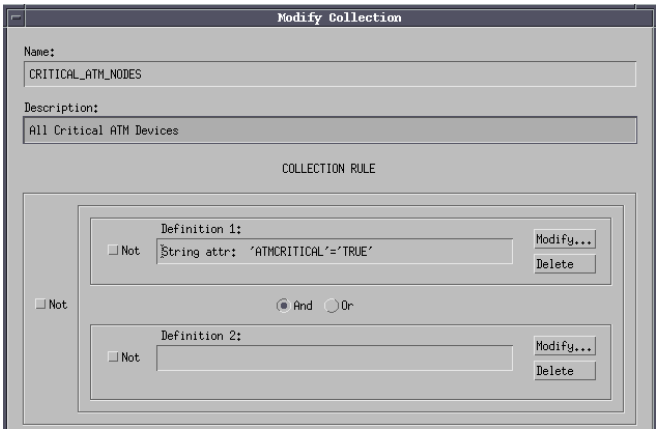


Figure 132. Modify the Collection

The collection settings are defined with the name set to ATMCRITICAL and the field set to ATMCRITICAL.

To activate the ruleset use **Create Dynamic Workspace** from the events window and enter the ruleset name in the Rules List field.

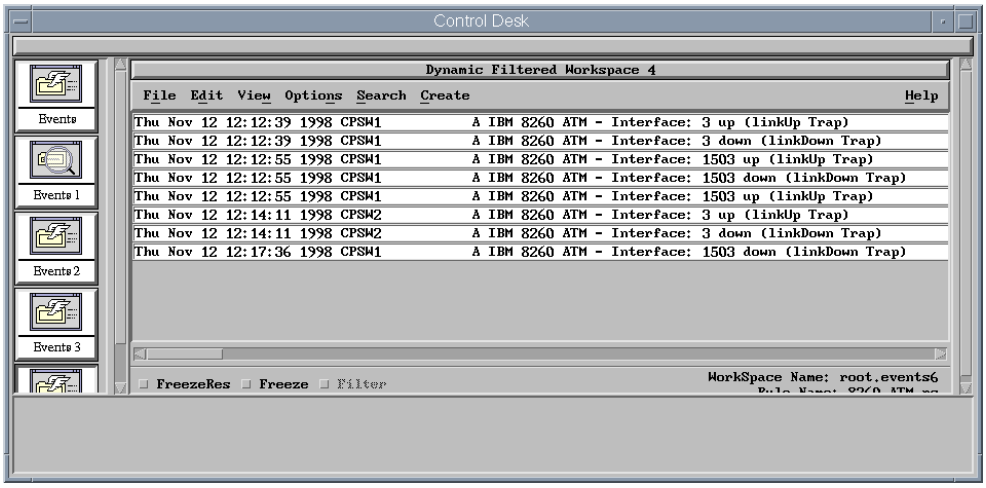


Figure 133. Ruleset Events Window

The events that will appear are based on the rules as shown in Figure 133 on page 161. The collection is populated when an event arrives as shown in Figure 134 on page 161.

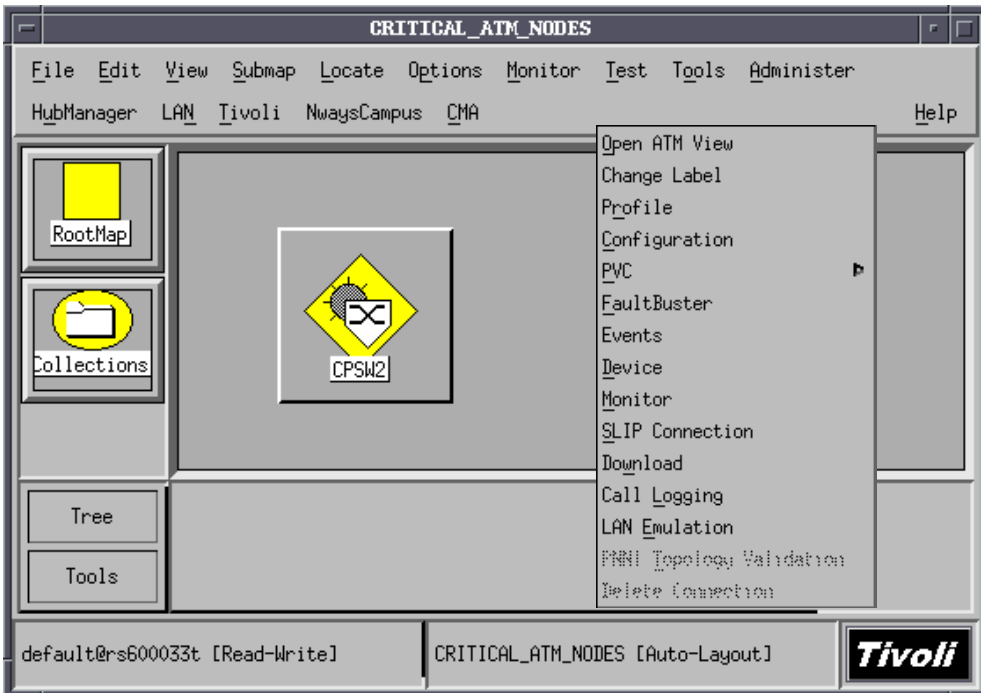


Figure 134. Node in CRITICAL_ATM_NODES Collection

The result is that when an event of the type Node Down for the CPSW arrives the icon appears in the CRITICAL_ATM_NODES collection.

6.3.2 Event Correlation

Extending the example even further, when the Link Up event is received by the events desk, then the Link Down event will be removed from the display. This is achieved by simply adding a new template to the existing rulebase.

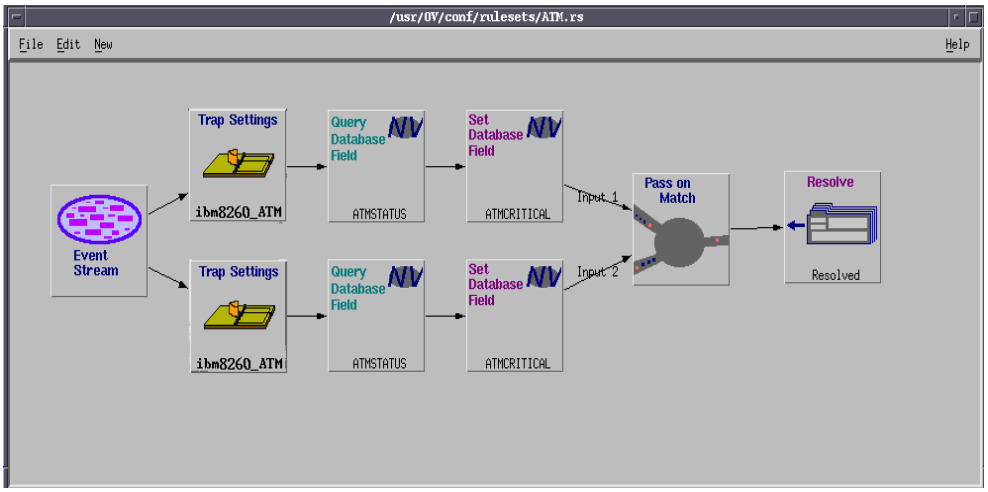


Figure 135. Further Event Correlation

The new template is called Pass On Match.

6.4 Performance Management

This section deals with performance monitoring of our network components and how to access these performance tools. The applications we show are as follows:

- SNMP Bridge Manager
- ATM Manager
- MSS Web Interface
- Remote Monitor
- Traffic Monitor
- Device Managers

The JPM is covered in Chapter 7, “Nways Java/Web Management Applications” on page 211.

6.4.1 PSM Performance Options

The PSM-based performance options can be launched by selecting from the pull-down menu of the PSMs **Management --> Performance --> Performance Options.**

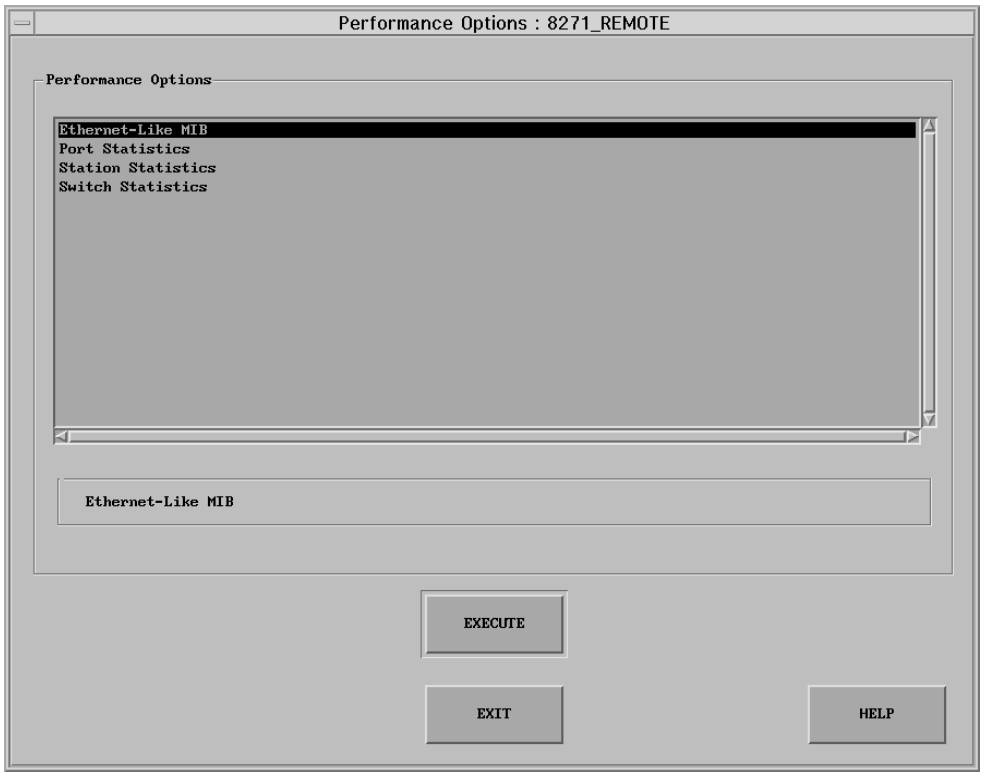


Figure 136. IBM 8271-108 Performance Options

Here we show you each of the performance options available and briefly explain what information they provide.

6.4.1.1 Ethernet-like MIB Statistics

These are the error statistics available for almost any type of standard Ethernet Interface as per RFC 1643. For an 8271 switch the interfaces are the ports on the switch. There are error statistics for each port on the switch

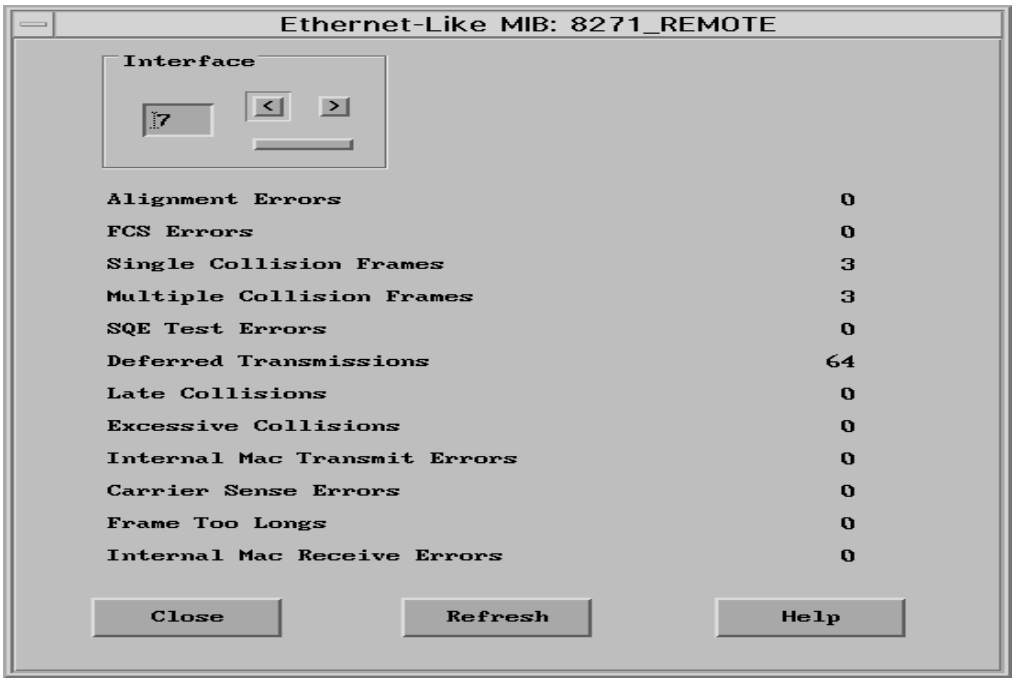


Figure 137. 8271-108 Ethernet-like MIB Statistics for Port 7

The statistics for port 7 of the 8271-108 switch are shown in Figure 137. You may switch to the statistics of a different switch port by using the left and right arrows. Also the statistics can be refreshed using the **Refresh** button.

As the port on the switch can be connected to a dedicated workstation, a shared hub, or another switch, the origin of the errors may also be any of the above mentioned. But the fact that the errors point to a specific port, gives the network troubleshooter, a reasonably narrowed down problem area to investigate.

6.4.1.2 Ports Statistics

The Ports Statistics panel provides statistics at a port level. Using the left and right arrow buttons you can switch to view the statistics of other ports.

The statistics are categorized into the following groups:

Receive Counters The frames/packets received by the switch

Transmit Counters The frames/packets transmitted by the switch

Error Counters Errors in frames detected by the switch

Station Counters Stations in terms of MAC addresses

Overflow Conditions Used for buffers or address tables

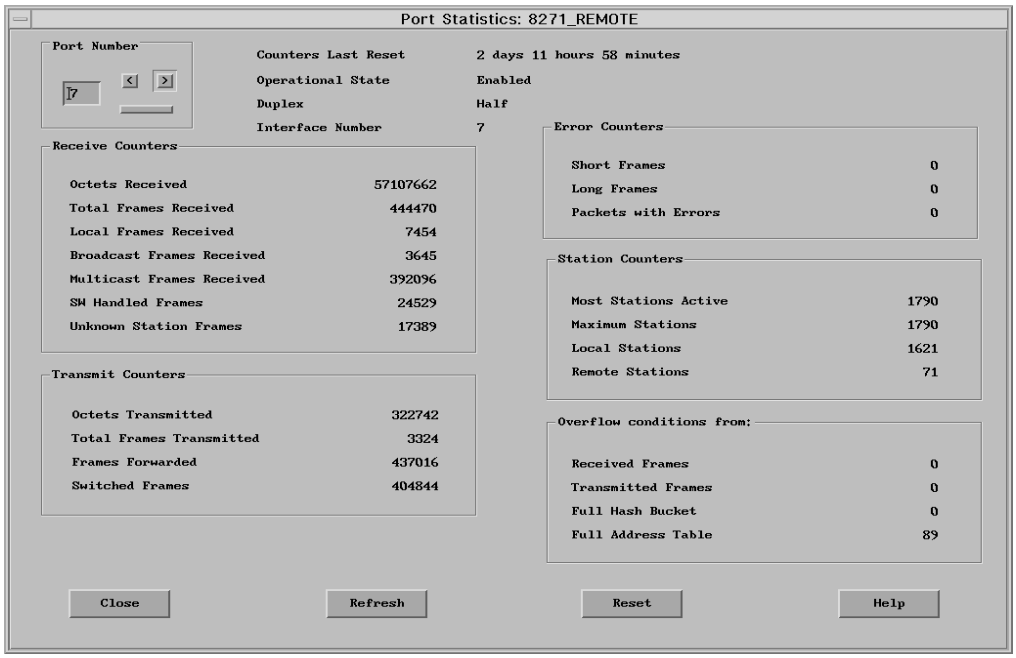


Figure 138. 8271-108 Port Level Statistics

Port 7 of the 8271-108 is shown in Figure 138. To generate traffic we connected the port on the switch to a large bridged Ethernet network.

6.4.1.3 Station Statistics

The port statistics cover statistics at a port level. A port can typically accommodate multiple stations. The station statistics provide data by breaking down the port into stations, then depicting the traffic flowing to and from a station.

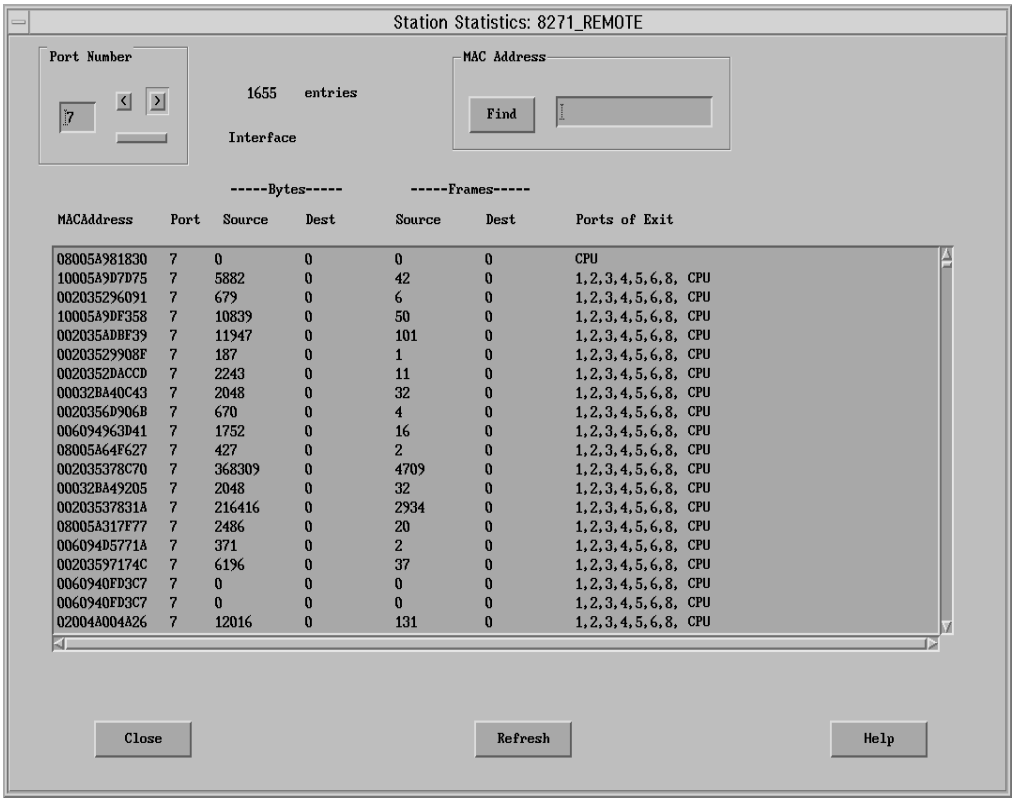


Figure 139. 8271-108 Switch: Station Level Statistics

The MAC address is the layer 2 address of the station.The port designates the port where the station resides. The source is when stations send frames and the MAC address of the station is in the SOURCE ADDRESS field of the frame. The Dest is when the station is the destination of a frame where the MAC address of the station is in the DESTINATION ADDRESS field of the frame. The Ports of Exit are all the ports to which the station has sent frames.

Again from a design and monitoring perspective, this is a basic tool to see how much traffic a station is transmitting and receiving.

6.4.1.4 Switch Statistics

The Switch Statistics window shows the overall statistics at a switch level.

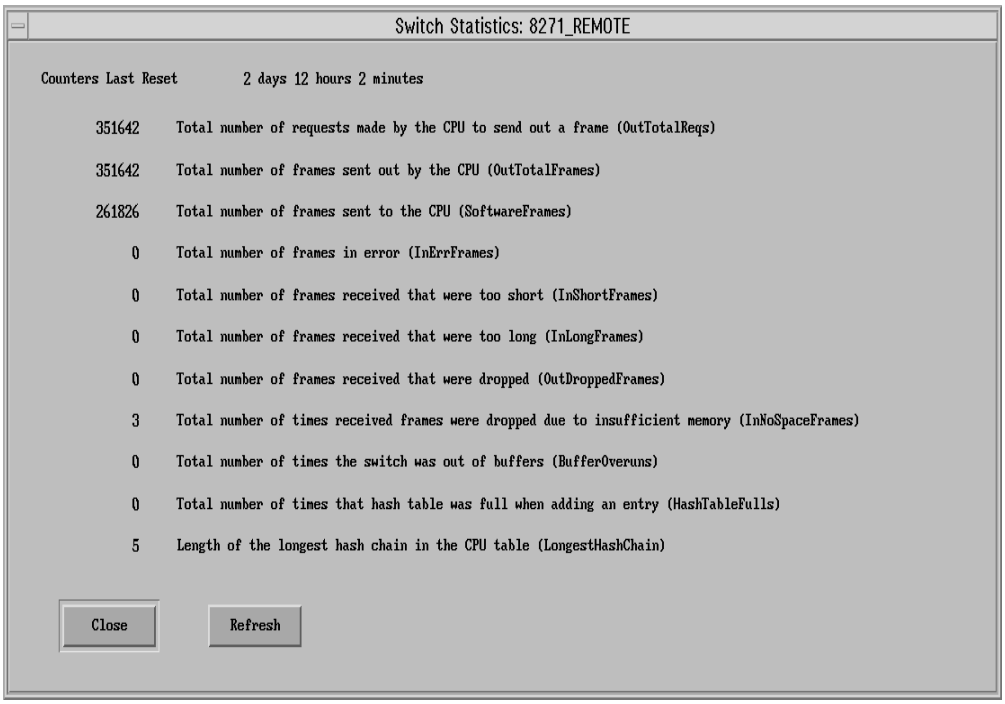


Figure 140. 8271-108 Switch Level Statistics

This can be used as an overall summary of the frames sent and received by the switch.

6.4.2 ATM Performance

ATM information can be viewed using the ATM performance application. From the ATM submap we selected the CPSW device. From the pull-down menu we chose **CMA->Monitor** (see Figure 141).

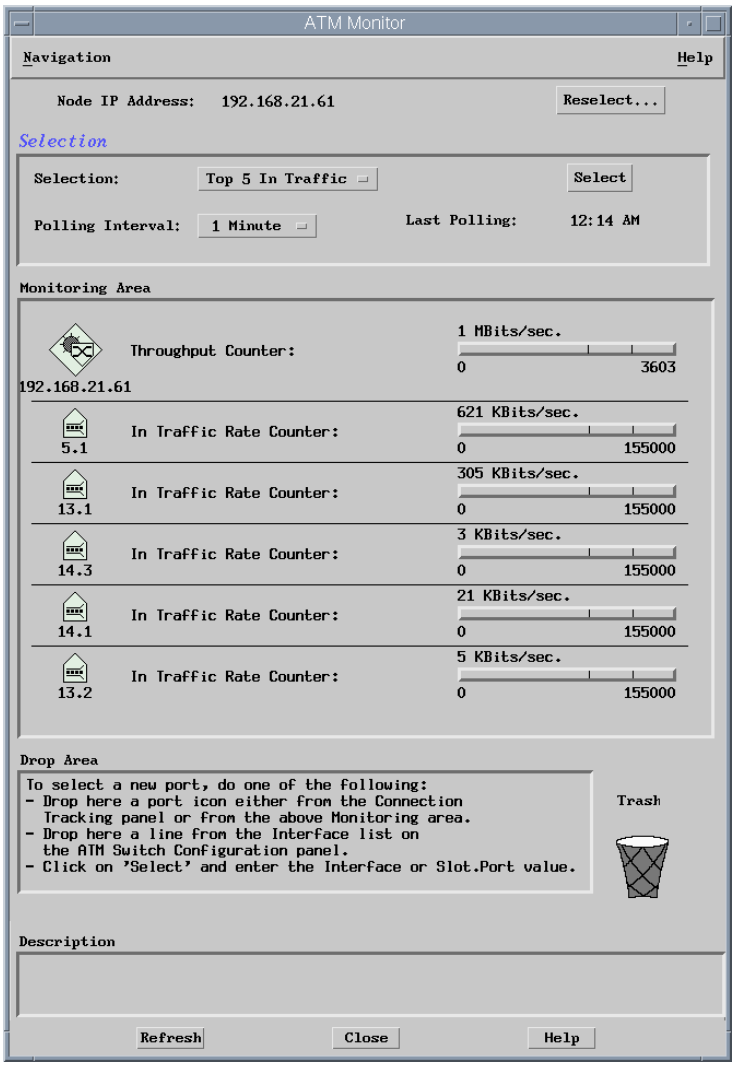


Figure 141. ATM Statistics

The information displayed shows the ATM port statistics ordered by the amount of traffic in and out of the port. The polling options can be modified using the **Polling Interval** button.

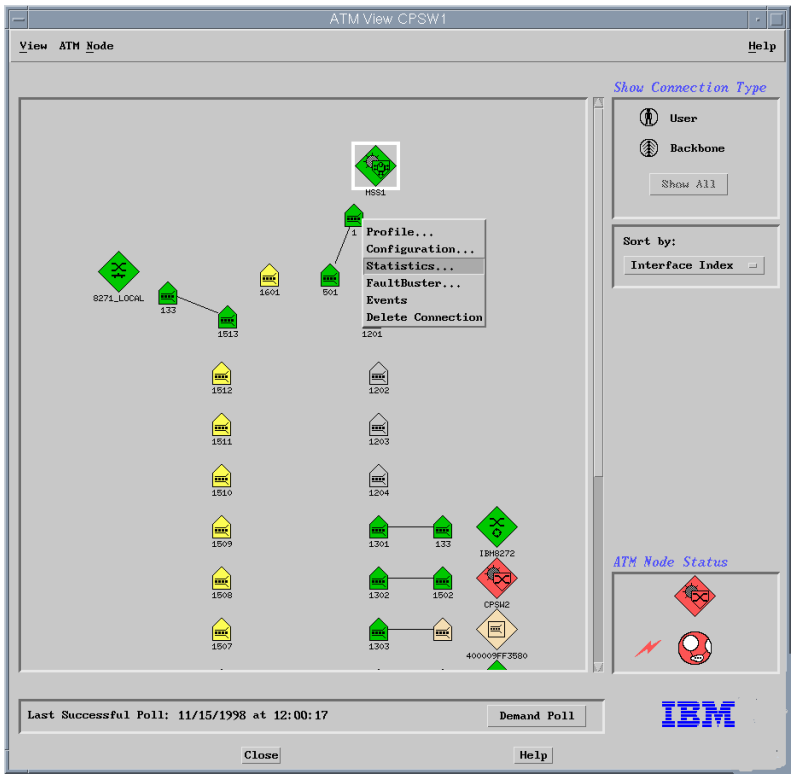


Figure 142. ATM Statistics

We can select the performance application from the ATM screen by selecting the node with the right-hand mouse button then selecting **Statistics** (see Figure 143 on page 170).

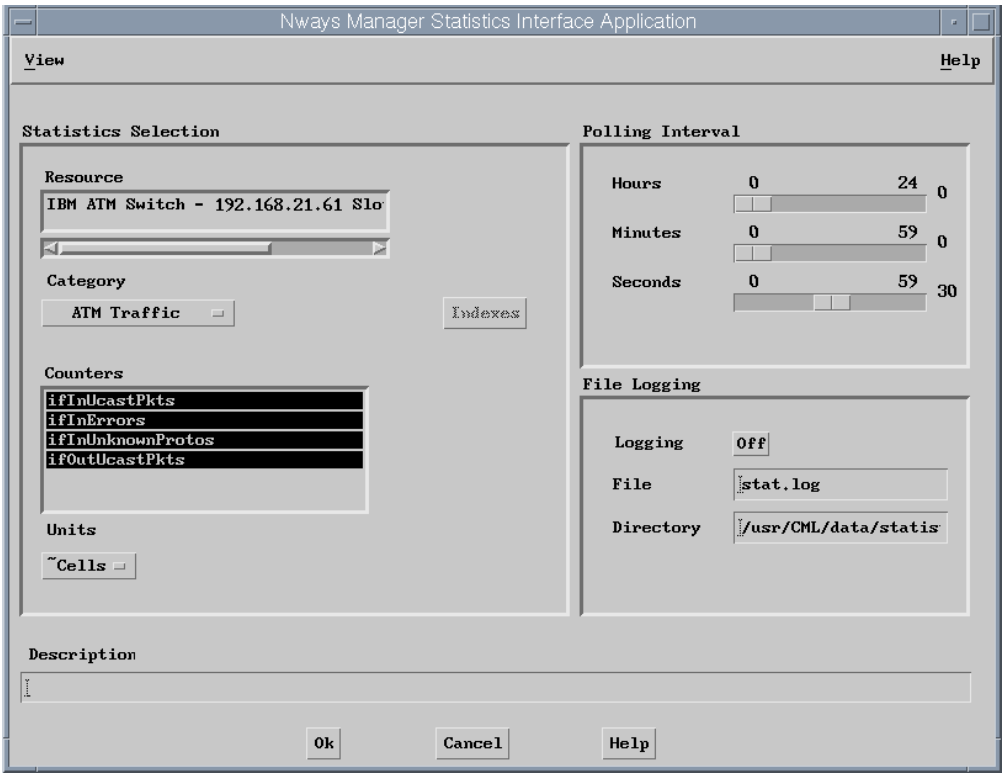


Figure 143. Nways Statistics

Select the data you want to graph by highlighting the options listed in the Counters window, then click on **OK** to start displaying the performance data, (see Figure 144 on page 170).

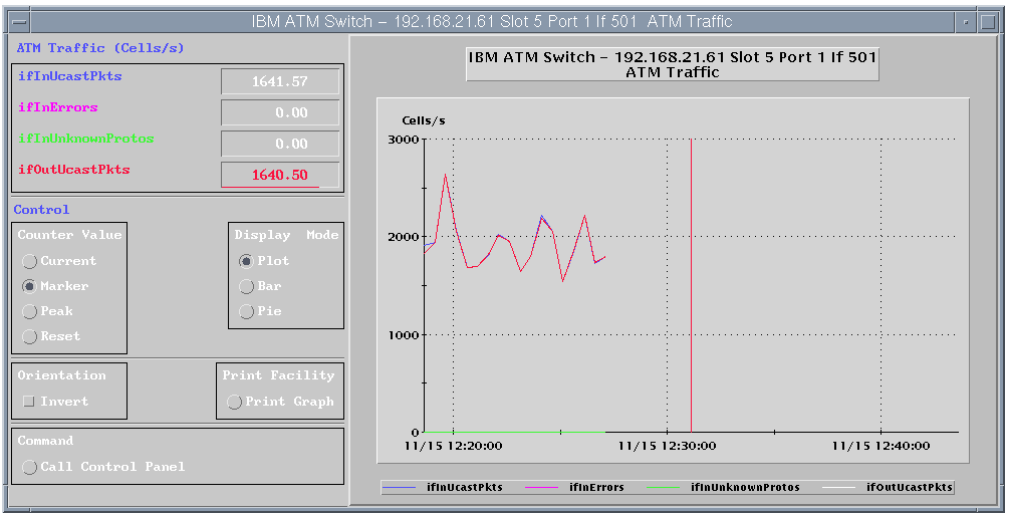


Figure 144. ATM Performance

LAN Emulation statistics can also be seen using this graphing tool. From the LAN Emulation configuration screen select the **LES/BUS**. Next click on **Configuration**.

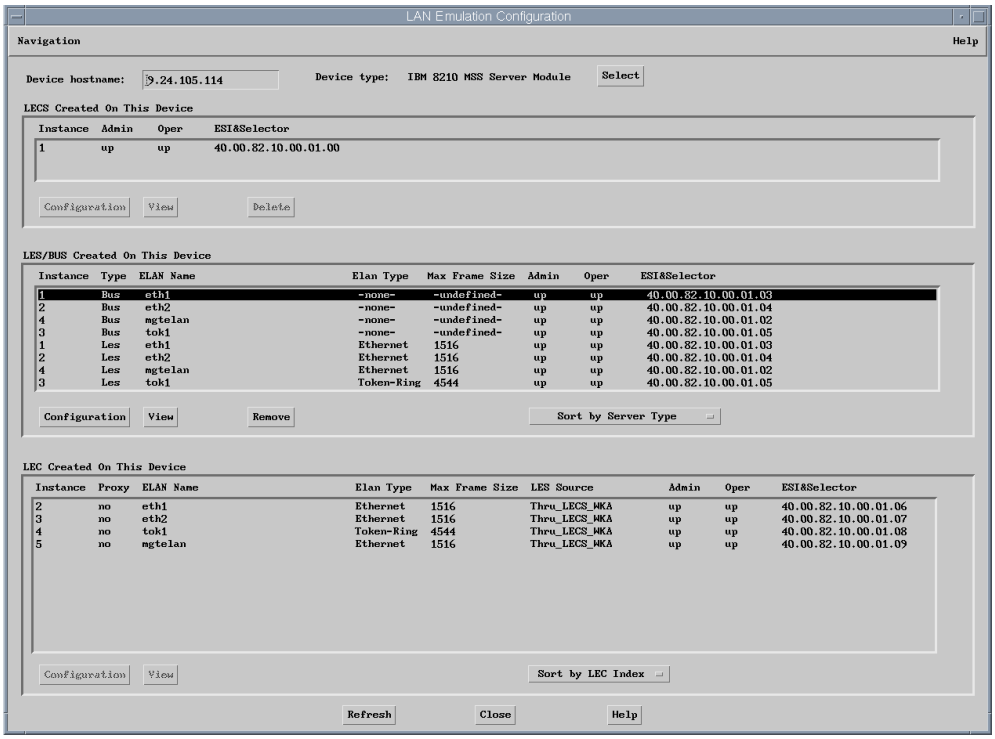


Figure 145. Choosing the LEC

From the pull-down menu select **Navigation** followed by **Statistics**.

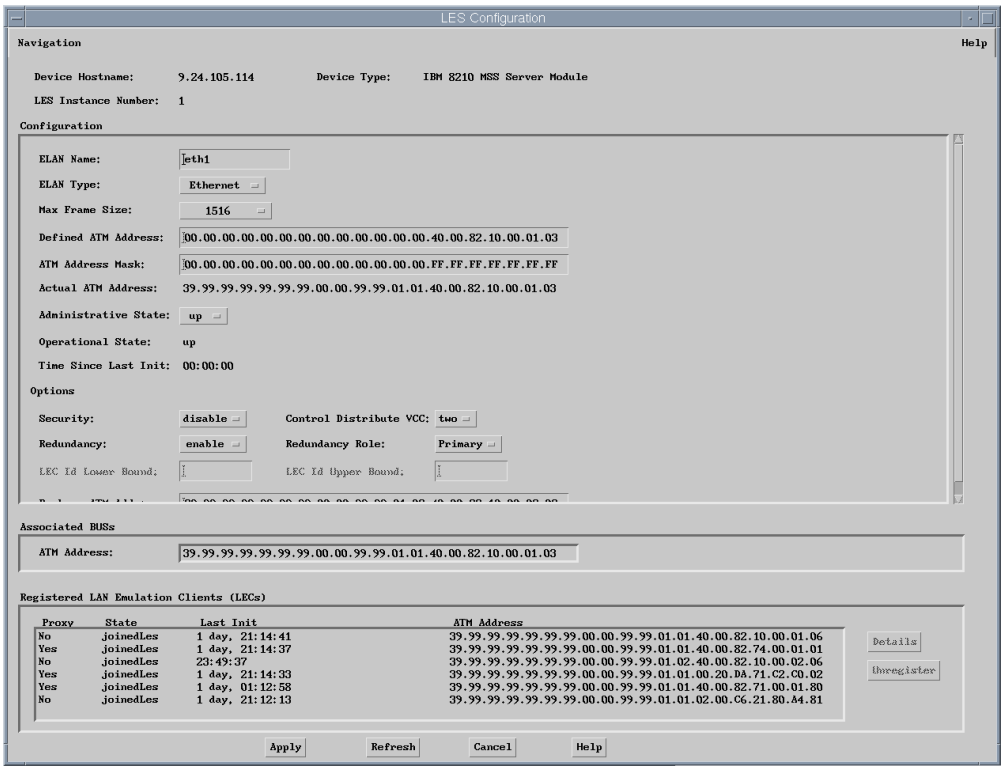


Figure 146. Selecting the Graphing Tool

The category is set to LES the monitor options can be selected in the Counters window.

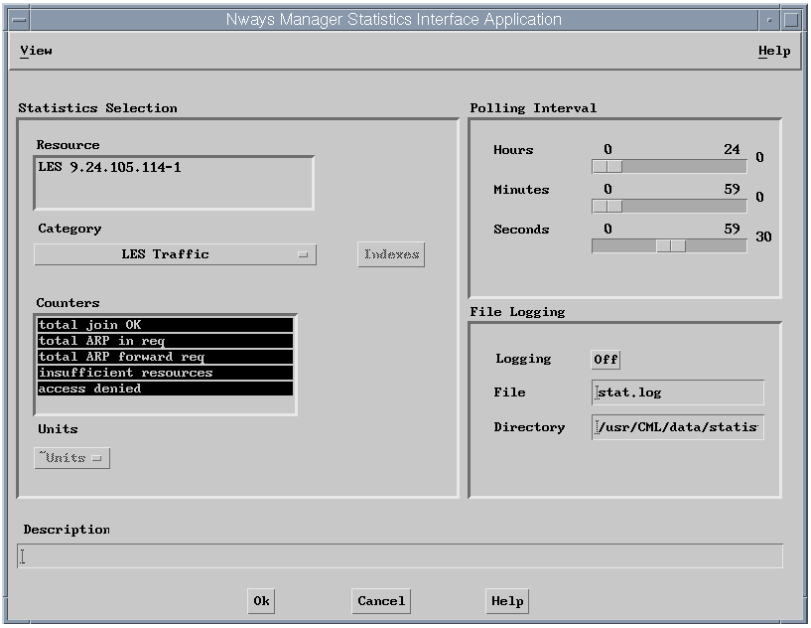


Figure 147. Graphing LES Traffic

Select **OK** to show the graph.

6.5 Remote Monitor for AIX

In this section we cover the Nways Remote Monitor product. Here we explain the detailed functionality of Nways RMON products using example scenarios for some of the IBM networking equipment that have RMON agents built-in.

We show examples of both RMON and RMON2 probes. The only networking device from IBM at the time of writing this book that has standard RMON2 capability is the IBM 8239 Stackable token-ring Hub. Of course, the HE-MAC, HT-MAC daughter cards, and 8250 Ethernet probe can support Enterprise Communications Analysis Module (ECAM) functions. ECAM is IBM's pre-cursor to RMON2 and uses a proprietary MIB structure.

Remote Monitor is packaged as part of Nways Manager for AIX, but does have the capability to run as a stand-alone product. It has no obvious dependencies on NetView or any of the Nways management products. Remote Monitor communicates directly with the RMON and ECAM/RMON2 agents in the devices and builds its own polling lists and user interface, plus maintains its own data collection directories and files. However, Remote Monitor can be fully integrated into the Nways management environment, so that it can be launched from a map view, PSM or JMA.

To launch the Remote Monitor from NetView, select **Monitor->Nways Manager-Remote Monitor.**

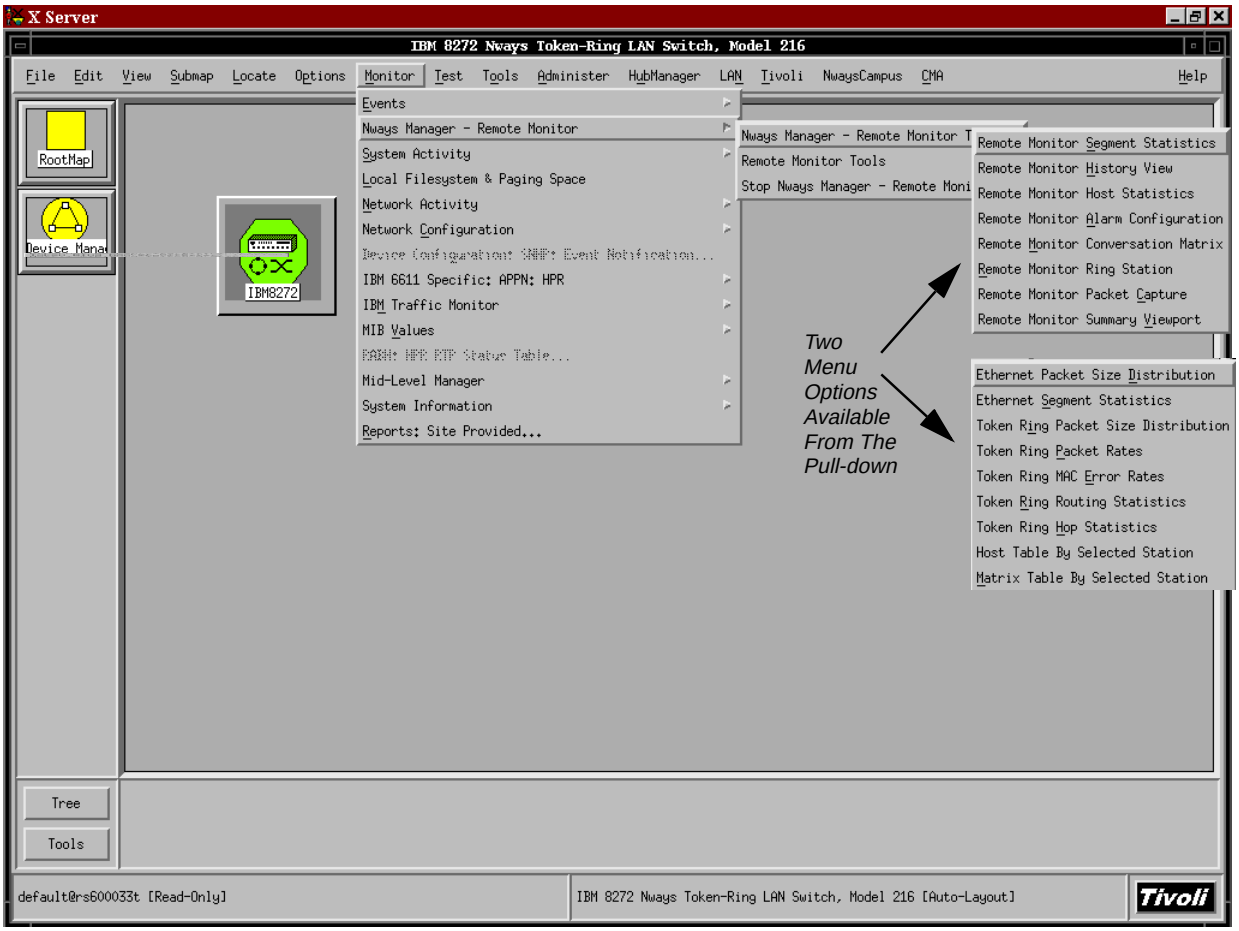


Figure 148. LANReMon Launch from Nways Desktop

The two menu pull-downs open Remote Monitor in different ways. The difference being the options for specific monitoring views of the device traffic. If no device has been selected on the map, then you must choose the submenu from the **Nways Manager - Remote Monitor Tools** item. This item opens Remote Monitor with no device selected but will prompt for a device from a list of discovered devices with RMON probes (see Figure 149).

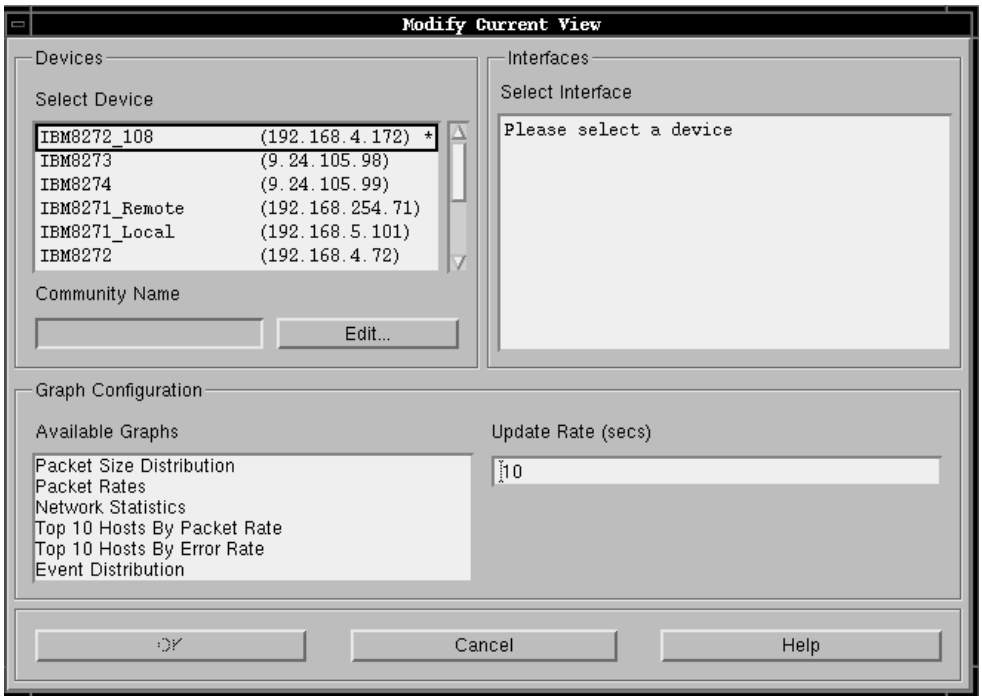


Figure 149. Remote Monitor Panels

Choosing another item from the same pull-down, such as Remote Monitor Host Statistics will open only the device selection panel and not the summary view.

Remote Monitor can be started from a PSM, the easiest method being to click on a port with the right-hand mouse button. This opens a context menu with the available Remote Monitor views for that device. Selecting any of these items will open Remote Monitor.

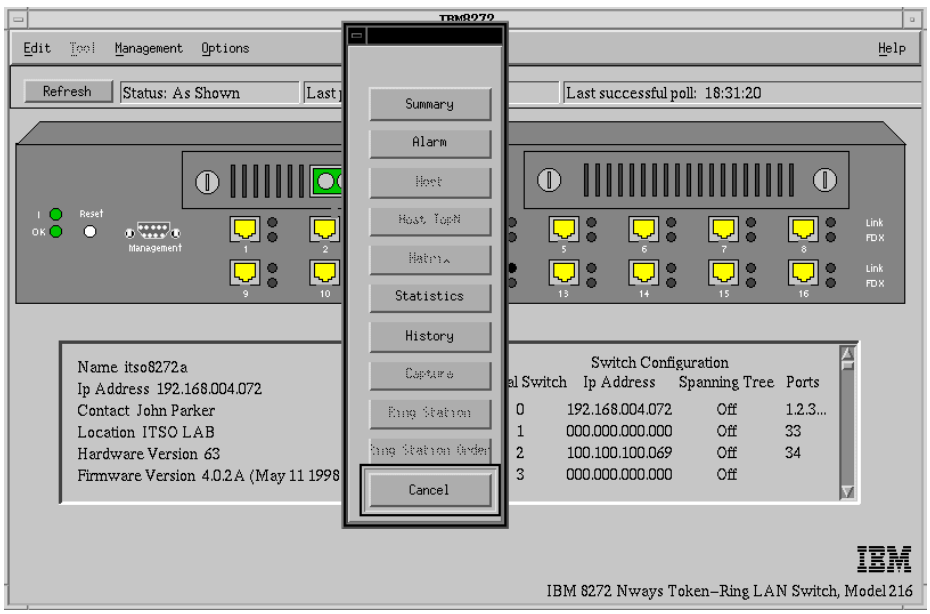


Figure 150. Remote Monitor Access from a PSM

When Statistics is selected Figure 151 is shown.

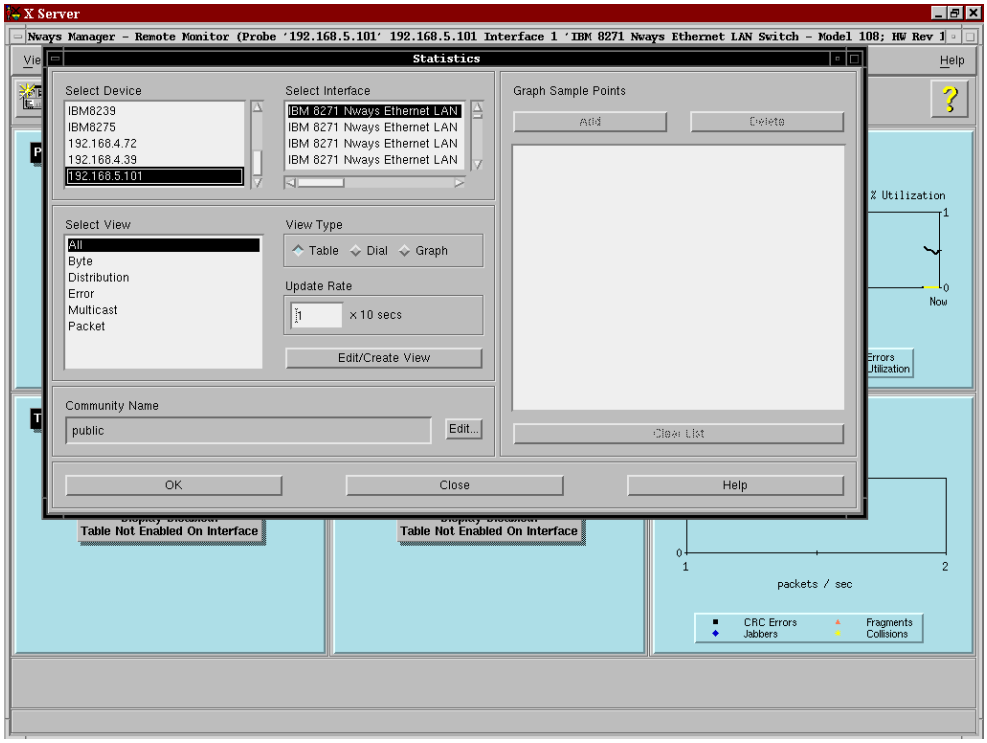


Figure 151. Result of Selecting Statistics Option from PSM

From a JMA, the user can also launch Remote Monitor. From the JMA tree structure on the left of the panel there is an item for Remote Monitor under Services. There is also an Rmon Management button where the JMA can be used to change some of the RMON probe attributes in the device.

The options are displayed in the RMON management window. The options can be enabled and disabled for the 8239 as shown in Figure 152 on page 176.

Figure 152. Rmon Management Item on JMA

The Remote Monitor application activated by clicking on Remote Monitor (see Figure 153).

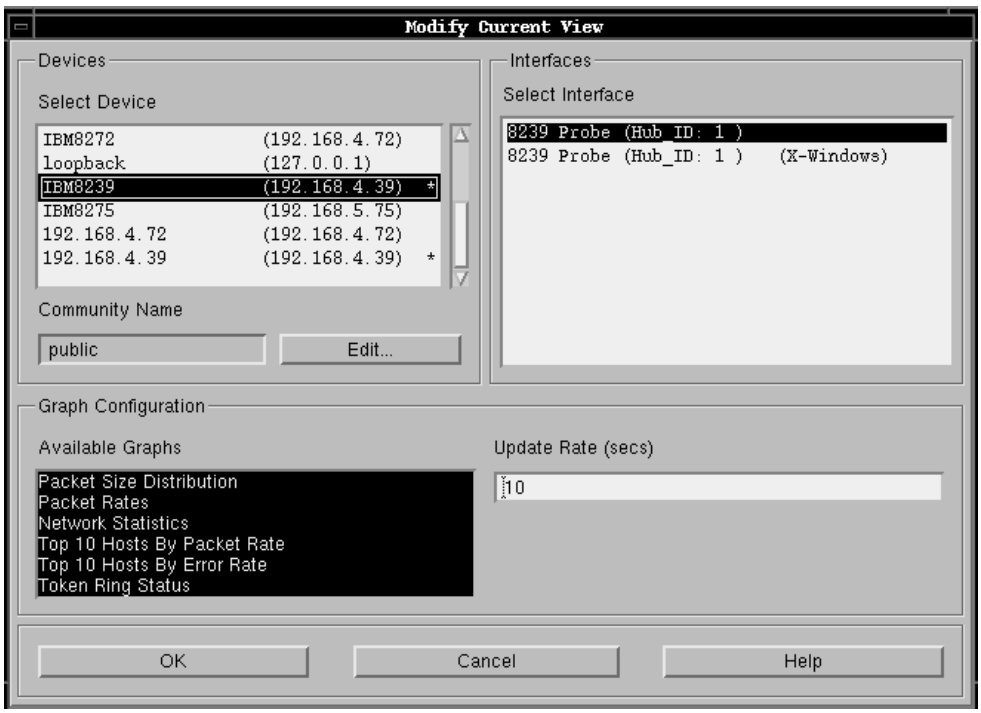


Figure 153. Remote Monitor Opened from JMA

Once Remote Monitor has been opened, the user has the choice to modify the existing view or select the device to run Remote Monitor against. This is done using the menu options shown below.

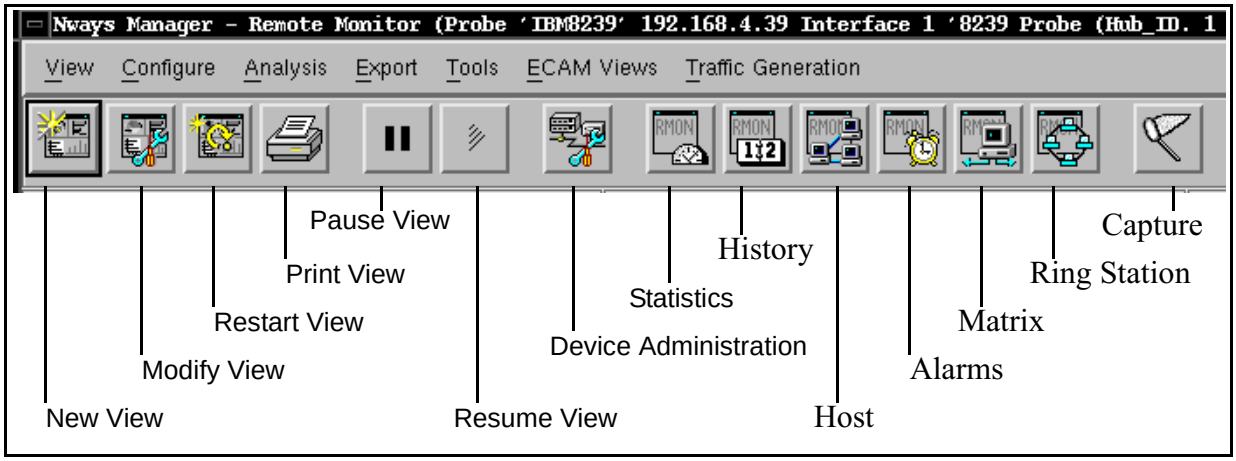


Figure 154. Remote Monitor Main Tool Bar

The device administration screen is shown in Figure 155.

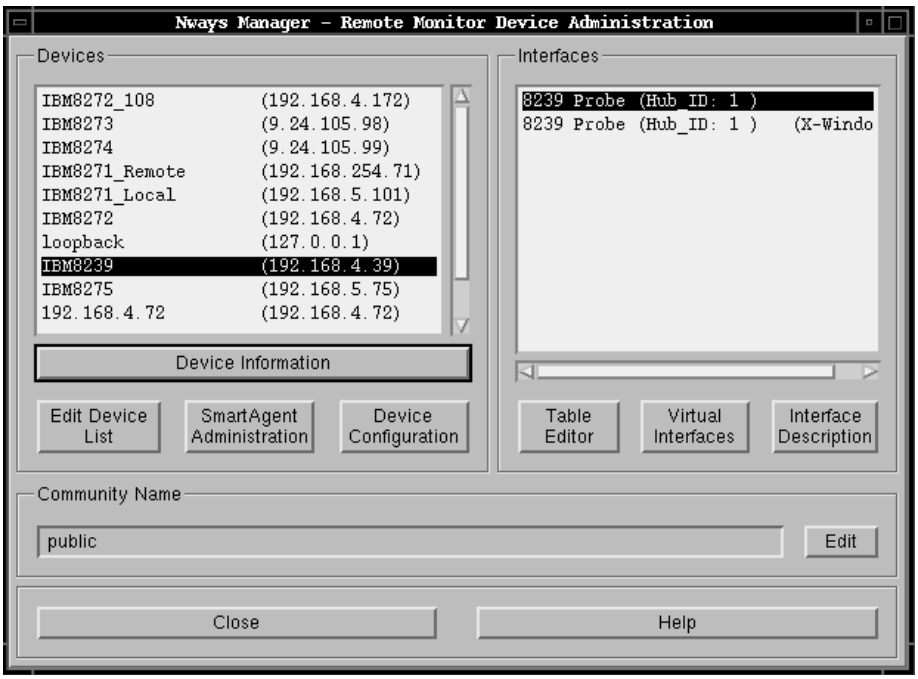


Figure 155. Remote Monitor Device Administration Window

This window can then be used to verify the details of the devices that Remote Monitor uses as RMON probes and can be used to add new devices to the list. This is done by selecting **Edit Device List**.

Figure 156. Edit Device List Window

Each device is identified by a unique name, IP address and also the default community name used to access the device. In this scenario the community name is set to private for most of the devices with read/write access.

The device information is displayed in Figure 157.

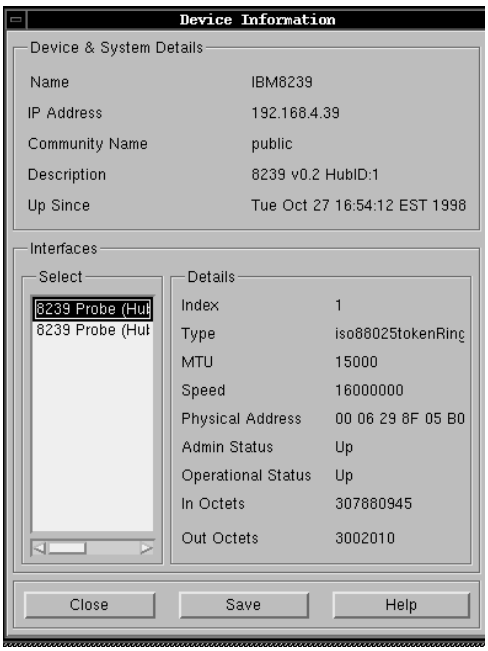


Figure 157. Device Information Window

The device configuration window is shown in Figure 158 on page 179.

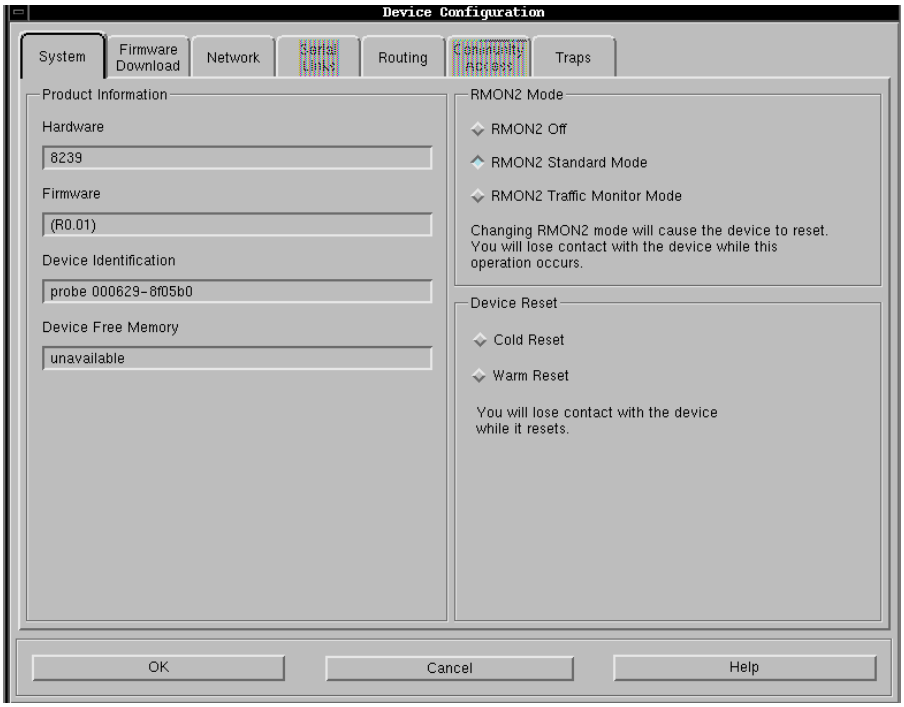


Figure 158. Device Configuration Dialog Window

The Device Configuration dialog allows the following actions to be taken by selecting the appropriate tag as follows:

- System Tab - View hardware/firmware, reset device, enable/disable RMON2 and set RMON2 mode
- Firmware Download - Upgrade the firmware
- Network - Set the IP address and subnet mask on each interface
- Serial Links - Set up serial link connections
- Routing - Set up static routes, default gateway, echo interval
- Community Access - Configure access control tables
- Traps - Configure trap communities and destinations

Further information on these setting can be found in the *Nways Manager - Remote Monitor User's Guide,* SA27-4195 or as an on line acrobat file in /usr/LANReMon/doc/lanremon.pdf.

In altering some of the above settings, the user needs to be aware that some of the changes will cause a reset of the device. The effect of these resets can be the loss of stored RMON data as well as some of the probe settings reverting to their default values. This is the case if the RMON2 mode is changed. By default it is set to standard mode, meaning that the device has set appropriate table sizes for use with Remote Monitor or another third-party management application.

The other available modes are Traffic Monitor Mode where the table sizes are set for use with Traffic Monitor 1.1 and above, and Off, where RMON2 is disabled to allow SmartAgent software access to the device. There are also the options to edit the tables available on a device and create virtual interfaces. The tables

available can be set using the **Table Editor** button on the Device Administration screen to open the panel below.

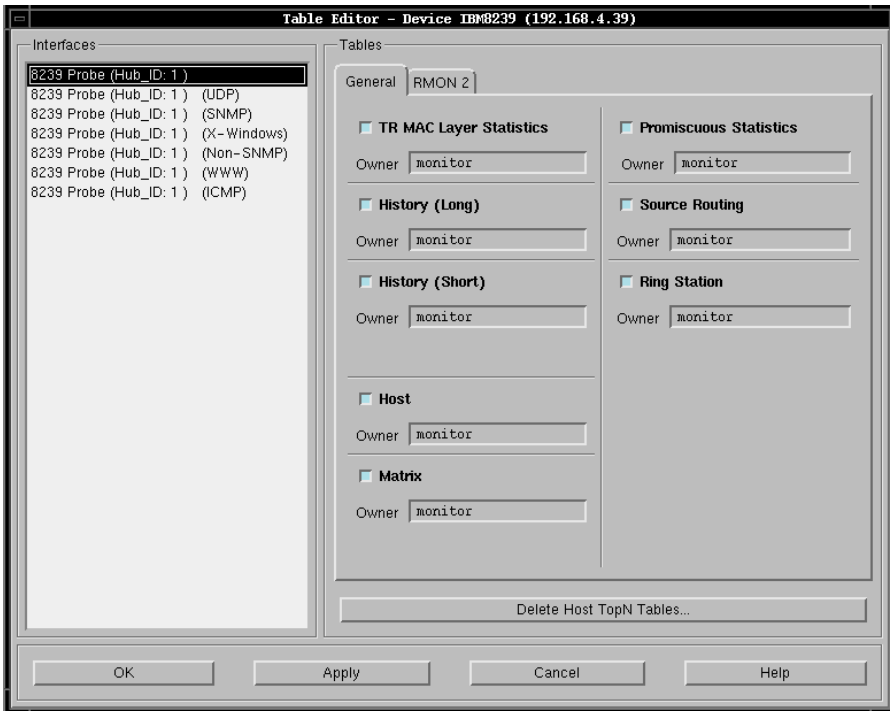


Figure 159. Table Editor Window

Virtual interfaces can be created on devices to provide some form of filtering for the traffic being monitored. Virtual interfaces are created on actual physical interfaces and are created by selecting the **Virtual Interfaces** button on the Device Administration window (see Figure 160).

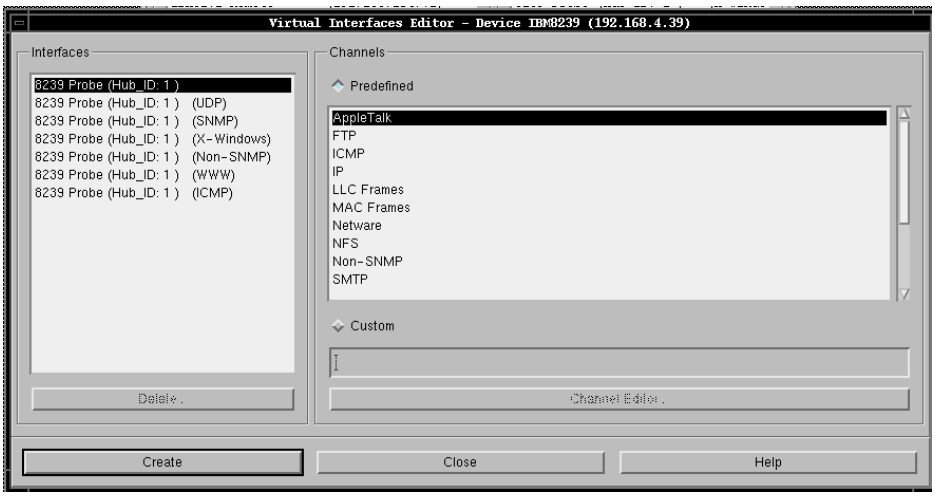


Figure 160. Virtual Interface Editor Window

Several virtual interfaces can be created for one physical interface. Each virtual interface can be created to use a pre-defined channel, a set of filters for a specific protocol or a custom channel.

This was not performed for this scenario, but a customized channel can be created to filter traffic according to many different protocol-specific templates, which allow the users to set parameters for the filters to work with when activated. This can create very complex filtering on a port, such as monitoring only the communications between two specific stations for one kind of packet. Each virtual interface that is created can then be used as a separate Remote Monitor monitoring gateway on the network.

In these scenarios the devices monitored by Remote Monitor are the 8239, 8273, 8274 and 8275. The 8260 hubs in the scenario can carry blades capable of running RMON and RMON2 probes, but in these scenarios were used to provide an ATM backbone only.

Once the main Remote Monitor window (referenced by the viewman task) is open, it is possible to modify this view to change the device being monitored, add a new device to be monitored, modify an existing device or open multiple view of devices. For instance, it is possible to view two different physical interfaces on a device, as below for the 8275.

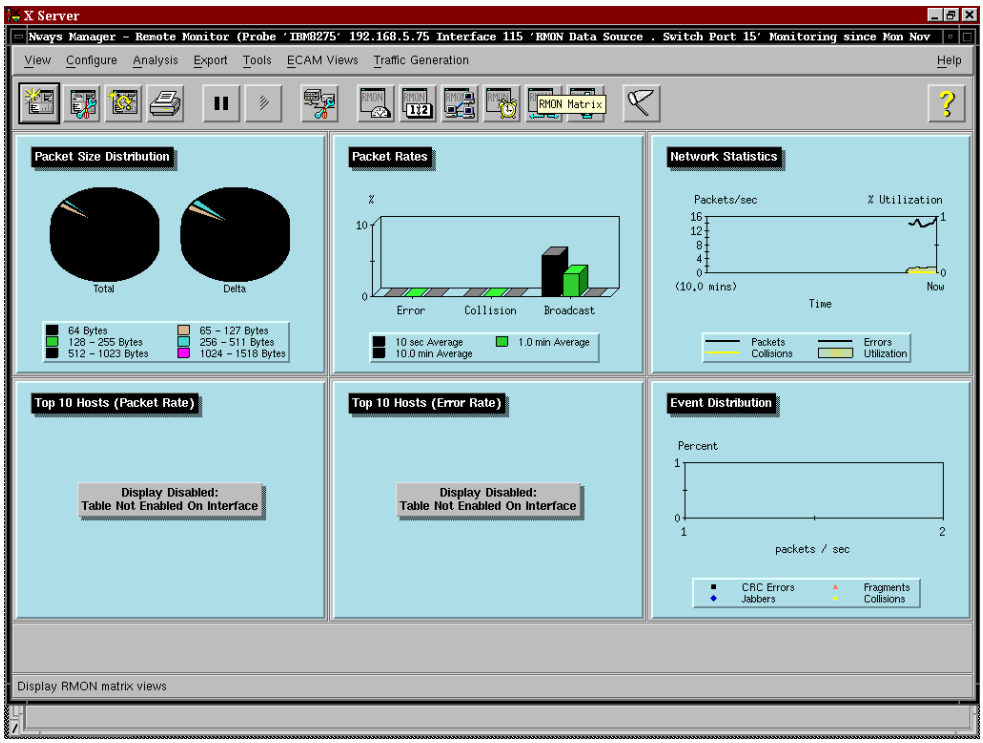


Figure 161. Remote Monitor View for 8275 Switch Port 15

It is possible to display two interfaces from the same physical location. The following views are of physical interface 1 on the 8239.

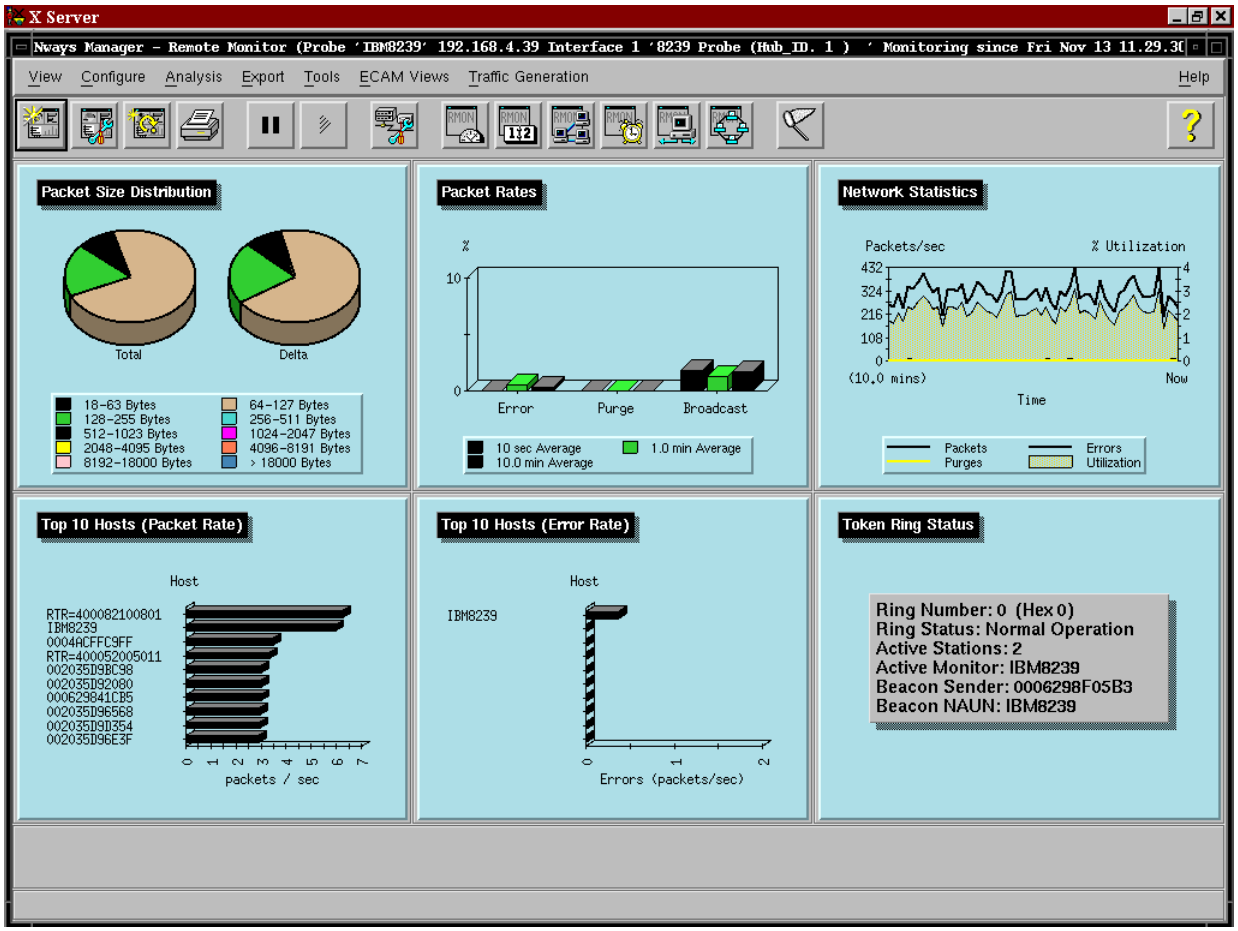


Figure 162. Remote Monitor View of 8239 Interface 1

The virtual defined view showing UDP traffic only is shown in Figure 163.

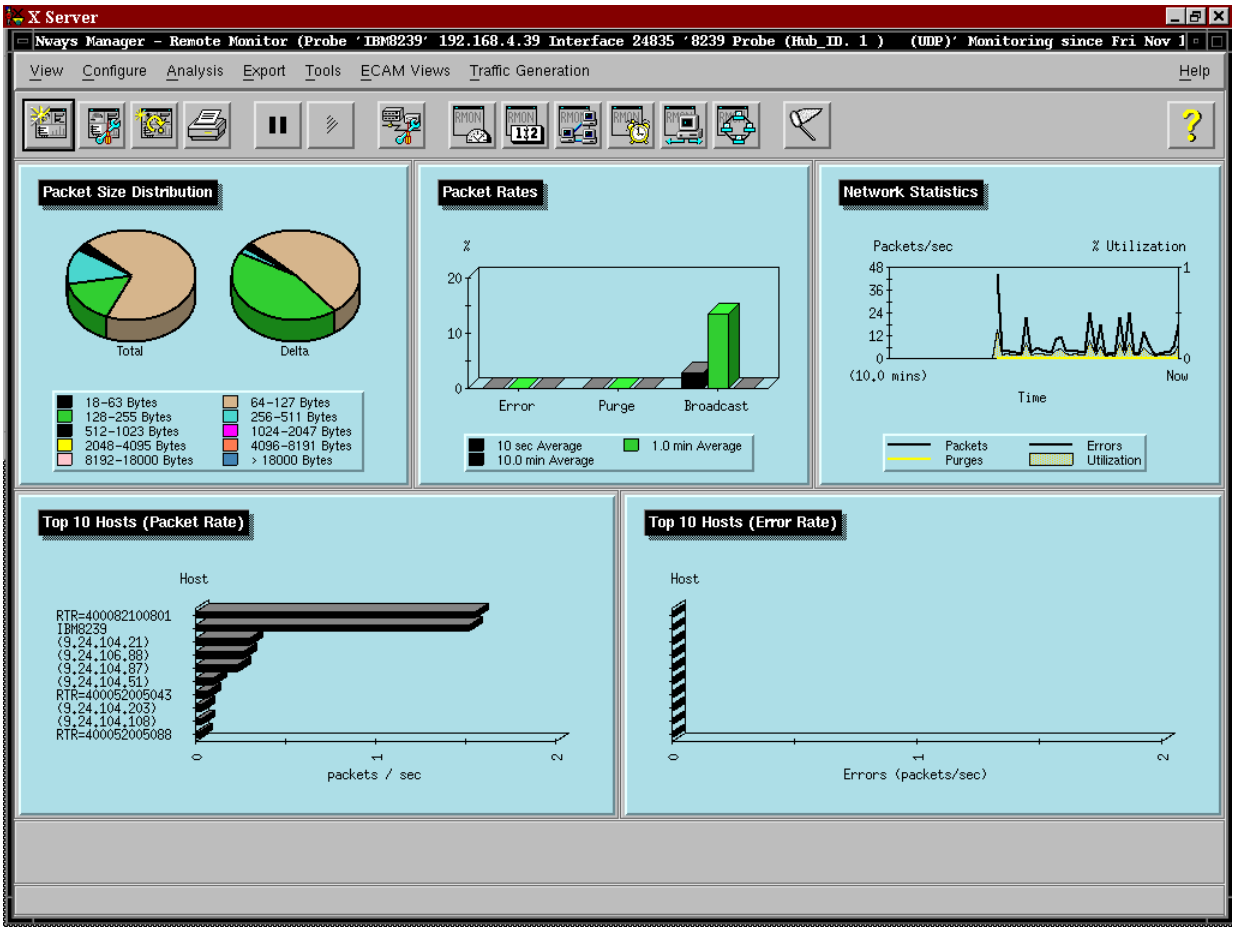


Figure 163. Remote Monitor View of 8239 Virtual Interface for UDP Traffic Only

The graphs shown on the main window are the default selections set at installation time but they can be altered. The following is a list of the graphs available by media type.

Table 15. Available Graphs By Media Type

Graph Type	Ethernet	Token-Ring	FDDI
Packet Size Distribution	Y	Y	Y
Packet Rates	Y	Y	Y
Network Statistics	Y	Y	Y
Top 10 Hosts By Packet Rate	Y	Y	Y
Top 10 Hosts By Error Rate	Y	Y	N
Top 10 Receivers	N	N	Y
Event Distribution	Y	N	N
Token-ring Status	N	Y	Y

The graphs that can be displayed are self-explanatory, with the possible exception of the Network Statistics graph, for which there are different variables depending on the media type.

Table 16. Network Statistics Graphs Available per Media Type

Variable	Ethernet	Token-Ring	FDDI
Collisions	Y	N	N
Aborts	Y	Y	Y
Packets	Y	Y	Y
Purges	N	Y	N
SMT Frames	N	N	Y
Utilization	Y	Y	Y

Remote Monitor has pre-defined views that are loaded when running, but these can be modified and new views created from the list of data variables available, to create customized views relevant to a particular network environment. This can be actioned by first selecting an existing Remote Monitor view, by clicking on one of the view icons or from the **Analysis** menu item and the subsequent **RMON Views** submenu. In the following example, the Statistics view was chosen.

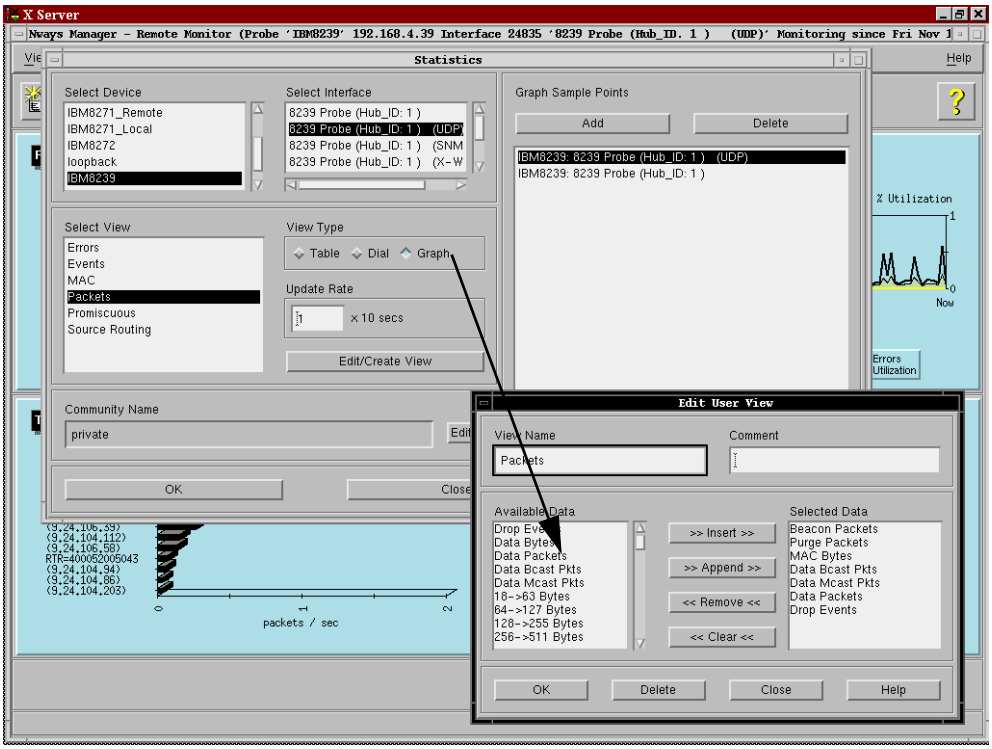


Figure 164. View Customization for 8239 Interface 1 and UDP Virtual Interface

Once the view window has been opened, the device and its interfaces can be selected. Multiple interfaces can be selected as long as they are of the same interface type, even if they exist on separate RMON-capable devices. Now the view can be selected or modified. Each view is a different collection of the data available for collection by the RMON probe. The **Edit/Create View** button allows

the view details to be opened, a list of the available collection data and what the view will actual collect. It is now possible to create a new selection of data to collect and save it as a new view. We did this for a new view called Packets_test, a modified version of the Packets view. The view will collect the following data.

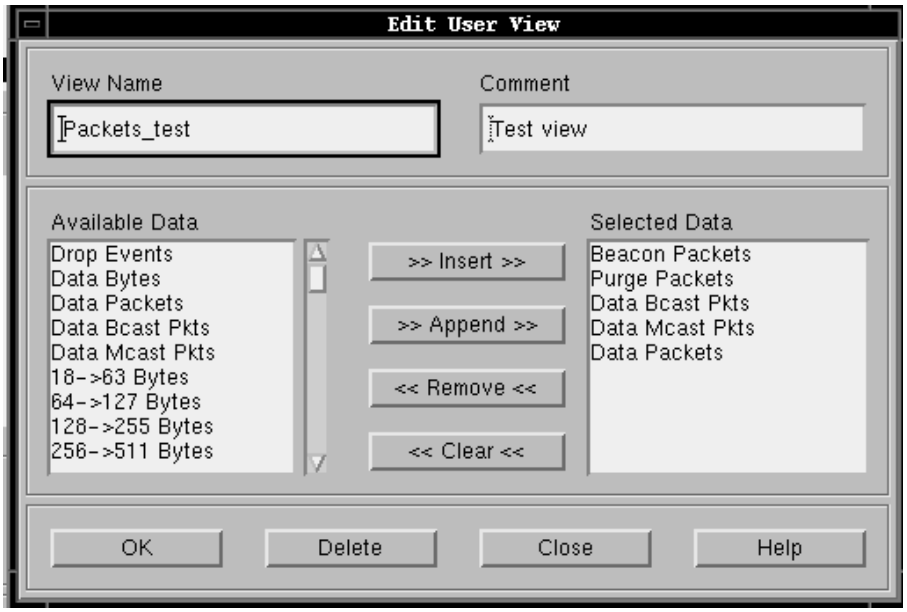


Figure 165. View Data Collected by 'Packets-test' View

Once the view has been created and selected, the Remote Monitor Grapher will open and display the requested information and display it in the requested format: table, graph and dial. These presentation windows can also be modified once they are opened.

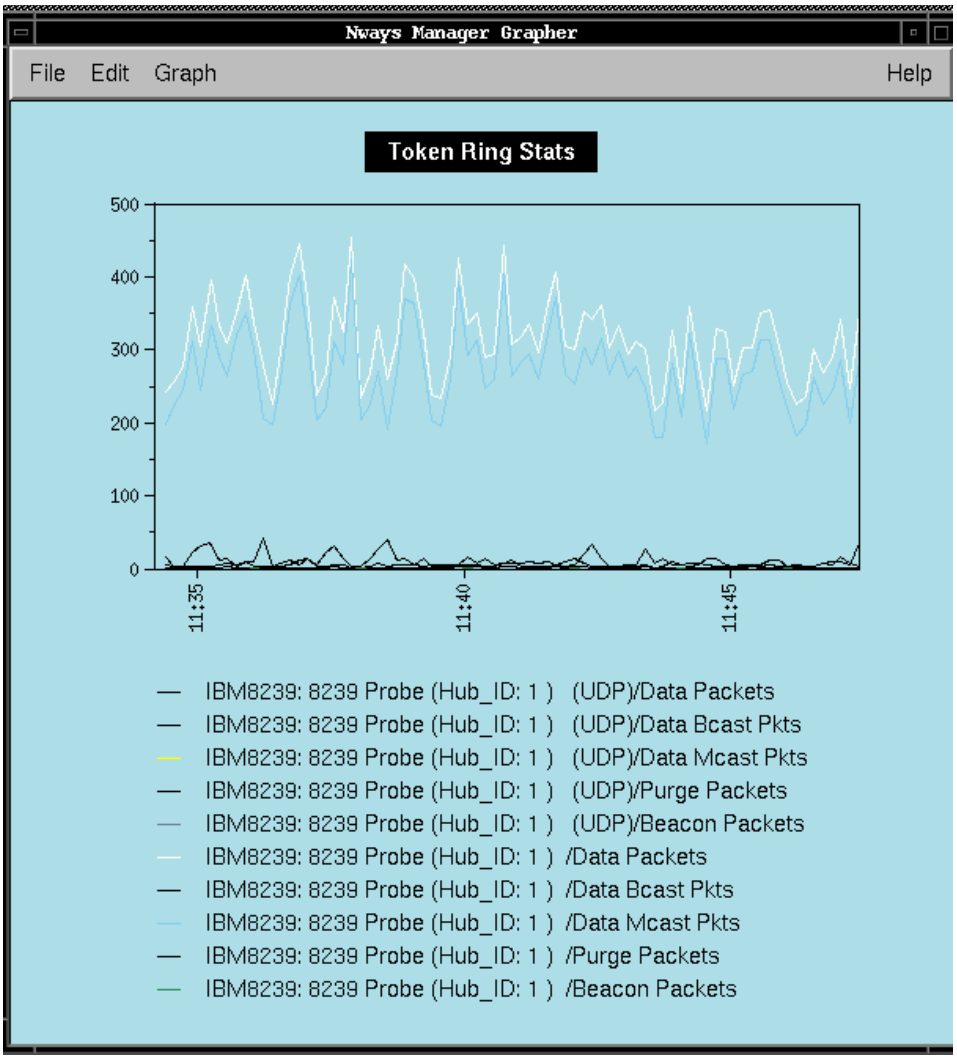


Figure 166. Token-Ring Statistics on the 8239 Interface 1

There are other options that can be taken, with regard to creating customized and using pre-defined views for the Host, History, Matrix and Ring Station views. However they would be more relevant in a larger network than in the test scenarios here. As with the statistics view, they can be set up to provide more granulation of the performance of the network and specific devices.

An important feature of the Remote Monitor product is that it can also provide historical performance information as well as real-time data monitoring. The collection of data is controlled by the Data Collector function. Prior to running the Data Collector, the device configurations should be checked on the devices that will be used for data collection. This is because the Data Collector can gather history, host and matrix information from the devices.

The history information is controlled by the history views defined on a device. If no history view exists then there will be no data to gather for the Data Collector.

The history views are created from the **History** item off the **Analysis** menu or from the **History Views** icon on the tool bar. Likewise, history views cannot be created until the history tables have been enabled on the devices in question.

This is achieved from the Device Administration panel by selecting the **Table Editor** button.

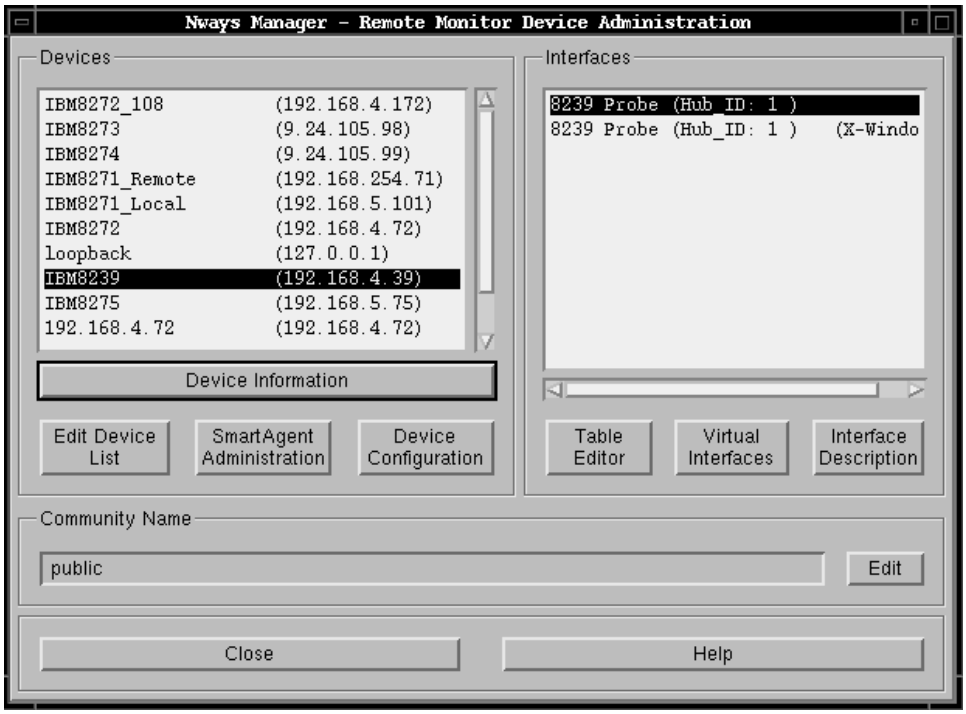


Figure 167. Table Editor Function on Device Administration Panel

The Table Editor will allow the user, provided they have the correct SNMP community access (read/write is required), to enable the tables on specific interfaces. There are two history tables; history short and history long.

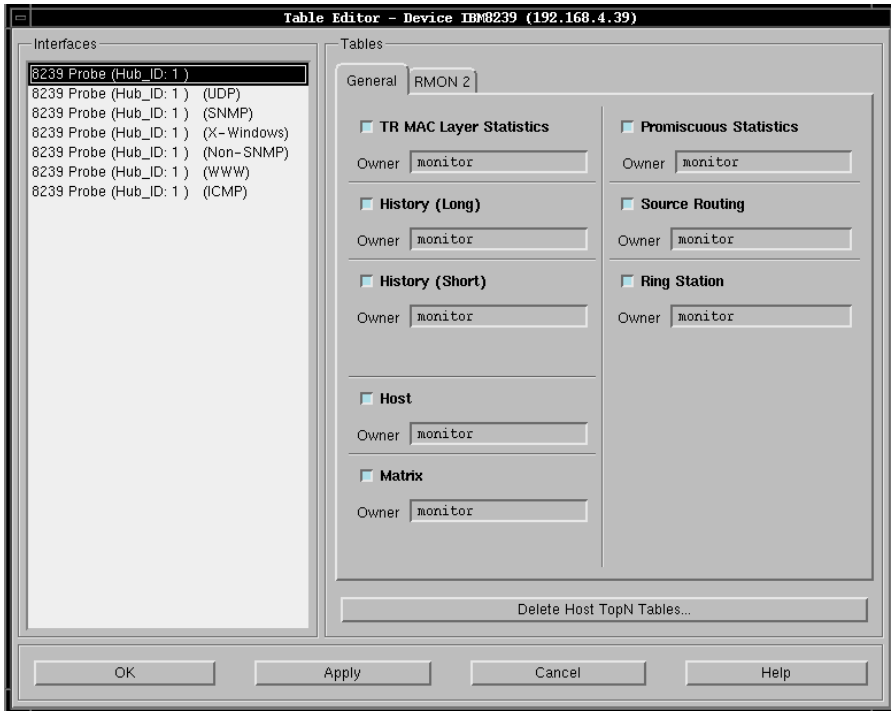


Figure 168. Table Editor View

The two tables should be enabled, so that history views can be created for both short and long sampling periods. To make the change permanent, click the **Apply** button. Now you can open the History View window and create some history views.

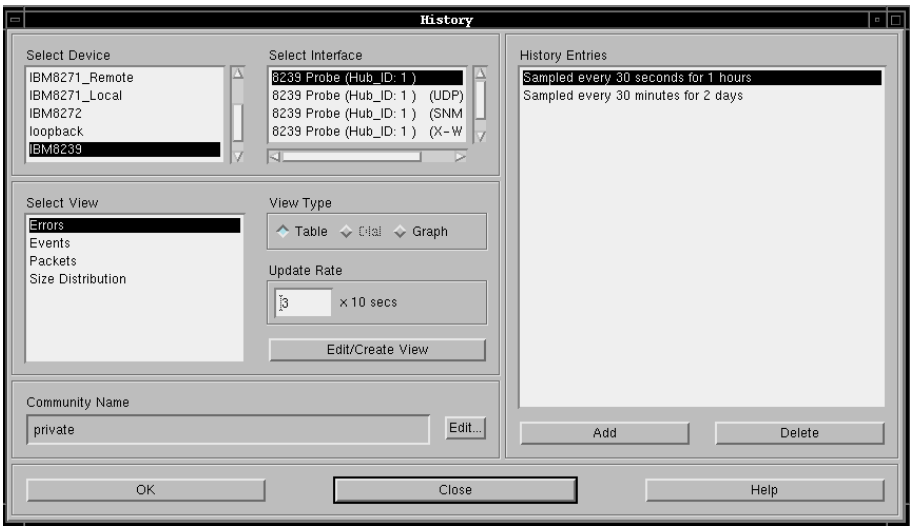


Figure 169. History View Panel

Click on **Edit/Create** to create a new history view. In exactly the same way as with the statistics view, users can define what data is to be gathered from which interface by creating new views. Then, new sampling periods can be defined by clicking on **Add.**

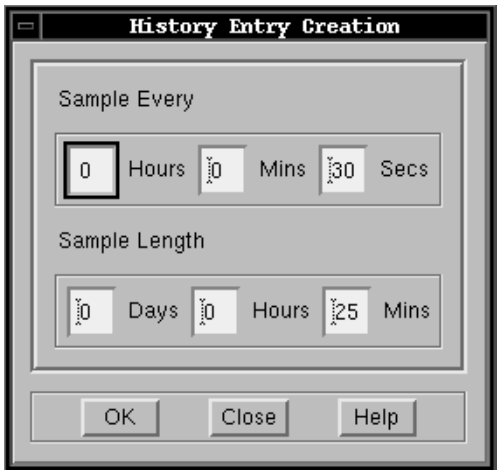


Figure 170. History Entry Creation Dialog Box

The only concern with history views is that the devices have to store the history entry details in specific memory locations or *buckets*. Each device has a pre-set number of buckets that can be used. For instance, a sample to be taken every 30 seconds for 10 minutes would require 20 buckets. If the history entries are going to exceed the number of buckets available, Remote Monitor will send out a warning message to indicate that there are insufficient resources to handle the request.

Once set, the history view will show the data requested over the defined sampling period, allowing some measure of trend analysis to be performed.

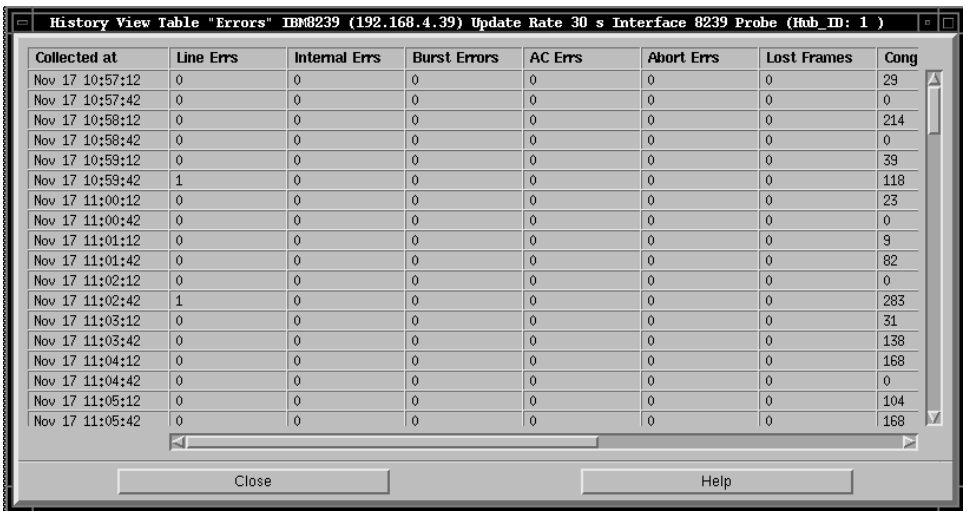


Figure 171. History Chart from 8239

The graph version of the history chart is shown in Figure 172.

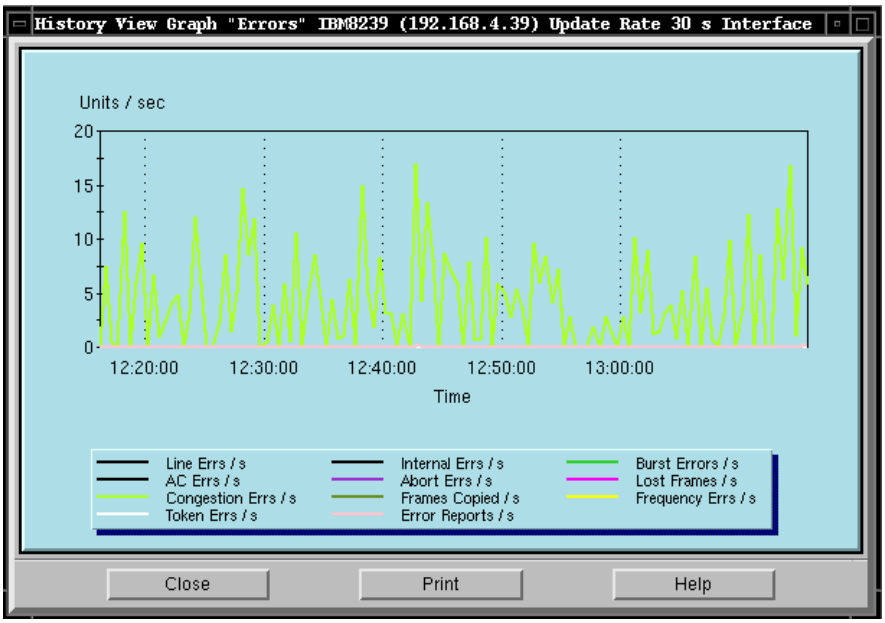


Figure 172. Graph Version of History Chart for 8239

History views can then be used as the basis for collecting long term information from network devices via the Data Collector. The Data Collector is started from the **Tools** menu item on the main view window.

Figure 173. Data Collector Launch from Tools Menu Item

Once launched, the Data Collector will open the main dialog box.

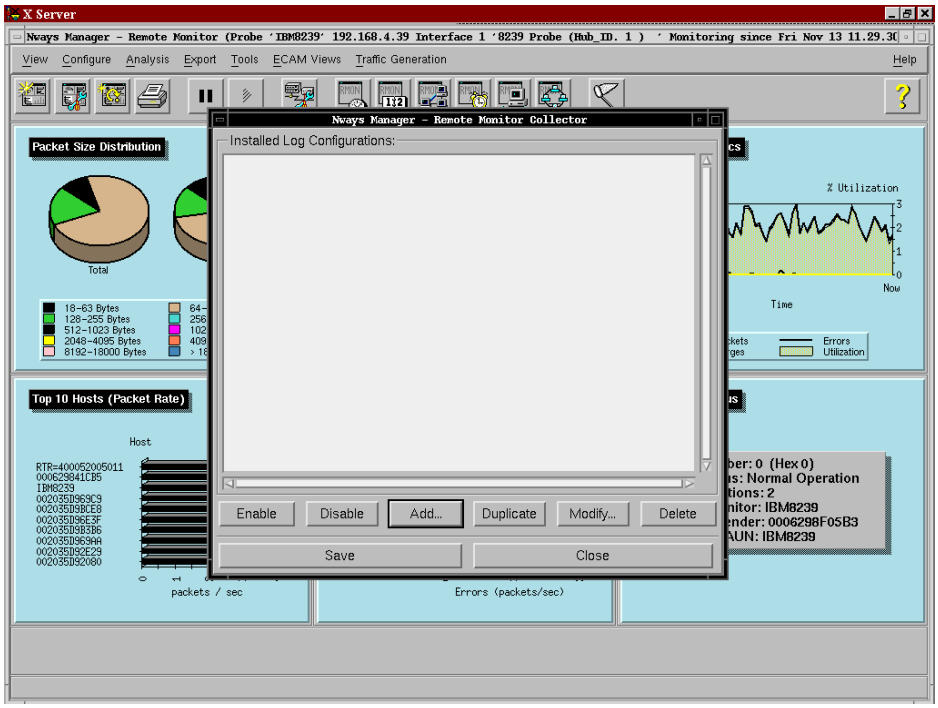


Figure 174. Data Collector Main Window

From here you can create the logging points and data collection configurations to run against the logging points. This action is limited to one user at a time, as the configurations are common to all instances of the Data Collector. The Data Collector makes use of the cron utility in AIX to schedule the data collection functions. An appreciation of the cron and crontab functions is required to help understand how the Data Collector works.

From the above main dialog window you can create, modify and delete data collection configurations. With a new installation, there are no configurations, so the user has to click on the **Add** button. This opens the Log Configuration Editor dialog window.

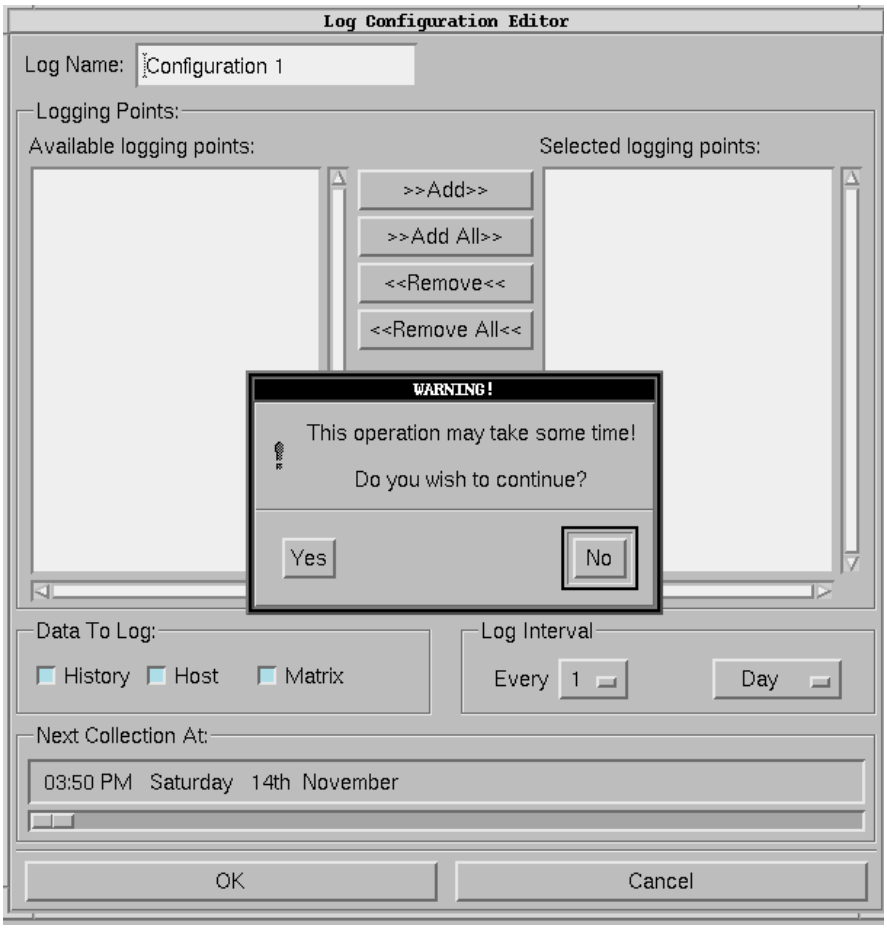


Figure 175. Log Configuration Editor Dialog Window

The first task in configuration is to discover all of the logging points that can be used for data collection. This involves interrogating all of the active RMON probes in the network to gather a list of the interfaces that are available. To activate this search, click on **Update Points** button. This opens a small dialog. Click on **Yes** to start the search. The search function takes some time, but has a progress window to show what devices are being interrogated and what logging points they contain.

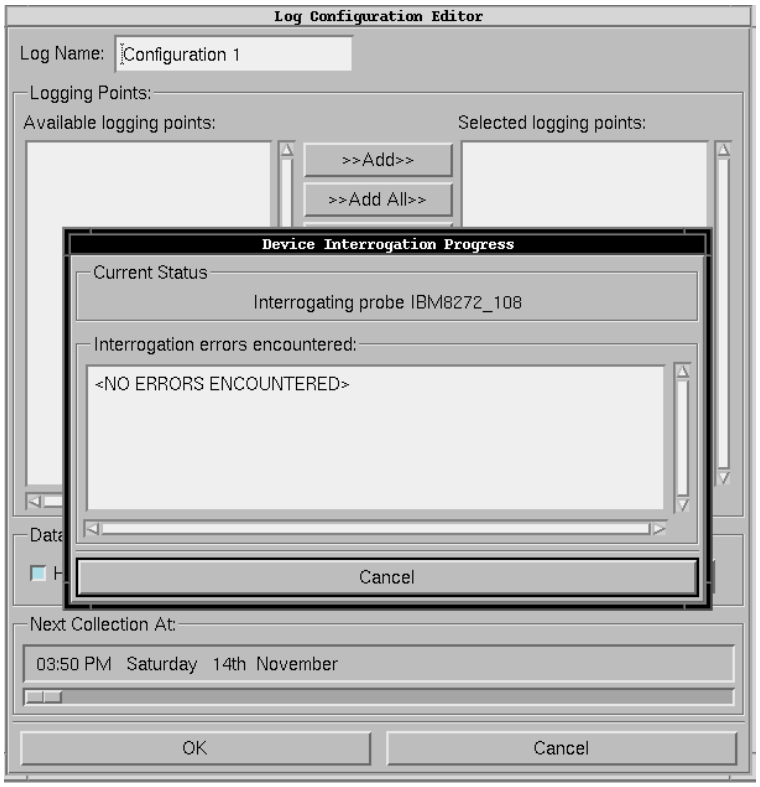


Figure 176. Updating Logging Points in the Data Collector

This list of logging points will then be displayed every time you try to create or modify a log configuration. The list is static, but can be updated by re-running the **Update Points** function, as would happen if new RMON-capable devices were added. The Data Collector reads the devices to interrogate from the probe.map file that Remote Monitor builds to list all of the available probes. Therefore, if a probe is deleted in Remote Monitor, the data collector will remove it from the logging points list at the next running of the **Update Points** function.

Before making changes to the list the Data Collector will warn of the changes that will happen if the user clicks **Process** in the resulting Device Interrogation Report screen (see Figure 177).

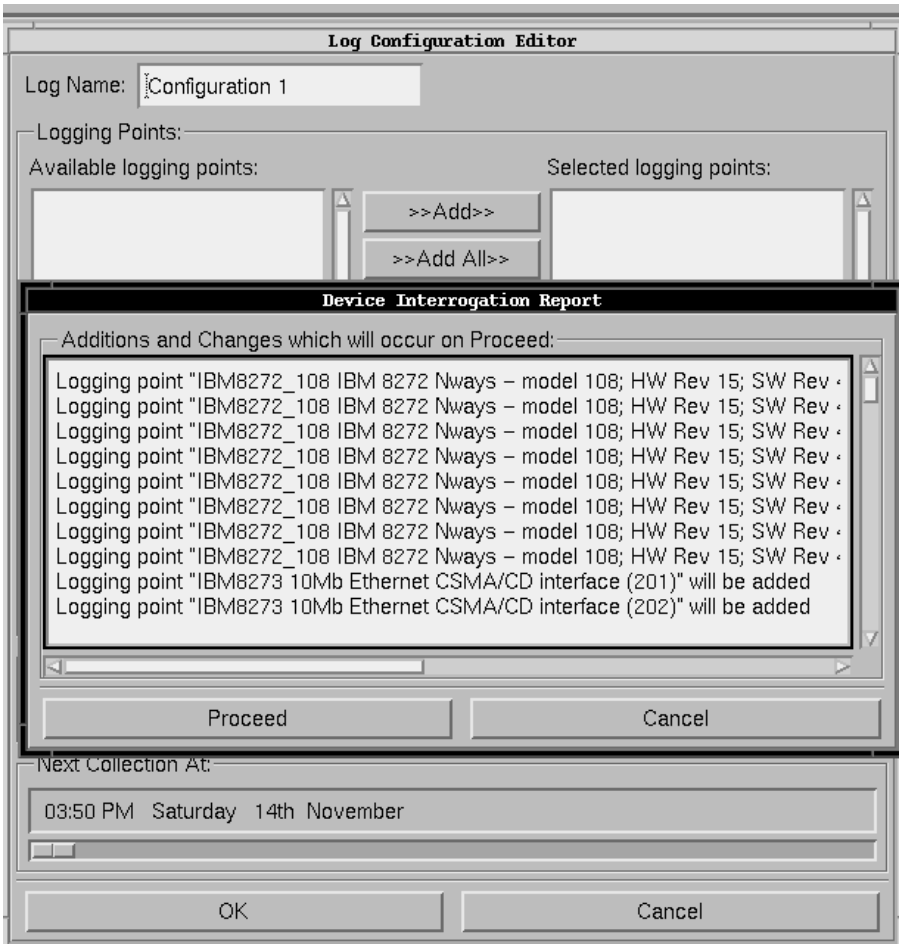


Figure 177. Device Interrogation Report Window

Once the **Process** button has been selected it will be possible to define which interfaces will be used as logging points for this particular collector configuration. Then we can decide what data should be logged, either history, host and/or matrix data.

Note

History data will only be collected from those devices for which a History view has been configured in Remote Monitor.

Now it is possible to set the Log Interval, the time at which collections should be made. The default is once a day and the exact time can be set in the Next Collection area, using the time bar. If the interval is greater than a day, the day and the time can be set. Intervals of less than a day can also be set, but they would be dependent on how regular the history view was being monitored.

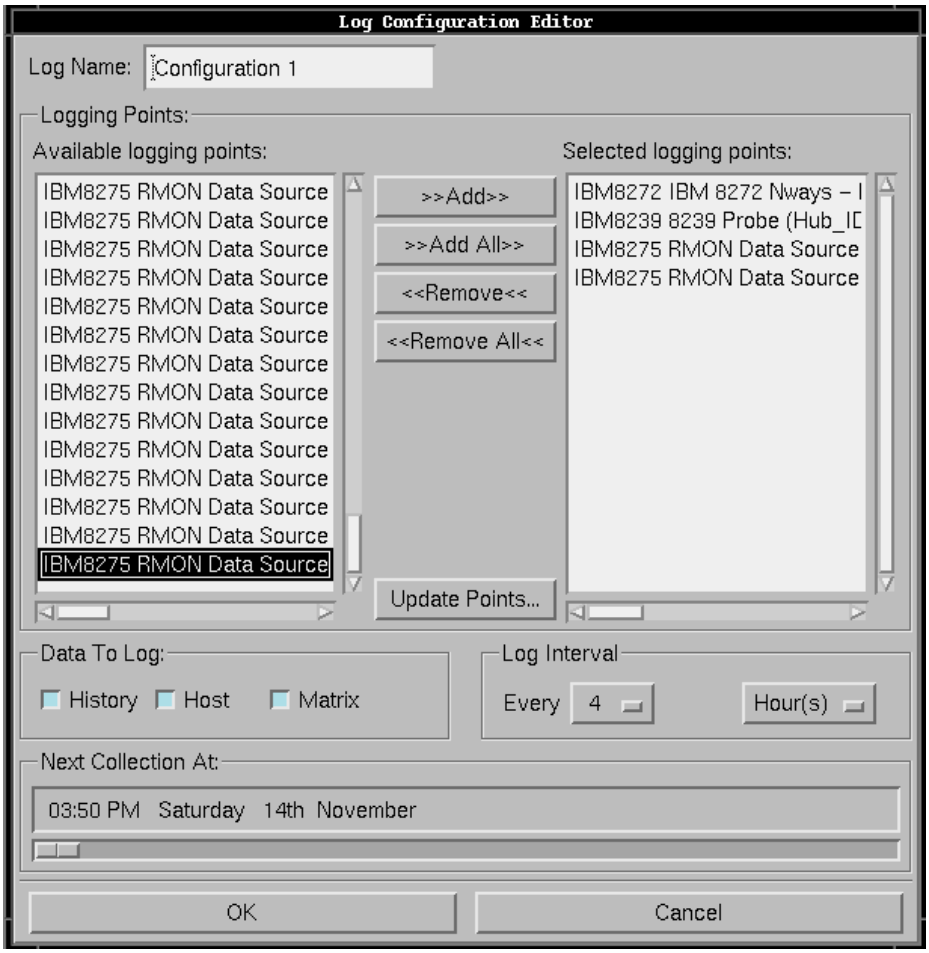


Figure 178. Log Configuration Editor Window

Once all of the details are correct, the configuration can be saved and identified by the name entered in the Log Name box. Created configurations can then be used as the basis for further configurations, the main Collector window being used to decide which configuration to enable.

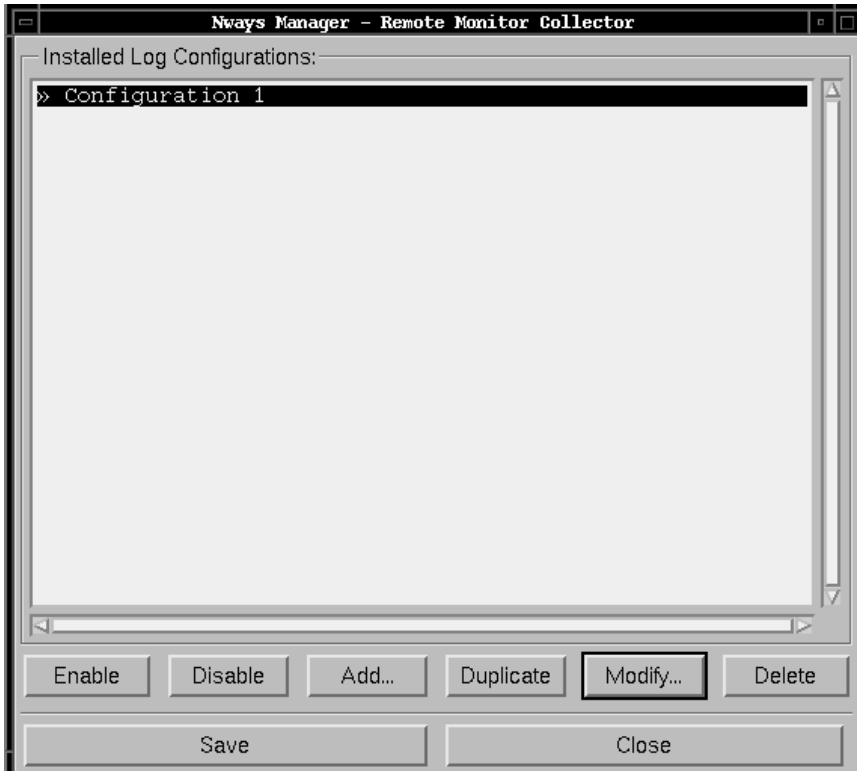


Figure 179. Collector Main Window - Active Configuration

NOTE

There should only be one data collection active at any given time of day. The collection process writes the data to common (and non-unique) file names. If more than one data collection is running at any given time, there is the possibility that the two processes would cause interference with each other and invalidate the data that was collected.

The collector stores the collected data in the /usr/LANReMon/rmon/LOGDIR directory in the Comma Separated Variable (CSV) format. This format means that applications that can handle the CSV format will be able to process the data and present in reports, graphs or spreadsheets. New data is appended to the existing files. The files created are as follows:

hist.csv Ethernet History Data
host.csv Host Data
matrix.csv Matrix Data
trml.csv Token-Ring MAC-Layer History Data
trp.csv Token-Ring Promiscuous History Data
fddihist.csv FDDI History Data

The size of these files will depend on the amount of data that is being collected, so frequent collections of large amounts of data from large numbers of devices will cause these files to grow quickly. The files are shown below.

```
rs600033t:/usr/LANReMon/rmon/LOGDIR > ls -l
total 190872
-rw-r--r--   1 root     system    215930 Nov 20 11:33 hist.csv
-rw-r--r--   1 root     system   53774199 Nov 20 11:10 host.csv
-rw-r--r--   1 root     system    2772327 Nov 20 11:10 host.dlt
-rw-r--r--   1 root     system   37508463 Nov 20 11:32 matrix.csv
-rw-r--r--   1 root     system    1756398 Nov 20 11:32 matrix.dlt
-rw-r--r--   1 root     system     837651 Nov 20 10:40 trml.csv
-rw-r--r--   1 root     system     849092 Nov 20 10:39 trp.csv
rs600033t:/usr/LANReMon/rmon/LOGDIR >
```

Figure 180. Logging File for Data Collector

After each sampling period has completed, there will be a message written to the /usr/spool/mail file of the user who is running the Data Collector. This is sent by the cron task and details any errors in the collection action, such as below, where there was no data to collect from several of the logging points.

```
                                aixterm
8.7) id LAA43562 for root; Mon, 16 Nov 1998 11:24:06 -0500 (EST)
Date: Mon, 16 Nov 1998 11:24:06 -0500 (EST)
From: daemon
Message-Id: <199811161624.LAA43562@rs600033t.itso.ral.ibm.com>
To: root

IBM8272 IBM 8272 Nways - Model 216; HW Rev 63; SW Rev 4.0.2A (May 11 1998 14:02:
35); SOLO Ver KS30P5; Token Ring; Base Port 1 (1) : No data for point
IBM8272 IBM 8272 Nways - Model 216; HW Rev 63; SW Rev 4.0.2A (May 11 1998 14:02:
35); SOLO Ver KS30P5; Token Ring; Base Port 1 (1) : No data for point
IBM8272 IBM 8272 Nways - Model 216; HW Rev 63; SW Rev 4.0.2A (May 11 1998 14:02:
35); SOLO Ver KS30P5; Token Ring; Base Port 1 (1) : No data for point
IBM8272 IBM 8272 Nways - Model 216; HW Rev 63; SW Rev 4.0.2A (May 11 1998 14:02:
35); SOLO Ver KS30P5; Token Ring; Base Port 1 (1) : No data for point
IBM8275 RMON Data Source : Switch Port 01 (101) : No data for point
IBM8275 RMON Data Source : Switch Port 01 (101) : No data for point
IBM8275 RMON Data Source : Switch Port 15 (115) : No data for point
IBM8275 RMON Data Source : Switch Port 15 (115) : No data for point


**************************************************************
        cron: The previous message is the standard output
        and standard error of one of the cron commands.

rs600033t:/usr/spool/mail > _
```

Figure 181. Output in /usr/spool/mail for Data Collector

Remote Monitor is used primarily as a tool for gathering data to perform network performance and service analysis with. It can be used as a real-time tool or as a trend-analysis tool. In real-time mode, it is possible to not only monitor the traffic, but to set some performance thresholds that can be used to provide early indications of out-of-line conditions or exceptions. The function in Remote Monitor to enable these thresholds is started from the Alarm toolbar icon or from the Alarms submenu item under the Analysis menu item.

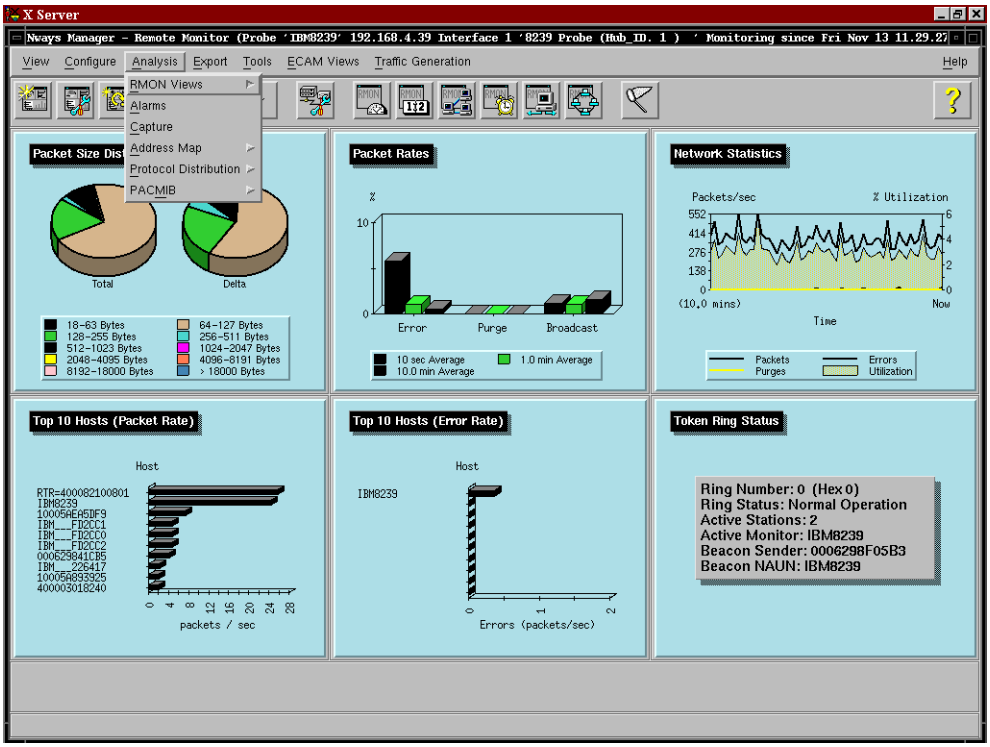


Figure 182. Starting Alarms from Remote Monitor Main Window

The first window to open will be an Alarms dialog box, which will be empty the first time it is opened. Each device, when displayed in the box, will show the message No entries found on that device.

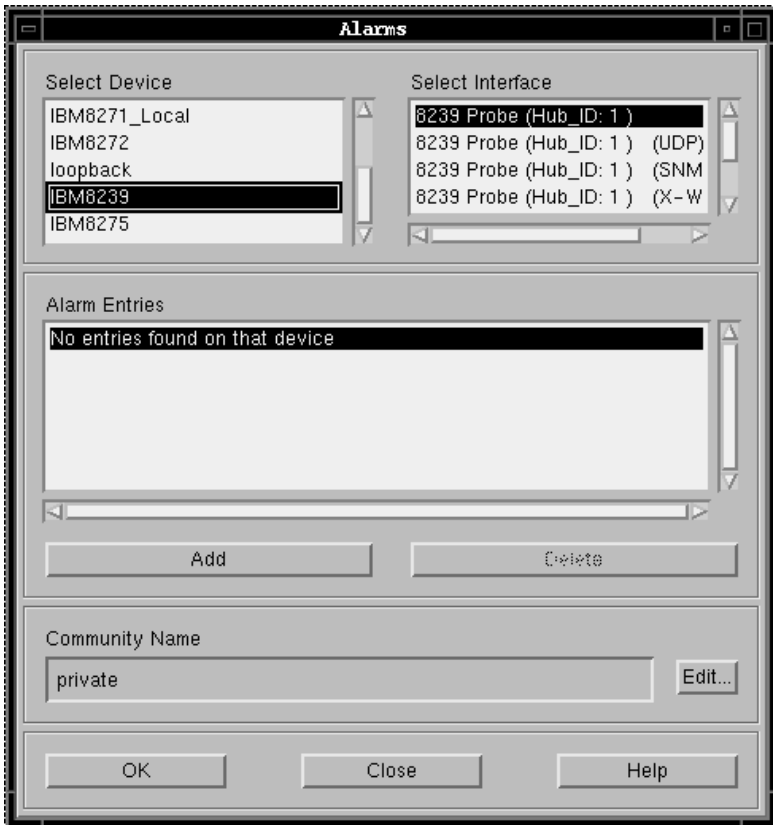


Figure 183. Initial Alarms Dialog Box

Clicking on **Add** will open the Alarm Entry Creation dialog box for that device.

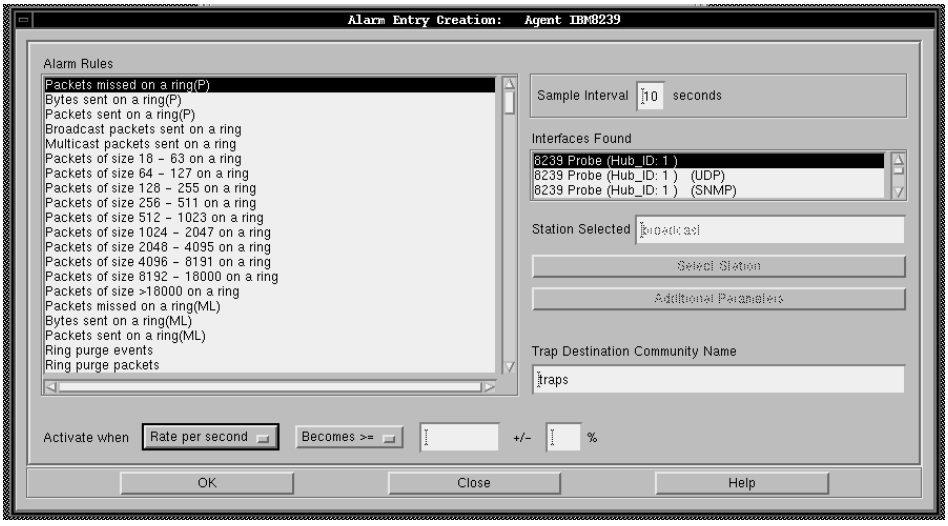


Figure 184. Alarm Entry Creation Dialog Box for IBM8239

The Alarm Rules shown in Figure 184 shows the alarm rules available by selecting an alarm rule you can list the valid interfaces for that rule in the Interfaces Found window; invalid interfaces will be grayed out in this window. In the Sample Interval area, you can set how often the event will be checked for. If a

station-specific alarm has been selected, then the Select Station option will become active and a station can be defined for the rule.

Certain alarms require further information in order to complete the alarm description and the **Additional Parameters** button will be selectable in order to do so. The final item to consider is the **Activate When** condition shown in the Figure below.

Figure 185. Options for Alarm Activation

We can specify the alarm monitoring for either a rate value or an absolute value. The trigger conditions allow for the alarm to be raised if the value monitored rises above or below a set threshold, or the crosses condition which is triggered when the monitored value crosses the threshold only and not when the monitored value stays above or below the threshold.

The percentage box allows some flexibility over the triggering value by specifying a *barrier zone* around the threshold. Clicking **OK** will create the alarm and initialize the alarm conditions within Remote Monitor.

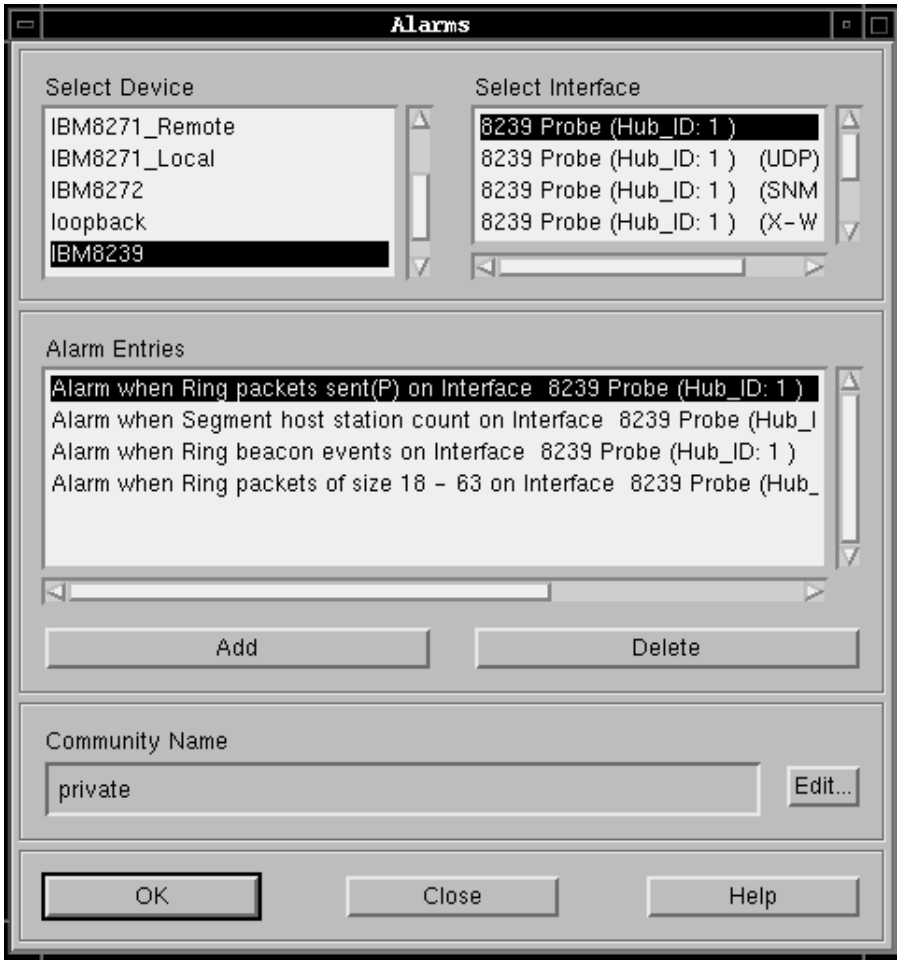


Figure 186. Alarms Window Showing Active Alarms

In Remote Monitor there will now be an Event Log window which will display the date and time that an alarm was triggered and the exact conditions of the event.

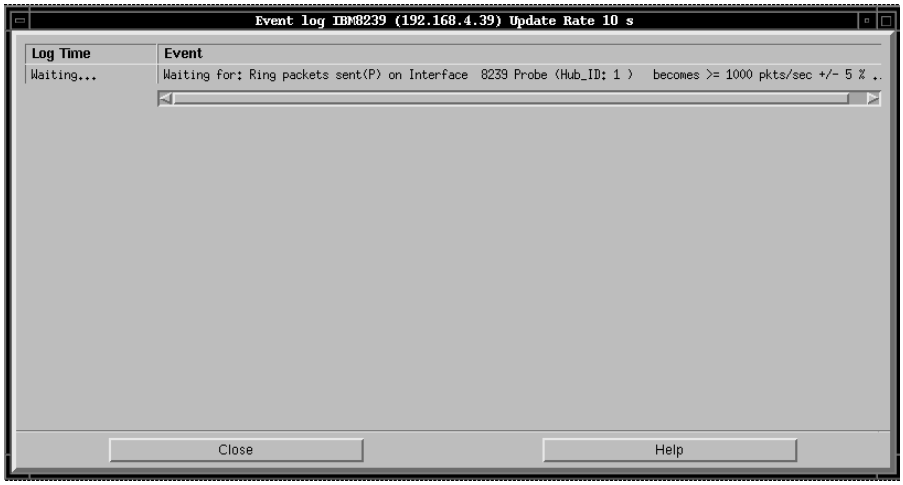


Figure 187. Remote Monitor Event Log Display Window

Also, there will be an indication on the main Remote Monitor window, in the form of an alarm icon. Pointing the mouse on the icon will give a description of the alarm event.

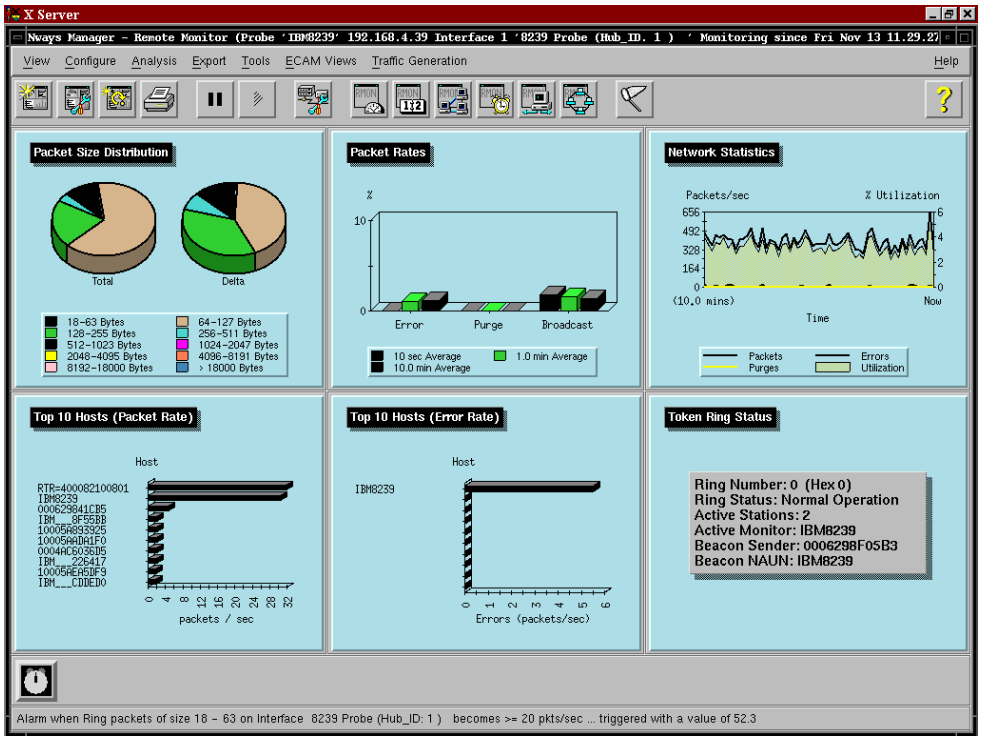


Figure 188. Alarm Display in Remote Monitor Main Window

As Remote Monitor can integrate into Nways Manager and NetView, the alarms are also available to the NetView Event Desk. This means that the NetView ruleset editor and event stream enhancement functions can be used to provide back end processing on Remote Monitor alarms. It also means that the alarms can be forwarded to Tivoli TEC and other network management focal points.

When the event is sent to NetView it will appear as shown in Figure 189.

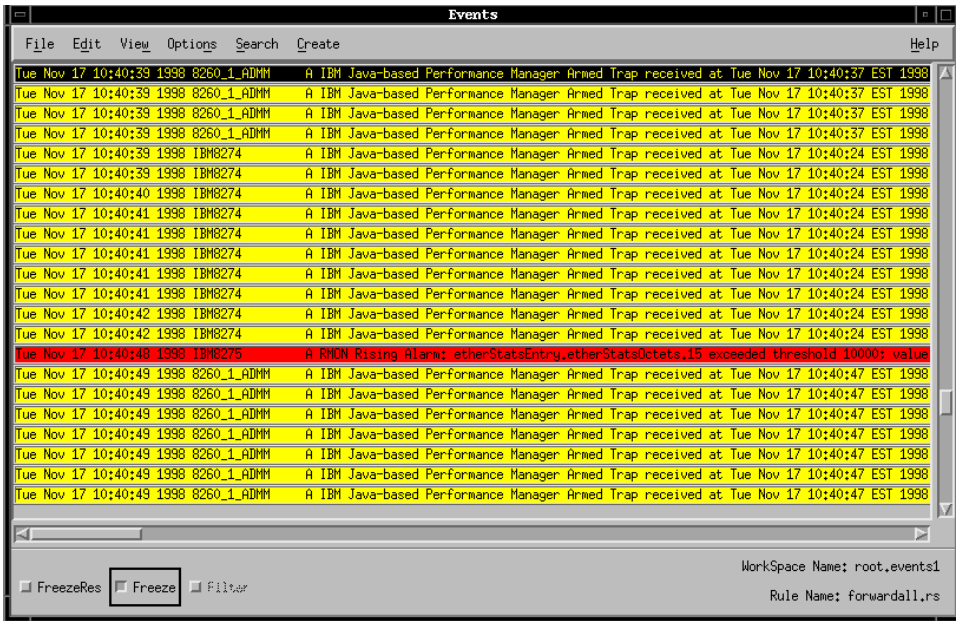


Figure 189. Event Desk Showing Remote Monitor Alarm

Another option is to create a dynamic workspace for Remote Monitor alarms only. The setup screen is accessed by the **Create->Dynamic Workspace** options from the Event Desk menu.

Figure 190. Dynamic Workspace Configuration for Remote Monitor Alarms

Here we can filter and display only the events we want to see.

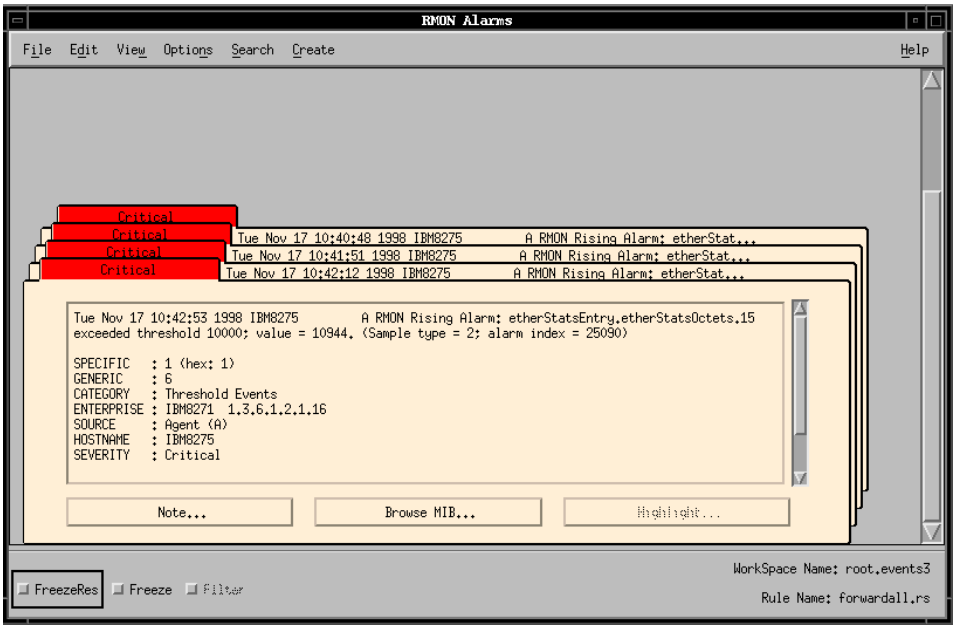


Figure 191. Dynamic Event Workspace RMON Alarms

Remote Monitor also has the ability to perform packet capture and decode, as well as some protocol distribution analysis and traffic generation functions. However, in this scenario, there was no real requirement for these functions so they were not discussed. The same applies to the Roving Analysis Port Application and Port Address Correlation MIB (PACMIB) support functions, as none of the modules that these applications support were used in the scenarios. Likewise, there were no HT-MAC and HE-MAC cards in the 8260 hubs, so there was no requirement to load and use the ECAM modules in the scenarios.

6.6 Traffic Monitor for AIX

We now take a very brief look at the Traffic Monitor application. Our network had no ECAM modules connected therefore we could not show the all the functions for the application. However we did have the 8239 running RMON 2, which we can use for Traffic Monitor.

To set up the application select **Monitor->IBM Traffic Monitor** from the NetView pull-down menu (see Figure 192 on page 205).

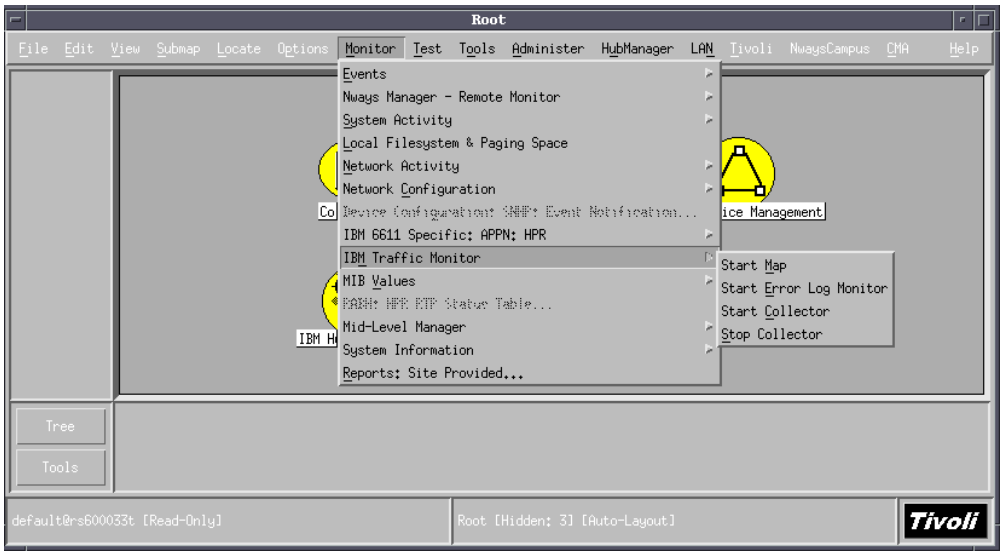


Figure 192. Starting Traffic Monitor

Select **Start Map** (see Figure 193 on page 205).

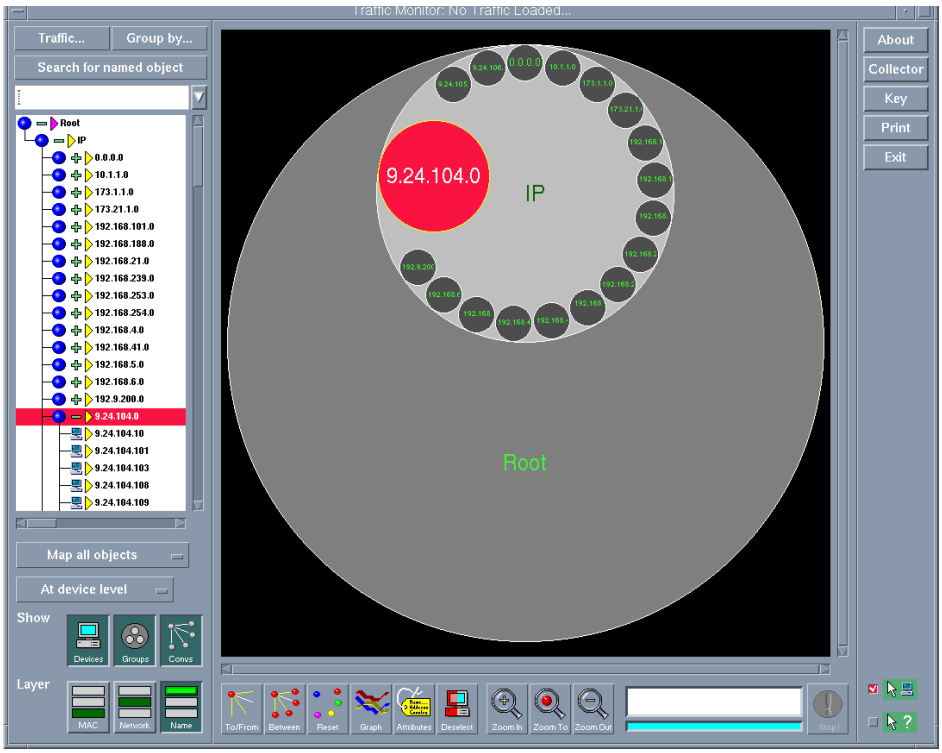


Figure 193. Our Discovered Topology

In order for this to work we had to define sample points, a sample point set and collection information. This following screens show what we did for the 8239.

The configuration screen is accessed by clicking on **Collector**.

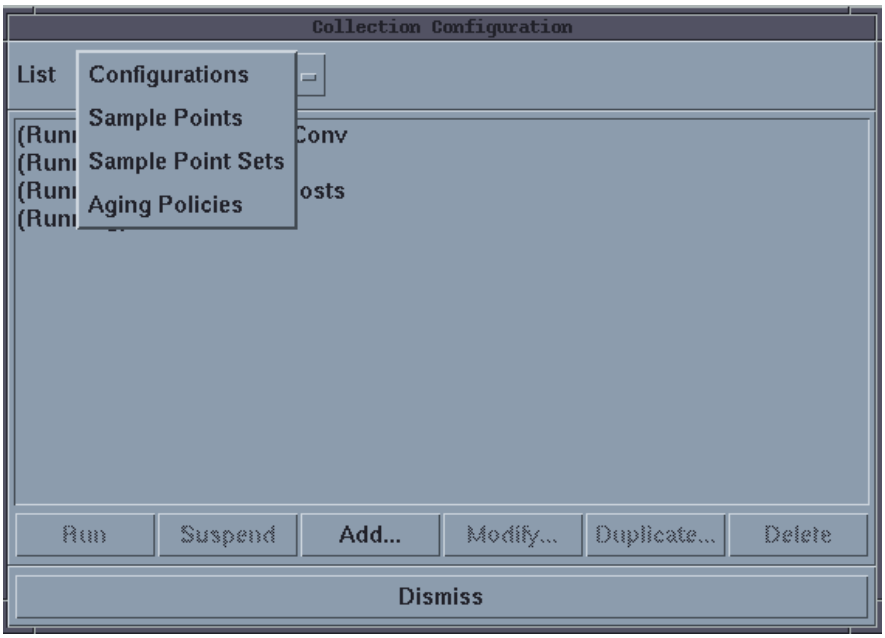


Figure 194. Collection Configuration

We added the 8239 as a node. This involves creating a sample point and toggling the option for List to **Sample Points**.

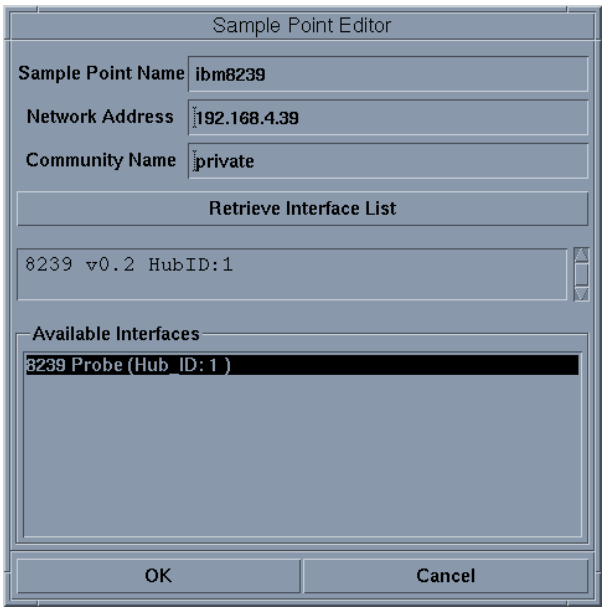


Figure 195. Sample Point Editor

Next we added a sample point set as shown in Figure 196 on page 207.

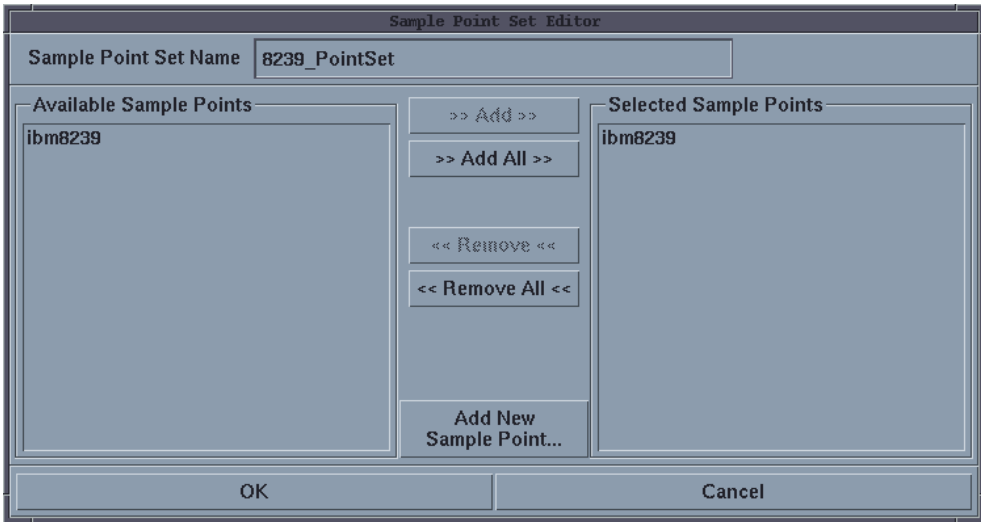


Figure 196. Setting Sample Points

Once added click on **OK**.

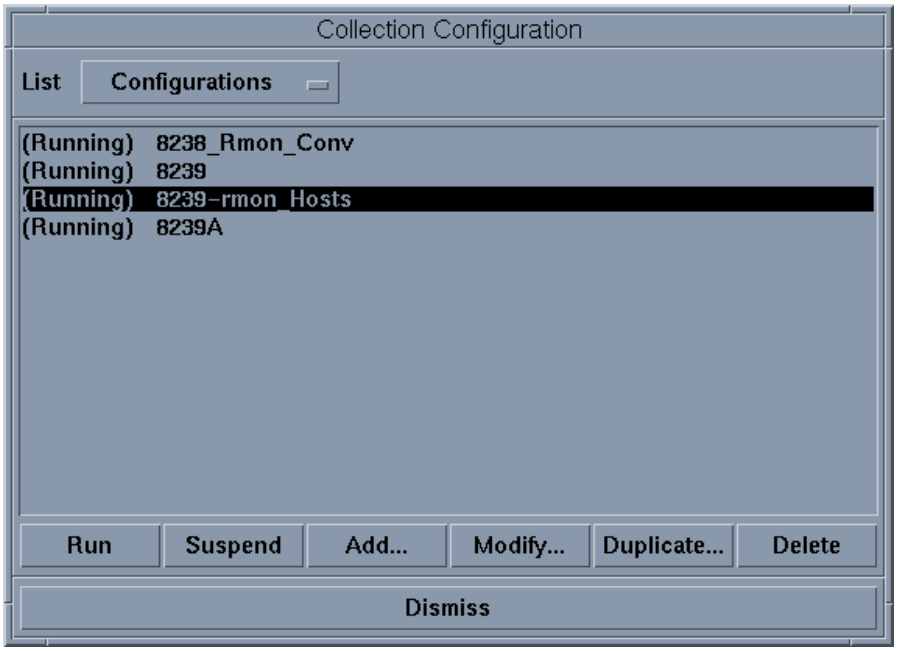


Figure 197. Collection Configuration

The final configuration option sets up the collections. The two configurations we created were for the RMON conversation statistics and the hosts stats (see Figure 198 on page 208).

Figure 198. Configuration Editor

To load data onto the map you must select **Traffic** from Figure 193 on page 205.

Figure 199. Load Traffic

To load the traffic data select **Use existing data**. These data files are held in the directory:

`/usr/LANRemon/traffic_db/current`

After loading the traffic we can see the traffic between subnets as shown in Figure 200 on page 209.

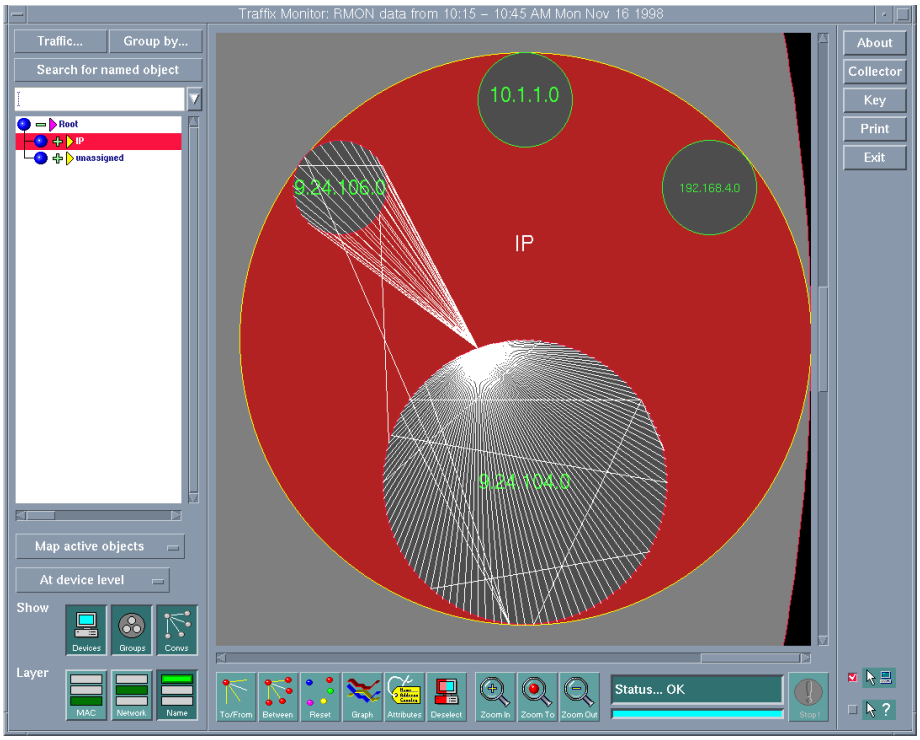


Figure 200. Traffic between Subnets

By using the right-hand mouse button you can access different graphs that show information such as the top ten hosts.

Chapter 7. Nways Java/Web Management Applications

This chapter concentrates on the Web interface to both NetView and the Nways management applications. The Web interface consists of accessing the Web clients for the NetView, Nways, Java device managers and the Java performance manager. The Java management applications are one application providing three different functions, these are:

- MIB browser and builder of the navigation tree
- Device management support under the SNMP bullets
- JPM configuration tools and performance views

Nways Manager has the capability of Web-based network management. The Web-based network management extensions provide access to the Nways Java-based management functions from Web browsers anywhere in the enterprise. When the Nways Manager is going to be installed and configured for Web-based and Java management, there are some requirements and concerns that must be addressed. This section describes the configuration for using Java-based management and Web-based network management applications.

7.1 Web Server Configuration

Nways Java Management provides the capability of Web-based access through a web browser. You must configure your Web server to locate the Nways Java Management Web pages subdirectory. The default Nways Web pages directory is /usr/CML/JMA/java/websvr.

Web servers supported for the Nways Web access include:

- ICS Apache Server (TME 10 NetView default Web server)
- IBM Internet Connection Secure Server
- Lotus Domino Go Server
- NetScape Enterprise Server

On the network management station, you must configure on the Web server the JMA and ATM applications to work properly through the Web, these are:

1. Assign an alias or logical name to the directory in which the Nways Java Management Web pages are stored on the management system
2. Assign an alias or logical name to the directory in which the Nways ATM Management Web pages are stored on the management system

If you are using a Web server other than ICS Apache Server or the IBM Internet connection secure server you can find configuration examples from the Nways JMA help files which are located in:

```
/usr/CML/JMA/java/websvr/help
```

Use the Web browser to access these help files. The main navigator file is toc.html and the help file for Web server configuration is:

```
/usr/CML/JMA/java/websvr/help/ibm.nways.subsys/ibm.nways.subsys.webtoc.html
```

7.1.1 Web Browser Configuration

The JDK Version 1.1.4-compliant Web browser is required for Web access to the Nways Java Management such as:

- UNIX platform
  - Sun HotJava Browser 1.0 or 1.1.4 only
- Windows platform
  - Microsoft Internet Explorer 4.0 or 4.01 with the RMI patch
  - Netscape Communicator Professional Edition 4.0.5 or later
  - Sun HotJava 1.1.4

Java support is provided with the browser. The Web browser can dynamically load the Java application.

7.1.1.1 Sun HotJava

There is a recommendation to expand the virtual memory of the HotJava workstation as follows:

- Initial size = 200MB
- Maximum Size = 200MB
- Max Registry Size = 13MB

Another concern on using HotJava is security. You have to configure the Applet Security from hotJava Preferences menu:

- From the **Preferences** option select **Applet Security.**
- Change security of unsigned applets to Medium Security.

When starting HotJava use the option:

```
HotJava -mx96M
```

7.1.1.2 Microsoft Internet Explorer

The Microsoft Internet Explorer 4.0 (IE4.0) and later versions include partial support for JDK 1.1. Microsoft's support for JDK 1.1 is incomplete. In particular, one of the missing features is Remote Method Invocation (RMI). Nways Manager has provided a patch utility with this product that adds the RMI feature. You can find it in the directory:

```
/usr/CML/JMA/java/websvr/RmiPatch
```

This directory contains a zip file, RmiPatch.zip that needs to be downloaded and unzipped on the client machine where you have IE4.0 running. The steps for installation of the RmiPatch are:

- Unzip the RmiPatch.zip into the temporary directory.
- Change directory to your temporary directory.
- Use the command rmipatch install to install.

When you use IE4.0 to view a JMA, you will notice that some of the colors are different. This is due to other shortcomings in the Microsoft Java support, but can't be helped.

7.1.1.3 Netscape Communicator

Netscape Communicator 4.05 or later is required with the Netscape JDK at 1.1.4 or greater. No additional configuration is needed.

7.1.1.4 Performance Considerations

When Nways Java applets are started for the first time, the Web browser may take some time to download all the applet code, which is about 11MB in size. However, once loaded the browser will keep the Java code in its cache, so the next time you use the same Nways Java Management applet, it should start much more quickly.

For better performance we copied those class definition files (applet code) to the Web client machines. To improve the performance of accessing Java Management through the Web you can do the following:

1. Copy the following files located in the directory /usr/CML/JMA/java/websvr/code from the Nways workstation to any subdirectory on the Web browser client.

   ```
   ClientClasses.jar
   CommonClasses.jar
   mlsoft.jar
   ```

2. Set the CLASSPATH environment variable on the Web browser client to include the full path and file name of the class files:

   CLASSPATH=*path*\ClientClasses.jar;*path*\CommonClasses.jar;*path*\mlsoft.jar;

   where *path* is your full path where the class files are located.

3. Start the Web browser and access the Web page at:

   http://*server*/nways/RemoteSubSys.html

   where *server* is the hostname of the Network Management server, and nways is the alias you assigned to the Network Management document directory.

Note

1. You must use the link http://server/nways/RemoteSubSys.html in order to prevent the Web browser from downloading the jar files from the Web server. If you use the link http://server/nways/SubSys.html or follow the link from the NetView page, the jar files will still be loaded from server.
2. This method has worked on Netscape Communicator, MS Internet Explorer, and also Sun HotJava.

From the RemoteSubSys.html page the user can access other Nways Manager pages, either through links on the page or by typing in the specific page name. RemoteSubSys.html must be accessed each time the Web browser is started in order to load the JAR files from the local workstation hard drive.

Note

This method of loading the JAR files locally does not work with the hotjava Web browser.

7.2 Configuring for the Java Device Management

The main component that is required is the Java Runtime Environment (JRE). In our example we used Version 1.1.6. To verify the current version of the installed JRE, execute the commands:

```
java -fullversion or lslpp -h 'Java*'
```

If your JRE version is lower than 1.1.4.4, you need to upgrade or re-install the JRE with the 1.1.4.4 Version or later. The current version is JRE 1.1.6. To get the installable code of the latest JRE version, follow the links:

```
http://w3.hursley.ibm.com/java/codedemos/quickdl.html or
ftp://hurftp.hursley.ibm.com/pub/java/aix
```

The list of Java Device Management components are as follows:

- IBM 2210 Nways Multiprotocol Router
- IBM 2216 Nways Multiaccess Connector
- IBM 8210 Nways Multiprotocol Switched Services (MSS) Server
- IBM 8239 Token Ring Stackable Hub
- IBM 8245 10/100 Stackable Ethernet Hub
- IBM 8271 Nways Ethernet LAN Switch Models E12, E24, F12, F24, 524, 612, 624, 712
- IBM 8273 Nways Ethernet RouteSwitch
- IBM 8275 Ethernet Desktop Switch
- IBM Network Utility
- IBM Switching Modules Series
- IBM MSS Client/Domain Client
- IBM Ethernet and Token-Ring Adapters
- Generic Java device management

These devices need SNMP to be configured to allow Nways Manager to access them. The default Community name is public which normally has authority to get SNMP values but cannot write to a device. So the community name that has both read and write permissions must be used.

7.2.1 Colors on Panels

When the JMA starts up, there is a device graphic view associated with the current device being managed. The device view shows the physical view of the device and the status of its modules and ports. There are colors associated with device status in the device view. The colors are listed below:

- **Green** - Normal.
  - All rows checked in the MIB table have status of Normal (ifOperStatus = up and ifAdminStatus = up).
  - One or more rows that were checked in the MIB table have a status of Normal and the remaining rows checked have a status of Unknown.
- **Yellow** - Marginal. One of the rows checked in the MIB table has a status of Critical (ifAdminStatus = up) but (ifOperStatus = down), and at least one other row has a status of Normal (ifOperStatus = up and ifAdminStatus = up).
- **Red** - Critical. Two or more of the rows checked in the MIB table have a status of Critical (ifAdminStatus = up) but (ifOperStatus = down).
- **Light Blue** - Unknown. One of the following conditions has occurred:

- All of the rows checked in the MIB table have status of Unknown (one of the following conditions):
  - ifAdminStatus = testing
  - ifAdminStatus = up but ifOperStatus = testing, dormant, or unknown
- One or more of the rows checked in the MIB table have status of Unknown and no higher severity level exists for any other rows checked in the table.

- **Light Grey** - Admin-Disabled. MIB-II has been administratively disabled. All rows checked in the MIB table have ifAdminStatus = down.
- **Wheat** - Unmanaged. All rows in the MIB table have a status collection turned off.

7.3 Configuring Java Performance Monitor

Java Performance Monitor (JPM) is a feature of Nways Campus Manager, which allows users to store, display and analyze the values of counter and gauge MIB variables on devices being managed by JMAs. The JMA can be specifically created for a particular devices or it can be the generic JMA, which can manage standard MIBs on any SNMP agent.

JPM uses a three-level architecture:

1. One or more Distributed Intelligent Agents (DIAs) to poll MIB variables on the agent
2. A JPM server which stores polled data in a relational database and processes requests from clients.
3. Clients that display historical data as part of a JMA or imbedded in performance reports.

7.3.1 Collection Values for the JPM

The JPM uses the data values that are collected by a Distributed Intelligent Agent (DIA). These data values are defined by expressions which allow a user of a DIA to collect data from agent systems and store them in histories on the DIA and have them sent to the server for forwarding to specific applications. An expression may be as simple as a single MIB variable, or a complicated combination of the values of MIB variables and constants.

The expressions are specified as a character string. Each string contains tokens and optionally whitespace. The tokens used to build expressions are:

- Mathematical operators:
  - +, -, * / These combine the values of specific MIB variables and constants in the normal way expected mathematically. The resulting data may be any floating point number. These operators can only be used on variables with an underlying numeric data type Counter, Gauge, Integer. * and / have higher presidence than + and -.
  - &&, || - These operators may be used on boolean values.
- Logical operators:
  - >, <, >=, <=, ==, !=, ! These combine MIB values and constants and produce boolean results. The operands may be any combination of MIB values and constants where the data types are numeric. When the values are non-numeric, only == and != are supported.

- &&, || - These operators may be used on boolean values normally the results of the previous logical operators to produce boolean values.

- Unary operators:
  - rate or r - Returns the rate (in units change per second) between the current data collected for a MIB variable and the previous data collected for the same MIB variable. This operator may only be applied to a MIB variable.
  - Delta or d - Returns the difference between the current data collected for a MIB variable and the previous data collected for the same MIB variable. This operator may only be applied to a MIB variable.
  - Constant or c - The following value is a constant value and should not be polled. This need only be used when the value looks like an OID that might be polled. The obvious example is an OID value. The poller has no idea whether you want the value associated with this OID or the OID itself unless you use the constant operator to differentiate.
- Conditionals:
  - if <boolean expression> then <expression> else < expression> or
  - <boolean expression>?<expression>:<expression>

  These two syntaxes are both supported to allow a resulting value to be based on the results of a conditional expression.
- MIB variables:
  - 1.3.6.1.2.1.11.1.0 - Represents the value of this specific MIB variable.
  - 1.3.6.1.2.1.2.2.1.10.* - Represents the values of each of the occurrences of this element in all of the entries in the table.
- Parentheses:

  (,) - Parentheses may be used to arbitrarily group portions of expressions. This may be for clarity, to enforce the order of evaluation, or to override the normal precedence of operations.
- Constants:

  Any numeric constants may be specified, either integer or floating point. For floating point values only the normal numeric form containing a decimal point is supported.

  Other constants are specified using the constant operator and a string representing the value. This value may be of any legal type for SNMP: OCTET STRING, OBJECT IDENTIFIER, BOOLEAN, etc.
- Separator:

  , - Separates expressions that are to be evaluated separately and the results are to be stored and reported together. This may be thought of as a shorthand for multiple expressions, but it has the added advantage of storing only one date object with multiple values instead of storing one date per value. This can potentially save almost one half of the space used to store the history.
- Inserts:

  [value] - When an expression is created any value or portion of a value can be specified using a keyword insert. When the expression is actually applied to polling, an associated table of values must be provided to allow complete MIB

variables and constants to be built by the distributed intelligent agent (polling engine). An example would be for an expression to include: 1.3.6.1.2.1.2.2.1.16.[interface]. When the expression is instantiated it will have a mapping that indicates for variable interface=2, which tells the polling engine to poll for 1.3.6.1.2.1.2.2.1.16.2. Inserts can be used as tokens in an expression (for example, as constants) or at the end of a MIB variable.

An expression may be formed by an arbitrarily complex combination of the preceding tokens. White space between tokens is not required, but it can be included between tokens when desired. White space is defined to be spaces, tabs or end-of-line characters. If the user wishes to collect more than one item of data, multiple expressions may be specified separated by commas.

Nways Manager provides the default performance objects, which are listed in Table 17. The user can add the new interested performance objects by using dpadmin tool covered later in this chapter.

A selection of these values is shown in Table 17 on page 217.

Table 17. Default Performance Objects Defined for JPM

Performance Objects	Expression	Unit
Interface Utilization	((((r 1.3.6.1.2.1.2.2.1.10.* + r 1.3.6.1.2.1.2.2.1.16.*) * 8) / (1.3.6.1.2.1.2.2.1.5.*) * 2) * 100)	Percent
Interface Good Input Pkts	(r 1.3.6.1.2.1.2.2.1.11.* + r 1.3.6.1.2.1.2.2.1.12.*)	Packets/Second
Interface Bad Input Pkts	(r 1.3.6.1.2.1.2.2.1.14.* + r 1.3.6.1.2.1.2.2.1.15.*)	Packets/Second
Interface Discarded Input Pkts	(r 1.3.6.1.2.1.2.2.1.13.*)	Packets/Second
Interface Good Output Pkts	(r 1.3.6.1.2.1.2.2.1.17.* + r 1.3.6.1.2.1.2.2.1.18.* - r 1.3.6.1.2.1.2.2.1.19.* - r 1.3.6.1.2.1.2.2.1.20.*)	Packets/Second
Interface Bad Output Pkts	(r 1.3.6.1.2.1.2.2.1.20.*)	Packets/Second
Interface Discarded Output Pkts	(r 1.3.6.1.2.1.2.2.1.19.*)	Packets/Second
Interface Unicast Input Pkts	(r 1.3.6.1.2.1.2.2.1.11.*)	Packets/Second
Interface Multicast Input Pkts	(r 1.3.6.1.2.1.31.1.1.1.2.*)	Packets/Second
Interface Broadcast Input Pkts	(r 1.3.6.1.2.1.31.1.1.1.3.*)	Packets/Second
Interface Unicast Output Pkts	(r 1.3.6.1.2.1.2.2.1.17.*)	Packets/Second
Interface Multicast Output Pkts	(r 1.3.6.1.2.1.31.1.1.1.4.*)	Packets/Second
Interface Broadcast Output Pkts	(r 1.3.6.1.2.1.31.1.1.1.5.*)	Packets/Second

For a full listing of all the performance MIBs for the JPM see Appendix C, “Java Performance MIBS” on page 409.

7.3.2 DIA Configuration

The JPM polls the devices in the network for performance data and threshold monitoring. For large numbers of devices, the impact of this polling traffic on the network and on the management workstation becomes a concern. To solve this concern, the Nways Manager for AIX include the capability of Java-enabled Distributed Intelligent Agents (DIA) that off load performance information polling from the manager workstation and conserve bandwidth across WAN links. One

copy of the DIA is installed on the AIX Network Management Station by Nways Campus Manager LAN. The JPM will use this default DIA to poll all JMA devices unless they are configured to point to another DIA on the remote workstation.

In addition to polling, DIAs can perform thresholding operations on polled variables. JPM thresholds can be explicitly configured, or JPM can automatically set thresholds based on the mean and standard deviation of previously polled values. By default, the threshold for all objects polled by JPM is three standard deviations above the mean, calculated after 20 polling intervals (and continuously updated thereafter).

When the DIA detects that a configured threshold has been exceeded, it notifies the JPM server. If a JMA is running for the agent which caused the threshold to be exceeded, a performance bullet on the navigation tree of that JMA will change the color to red. When the value returns below the threshold, the performance bullet will return to green. These performance status changes are propagated up the navigation tree, causing higher branches in the tree to be red, yellow, or green, depending on the composite status.

Currently the status changes caused by the DIA detecting a threshold-exceeded condition are not propagated to the IP topology on either NetView or Nways Workgroup Manager. In future releases of Nways Manager, these status changes will be propagated to the IP topology to allow status-at-a-glance for threshold conditions.

The JPM server does send a trap indicating that the threshold has been exceeded to the local workstation, so the trap can be viewed on the events desk.

DIAs are installed on remote workstations in the network. They are then configured to poll for performance data and only report back to the management workstation when a threshold has been exceeded or polling results are requested. Thus, both the management workstation's involvement in polling and network traffic due to polling are reduced.

Since data collection using the DIA is distributed among several systems it is possible for one of the systems to be stopped without all of the systems stopping. The DIA and the JPM are designed to recover from failures of the server, the DIA or both. Under certain loads, if the server is restarted and one or more DIAs have continued running, there may be some delay in completing the connection between one or more DIAs and the new server. This is due to load on the server and will correct itself. The DIAs will re-establish the connection with the server and the states of the server and DIAs will be synchronized.

The DIA code is not automatically installed on each remote polling workstation. Instead, the code is provided on the Nways Manager workstation. A simple script file is used on the remote workstations to start a Java run-time session and load a local Java class that downloads the DIA code from the HTTP server. The script file also defines the Nways Manager workstation to which the DIA will report polling data.

7.3.2.1 System Requirements for Remote DIA Workstation

The use of remote DIAs require additional licenses that come in tiers of 1, 5 or 10 at an adjusted price. The code is delivered with the Nways LAN component, but can legally only be used on the network management server without additional

licenses. The DIA requires a JRE Version 1.1.4 or later. If the target workstation does not have a suitable environment, Version 1.1.4 of the JDK or Version 1.1.4 of JRE for the target operating system must first be installed.

The DIA will run on the following operating systems:

- Microsoft Windows NT Version 4.0
- Microsoft Windows 95
- IBM AIX Versions 4.1 and 4.2

Note

The DIA has been tested on Windows 95. The installation and configuration is similar to that on Windows NT. We do not recommend running the DIA on Windows 95 due to memory management problems associated with Windows 95. These problems result in the total memory utilization of Windows 95 increasing to the total virtual memory defined.

7.3.2.2 Remote DIA Installation

The installation steps of the DIA on remote workstations is described in "Remote Distributed Intelligent Agents (DIAs)" on page 52.

In our scenario the remote DIAs are installed on three workstations: NT_RV1 , WIN9501 and NT_NWAYS1. After installing the DIA on the remote workstations, you must run the command `/usr/CML/JMA/bin/dpadmin`.

to configure the polling IP addresses for the remote DIAs. Table 18 shows the list of IP addresses polled by each DIA workstation.

Table 18. DIA Polling Addresses List

DIA Workstation	DIA's IP Address	Polling List
WIN9501	192.168.5.125	192.168.5.0 - 192.168.5.255
NT_RV1	9.24.105.112	9.24.105.70 9.24.105.90 9.24.105.114 192.168.4.0 - 192.168.4.255
NWAYS_NT	192.168.254.113	192.168.253.0 - 192.168.254.255
rs600033t	9.24.104.246	(All range excluded from above remote DIA) 0.0.0.0 - 9.24.105.69 9.24.105.71 - 9.24.105.89 9.24.105.91 - 9.24.105.113 9.24.105.115 - 192.168.3.255 192.168.6.0 - 192.168.252.255 192.168.255.0 - 255.255.255.255

The following procedure shows the steps to configure the IP addresses for the remote DIAs:

1. Start the Performance Management configuration by entering:

   `/usr/CML/JMA/bin/dpadmin`

   The DIA Topology panel will appear with new installed remote DIAs appearing in the top-left hand corner, (see Figure 201). If these do not appear, click on the **Refresh** button.

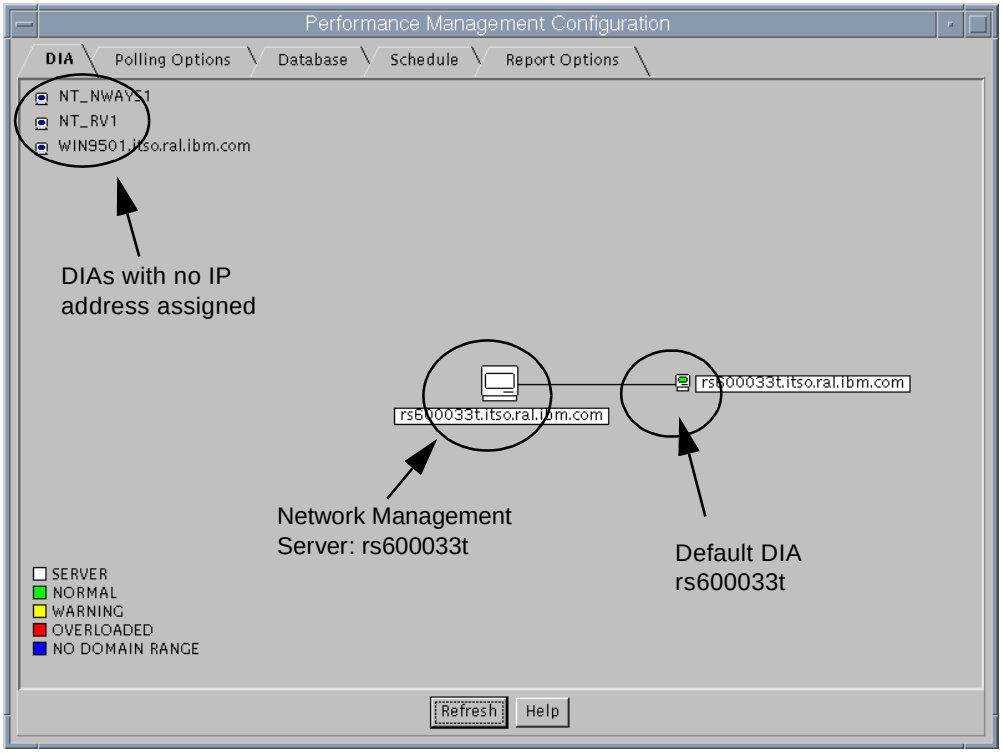


Figure 201. DIA Topology with Unconfigured Remote DIAs

Important

If the runDIA script is successful on the remote workstation (message "Bound successfully to the server ...") but no DIA icon is displayed on the topology panel, you must check the TCP/IP host name on the DIA workstation to ensure that it is *exactly* the same as host name defined in the DNS or the local /etc/hosts file.

2. Using the left mouse button, drag the remote DIA icon and drop it over the white Network Management Server icon. You should see the DIA's IP configuration screen. Figure 202 shows the configuration for NT_NWAYS1.

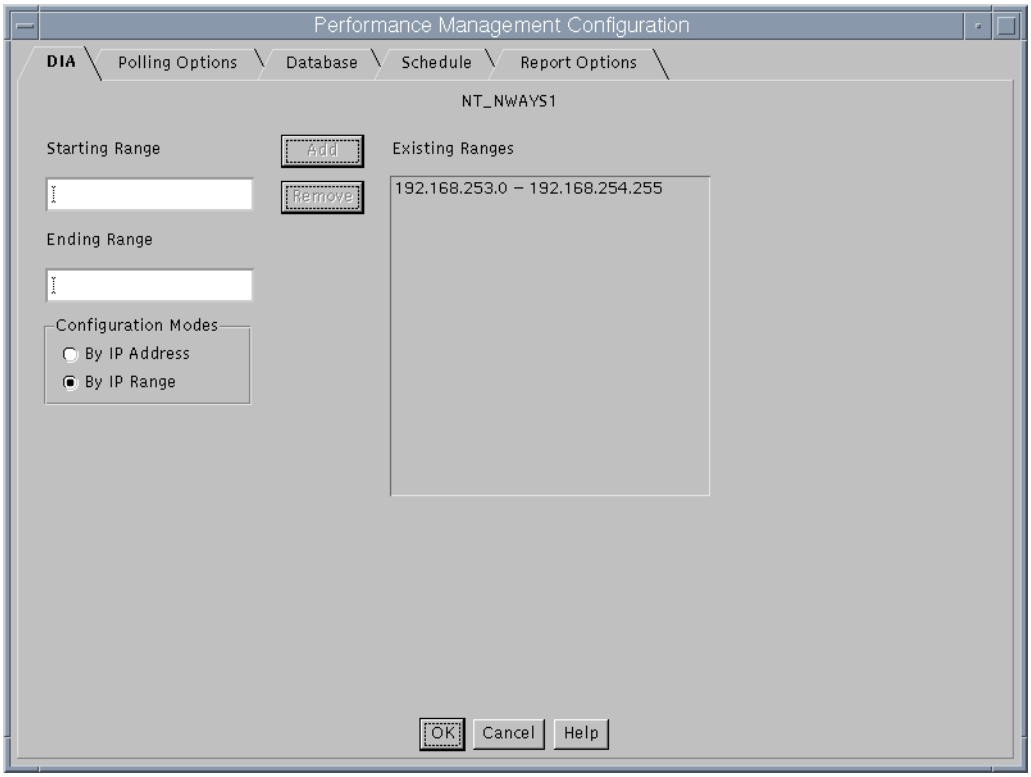


Figure 202. Configuring IP Address Range

3. From this screen you can assign the IP address of target nodes to be polled by NT_NWAYS1. You can enter the IP address either by specifying an IP address or IP address range. We set the IP address range of 192.168.253.0 - 192.168.254.255 for the NT_NWAYS1. These steps are:
   - Select Configuration Modes as **By IP Range.**
   - Enter the lower IP address of `192.168.253.0` as the Starting Range.
   - Enter the upper IP address of `192.168.254.255` as the Ending Range.
   - Click on **Add** to accept the range into Existing Domain.
   - Click **OK** when finished, Figure 203 will appear.

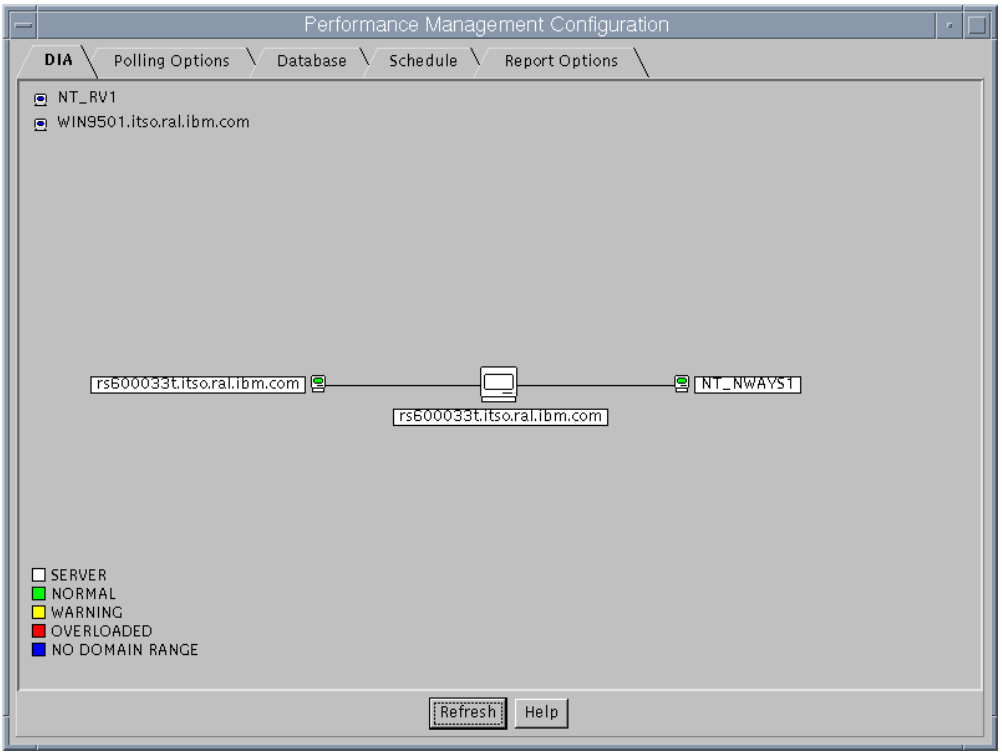


Figure 203. DIA Topology after Configuration

4. For the NT_RV1 workstation we assigned the IP addresses for the MSS1, MSS2, and 2210_LOCAL devices to be polled by this DIA. The steps of configuration are:
   - Drag and drop the icon NT_RV1 over the Network Management Station rs600033t to bring up NT_RV1's IP address polling screen (see Figure 204).
   - Select Configuration Modes as **By IP address.**
   - Enter the MSS1 address `9.24.105.114` as IP Address then click on **Add.**
   - Enter the MSS2 address `9.24.105.90` as IP Address then click on **Add.**
   - Enter the 2210_Local address `9.24.105.70` as IP Address then click on **Add.**
   - Select Configuration Modes as By IP Range.
   - Enter the lower IP address `192.168.4.0` as Starting Range.
   - Enter the upper IP address `192.168.4.255` as Ending Range.
   - Click **Add** to accept the range into existing domain.
   - Click on **OK** to finish.

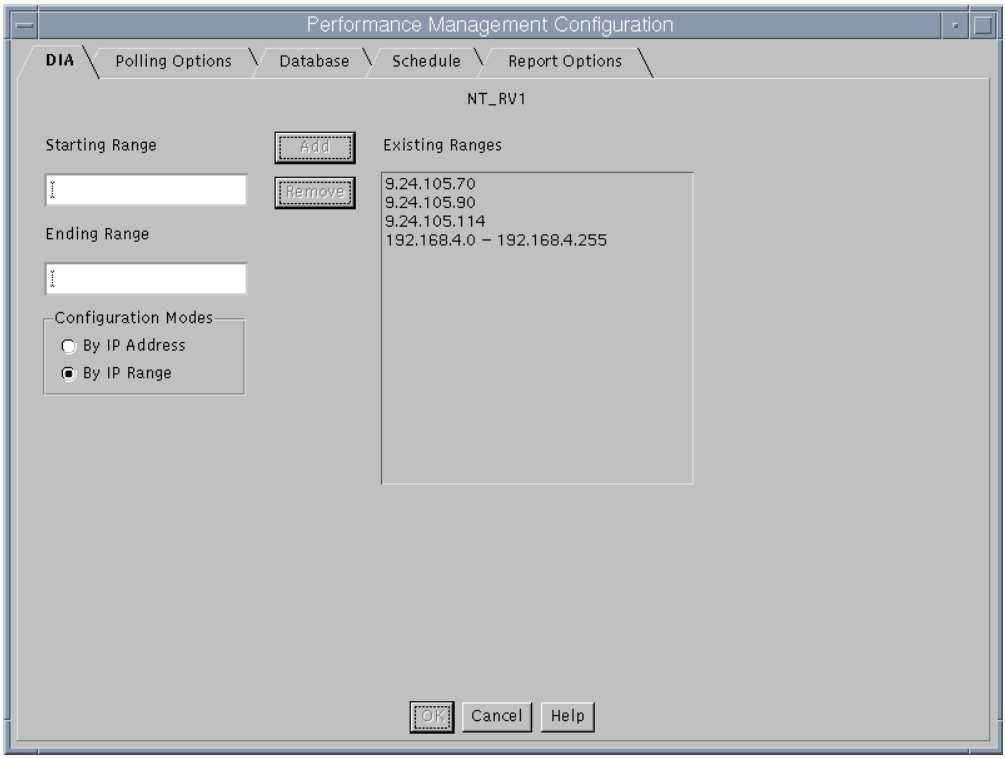


Figure 204. Configuring Specific IP Addresses

5. Repeat step 2 for the WIN9501 workstation and add the IP address range of 192.168.4.0 - 192.168.5.255 into the existing domain.

After configuring the three remote DIAs, the DIA topology will display as Figure 205. Each DIA icons will show the color of its workload:

- Green - Normal
- Yellow - Warning
- Red - Overloaded

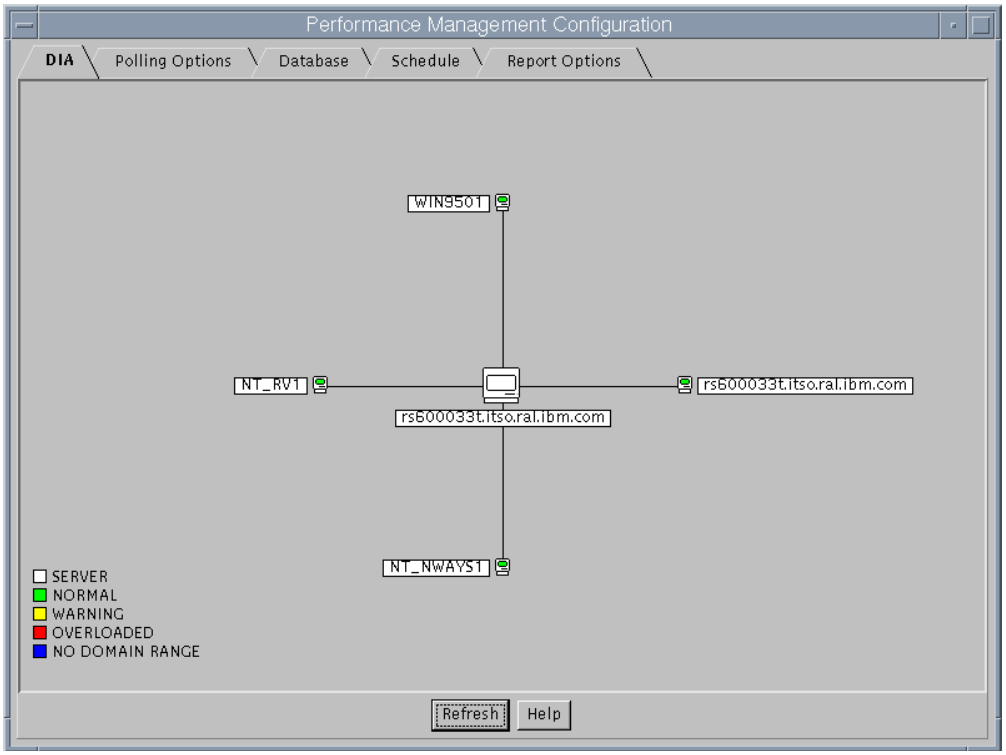


Figure 205. DIA Topology with DIAs Running

Note: You can also reconfigure the IP address or IP range for each DIA by double-clicking on the DIA icon on the DIA topology while holding the **Ctrl key**.

If you double-click on any DIA icon, you will see that DIA status as shown in Figure 206 on page 225.

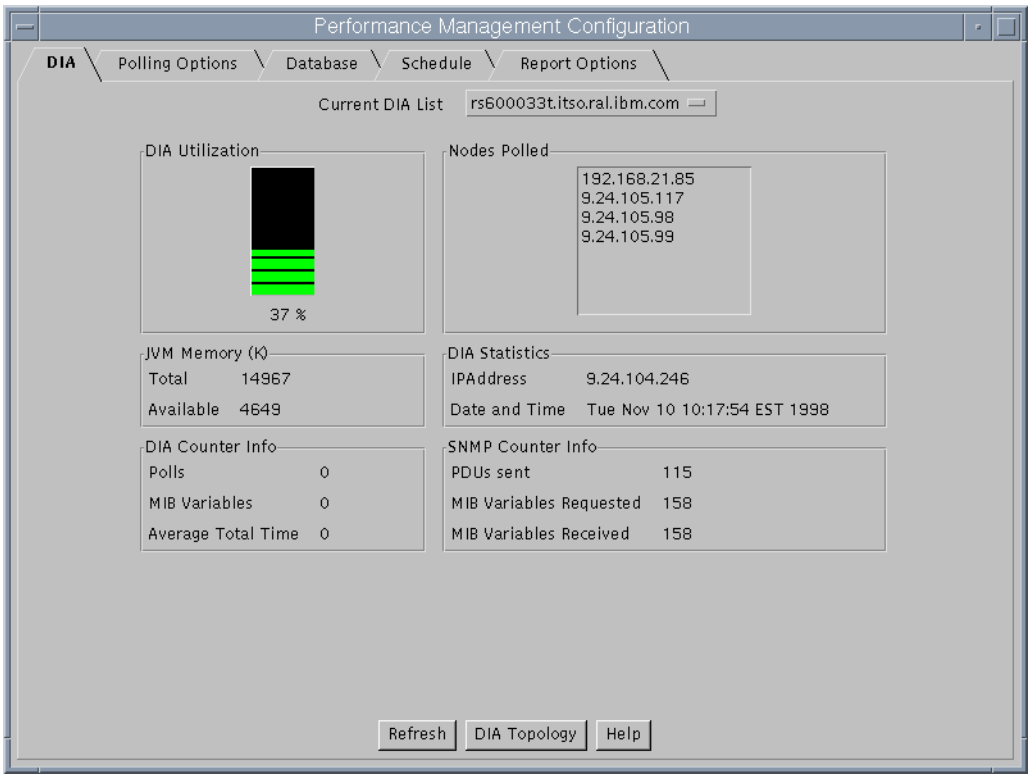


Figure 206. DIA Workload Status

7.3.3 JDBC Database Configuration

7.3.3.1 Database Considerations

When first installed, JPM does not use a database. A limited amount of historical data is stored in memory, and this data is lost when new data is received. The cache is wrapped when it overflows and no relational database is configured for Nways JDBC connectivity. All data collected so far will be lost and the collection will begin again.

To start storing information in the database, you must specify the database location and drivers using the dpadmin/dpconfig tool.

You should ensure that you have adequate free space on the database file system before starting database storage with JPM. The amount of space needed is highly dependent on the number of agents being polled and the polling interval. As a starting point, polling 20 agents with the default 20 minute polling interval, a 250MB file system could be filled up in 3-4 weeks of continuous polling. IBM recommends that you monitor the amount of storage consumed by the JPM database for several weeks after you start using the database, and develop a database maintenance plan based on your observations.

JPM uses a JDBC-compliant database to store the historical data that it captures. IBM has successfully tested JPM with the following databases:

- DB2 Universal Database
- Oracle
- Sybase
- Microsoft SQL Server (Nways Workgroup Manager for NT)

With each database, you must unzip the database drivers (Java class files) provided by the database manufacturer into the directory:

```
/usr/CML/JMA/java/websvr/code
```

7.3.3.2 IBM DB2 Universal Database

With IBM DB2 Universal Database, no special customizations are needed to achieve adequate performance.

- Driver Name: COM.ibm.db2.jdbc.app.DB2Driver
- Database URL: jdbc:db2:IBMNMPDB

7.3.3.3 Sybase

Use the following driver name and database URL when instructing JPM to begin using a database:

- Driver Name: com.sybase.jdbc.SybDriver
- Database URL: jdbc:sybase:Tds:<hostname>:5000/IBMNMPDB

7.3.3.4 Oracle

Use the following values in the fields Driver Name and Database URL on the database page:

- Driver Name: oracle.jdbc.driver.OracleDriver
- Database URL: jdbc:oracle:oci8:@ibmnmpdb.world

7.3.4 JPM Server Configuration

The user can customize the MIB objects that are presented on the JMA when a bullet labeled **Performance** is selected on the JMA navigation tree. IBM has made default selections that provide basic information about the interfaces, protocols and system elements in the navigation tree. However, because of the limited capacity of the JPM server, some MIB counters and gauges that may be of interest to many users are not polled as part of the default configuration. You can use the dpadmin/dpconfig tool to customize the data which is displayed under a Performance bullet in the JMA navigation tree.

In this section, the JPM data concepts are explained, and tips are presented for using the dpadmin/dpconfig tool to modify the default JPM customization.

JPM organizes MIB objects hierarchically as follows:

- Performance Object - A MIB object or mathematical combination of MIB objects (see Table 17 on page 217).
- Graph - One or more performance objects to be shown on the same graph. All performance objects on the same graph should have the same units (for instance octets/second), but JPM cannot enforce this.
- View - One or more graphs that are displayed on the same notebook page by the JPM.
- Template - All the notebook pages that are grouped under a single Performance bullet in the navigation tree.

The IBM-provided default configuration of these objects are stored in text files found in the directory /usr/CML/JMA/java/properties/startup. It may be useful to customize two aspects of JPM performance which affect all these default objects

by modifying these text files prior to beginning JPM polling. These two properties are:

- The polling interval used by the DIAs for polling all performance objects
- The time period covered on a graph when viewing performance data in a JMA

Note

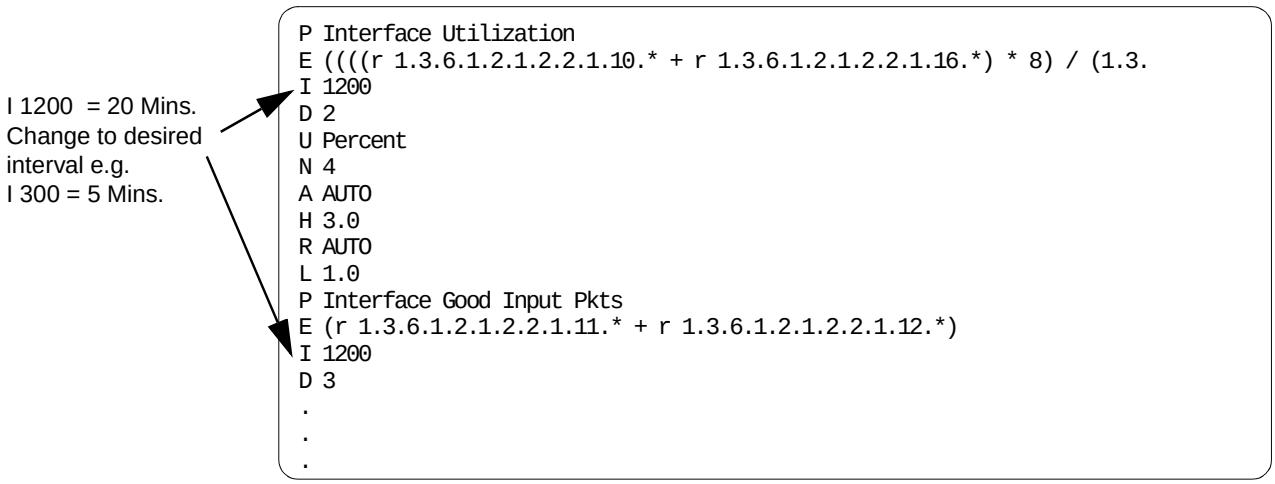
If you follow these instructions and modify the default configuration, you will lose all data polled and stored in the database. This shortcut should only be used prior to starting all polling with JPM.

The default polling interval for all performance objects is 20 minutes. That means that when viewing a graph containing a particular performance object, points on the graph will be 20 minutes apart. To modify the polling interval for all performance objects, do the following:

- Make a backup copy of all files in the directory:

  `install_dir/java/properties/startup`

- Edit the file pollobj.def located in the start up directory.
- Do a global search and replace, changing the string `I 1200` to `I n`, where n is the number of seconds you wish to use for a polling interval.



To reload the default configuration, do the following. You will lose all historical data stored in the database, as well as any configuration changes made so far. Follow these instructions to modify the default configuration:

- Exit Nways Workgroup Manager for NT, or on AIX, stop the JMAintegrator daemon by issuing:

  `/usr/OV/bin/ovstop JMAintegrator`

- Remove the directory and all files and subdirectories:

  `/usr/CML/JMA/java/properties/config`

- Remove the IBMNMPDB database, and create a new database. With DB2 on AIX, this is done by entering the db2 command environment by issuing:

  ```
  db2
  drop database IBMNMPDB
  ```

```
create database IBMNMPDB
```

- Restart Nways Workgroup Manager for NT, or on AIX, restart the JMAintegrator daemon by issuing:

  ```
  /usr/OV/bin/ovstart JMAintegrator
  ```

You may change the polling interval later for individual polling objects by using the dpadmin/dpconfig tool. Keep in mind the total load placed on DIAs by polling and the volume of SNMP traffic generated in your network, and recognize that a smaller polling interval increases this load. The default View Length is 4 hours. This means that by default, when viewing a graph by selecting a Performance bullet in a JMA navigation tree, data is retrieved for the last 4 hours. To modify the default View Length, do the following:

- Make a backup copy of all files in the directory:

  ```
  install_dir/java/properties/startup
  ```

- Edit the file view.def in the start up directory.
- Do a global search and replace, changing the string `R 4,2` to `R n,x`, where n is the length you wish to change the View Length to, and x is the units, with 1 representing minutes, 2 representing hours, 3 representing days, and 4 representing weeks.

R 4,2 = four hours.
Change to desired
period e.g.
R 6,2 = six hours.

```
V Interface Utilization
R 4,2
G Interface Utilization
T 0
U Percent
P Interface Utilization
V Interface Packet Quality
R 4,2
G Interface Input Quality
T 0
U Packets/Second
P Interface Good Input Pkts
P Interface Bad Input Pkts
P Interface Discarded Input Pkts
.
.
```

After the default JPM configuration has been loaded, you can use the dpadmin/dpconfig tool to modify the JPM configuration. This tool can be launched two ways:

1. From any JMA, select the **Performance Configuration** option under the **System** and **General** branches of the navigation tree. Although you are running this from a single JMA, any changes you make will affect all JMAs that use the object definitions you modify.

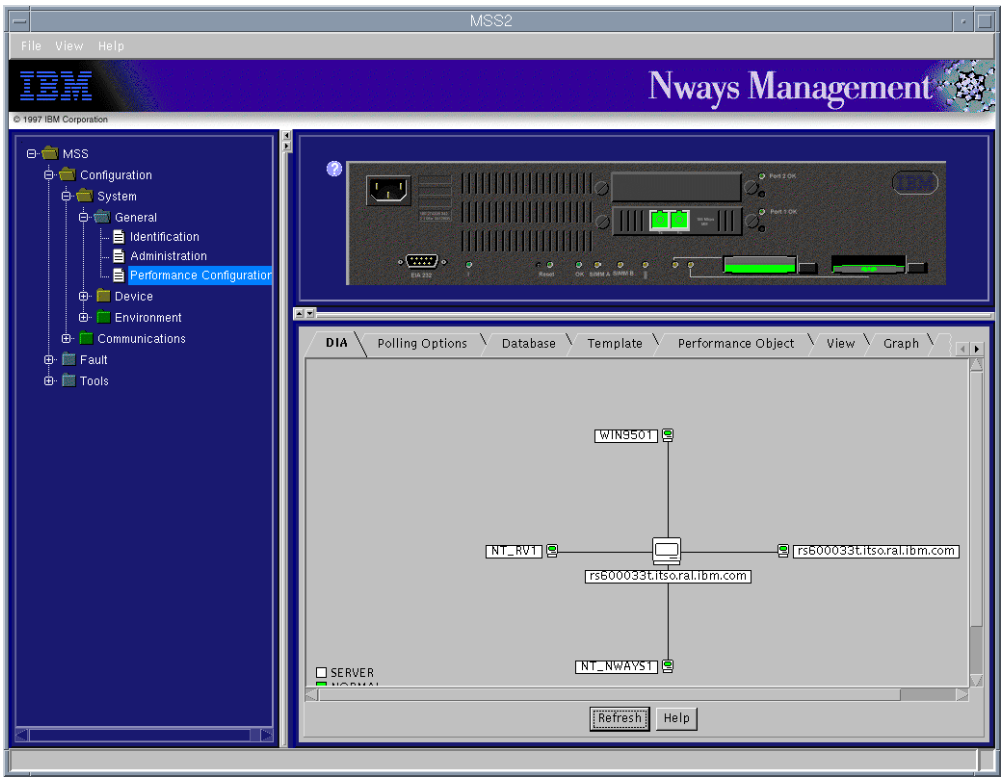


Figure 207. Launching the dpadmin Tool from JMA

2. From a command prompt on the Nways Manager workstation, issue the command:

   ```
   /usr/CML/JMA/bin/dpadmin <hostname> <web_browser_name>
   ```

   The second parameter is only necessary if you wish to view help files while running DpAdmin.

Note

By launching the dpadmin tool from the command line, you will see only the tabs: DIA, Polling Options, Database, Schedule, and Report Options. To configure the Template, Performance Object, View, and Graph, you must issue the command:

```
/usr/CML/JMA/bin/ dpconfig <node>
```

Where <node> is the hostname of the device being configured. Figure 207 on page 229 shows the result of the command dpconfig MSS2.

The tabs on the DpAdmin notebook allow you to configure a wide variety of behavior associated with JPM:

- DIA Monitor - This page is used to configure and monitor Distributed Intelligent Agents. The page that is first displayed shows a graphical representation of the DIAs currently configured. Double-clicking on a DIA will show you status for that DIA. Double-clicking on a DIA while holding the Control key will allow you to configure nodes for that DIA or create a configuration for a new DIA.

- Polling Options - This page is used to discontinue polling a network agent after polling has been started by launching the JMA for the device. Once a JMA is launched, polling continues for that agent whenever the JMA server is running. Selecting an agent on this screen and selecting **Stop polling this host** is the only way to discontinue polling for a particular agent.
- Database Configuration - This page is used to tell JPM about which relational database to use. The JDBC driver and Database URL fields are filled in with the correct information for using DB2. For other databases, use the information supplied by the database manufacturer, using IBMNMPDB for the database name. Remember that you must manually create a database named IBMNMPDB, since the JDBC API does not allow Nways Manager to create a database programmatically.
- Schedule - This page is used to create periods of time during a week for which different thresholding criteria are used. This schedule only applies for performance objects that use JPM's auto-thresholding mechanism. Click on the **Help** button on this page for detailed information on how to create a polling schedule.
- Options - This page is used to modify reporting options. The report options define a weekday to the JPM report programs (see 7.6, “Nways Java Management Reports” on page 251).
- Template - Templates are the highest level of the JPM data structure hierarchy, and have a one-to-one correspondence to a Performance bullet which is an endpoint in the JMA navigation tree. You cannot create additional templates, so all JPM views must fit in the navigation tree at one of the existing points. The template names use a dotted notation, which may seem somewhat cryptic, but the last segment of the name is the same as the folder on the navigation tree under which the Performance bullet appears. From this page in the DpAdmin notebook, you can add views to a template. You also must add all performance objects contained in any views you add in order to begin polling the performance objects.

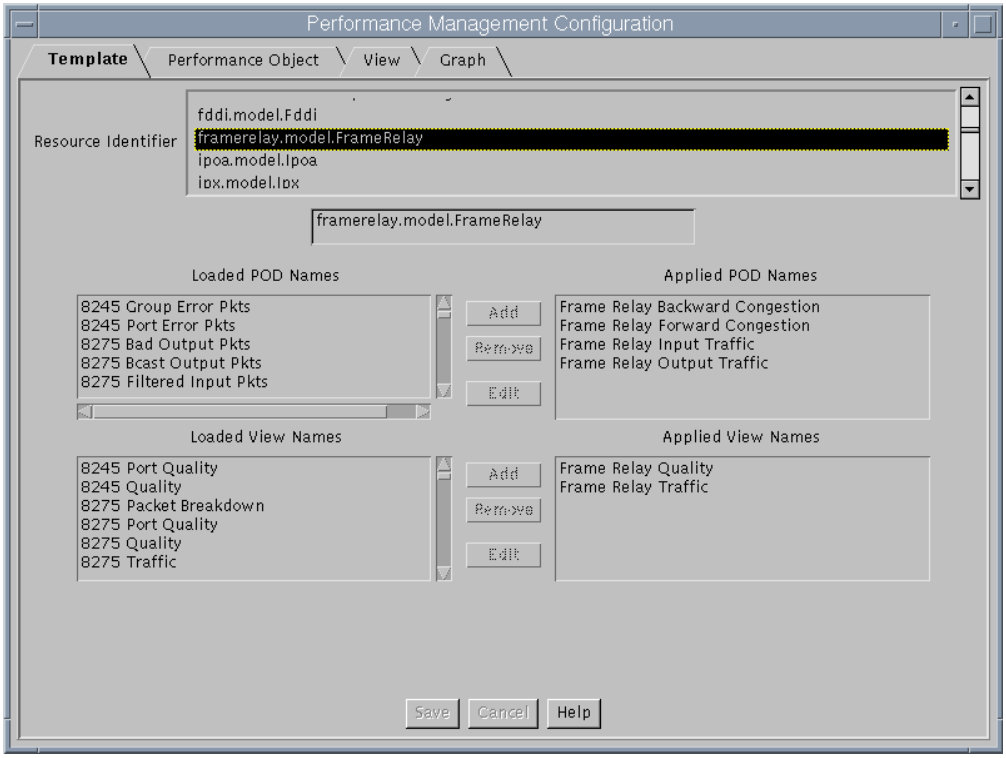


Figure 208. Example Template: framerelay.model.FrameRelay

- Performance Object - This page is used to create or modify the performance objects that are polled by JPM. Select the **Help** button on this page for detailed information about what the fields on this page mean (see also 7.3.1, “Collection Values for the JPM” on page 215). In order to define new performance objects you must know the object identifier (OID) for any MIB objects that the performance object is based on.

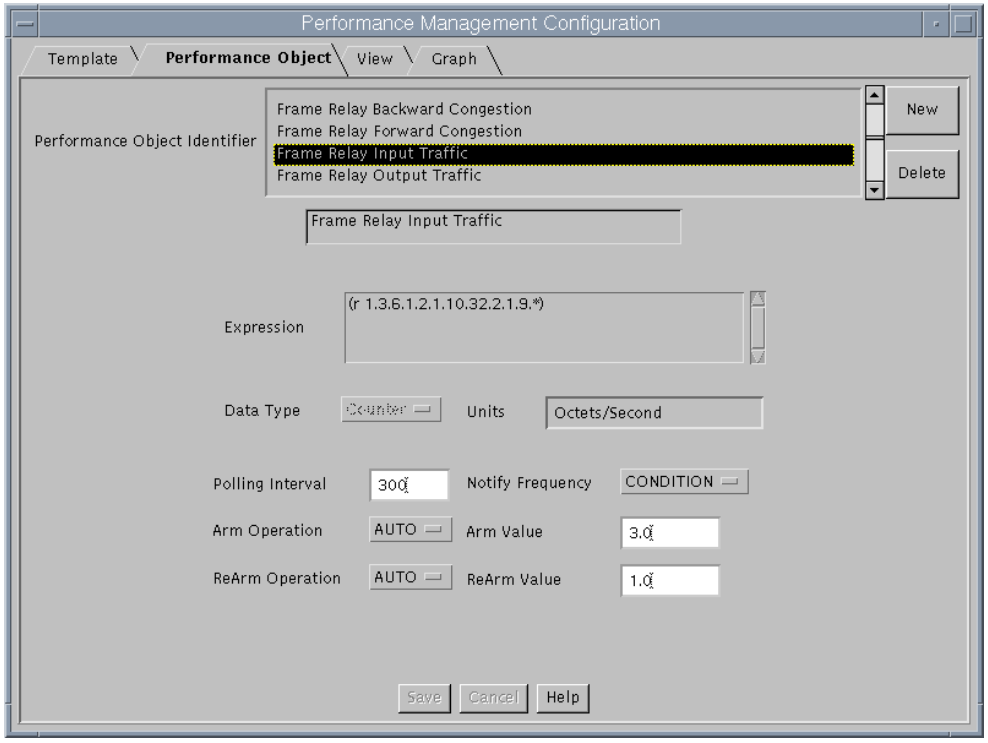


Figure 209. Example Performance Object: Frame Relay Input Traffic

- View - This page is used to create or modify views. You may combine any Graphs that exist (and are displayed in the left-hand list box) to create views (see Figure 210).

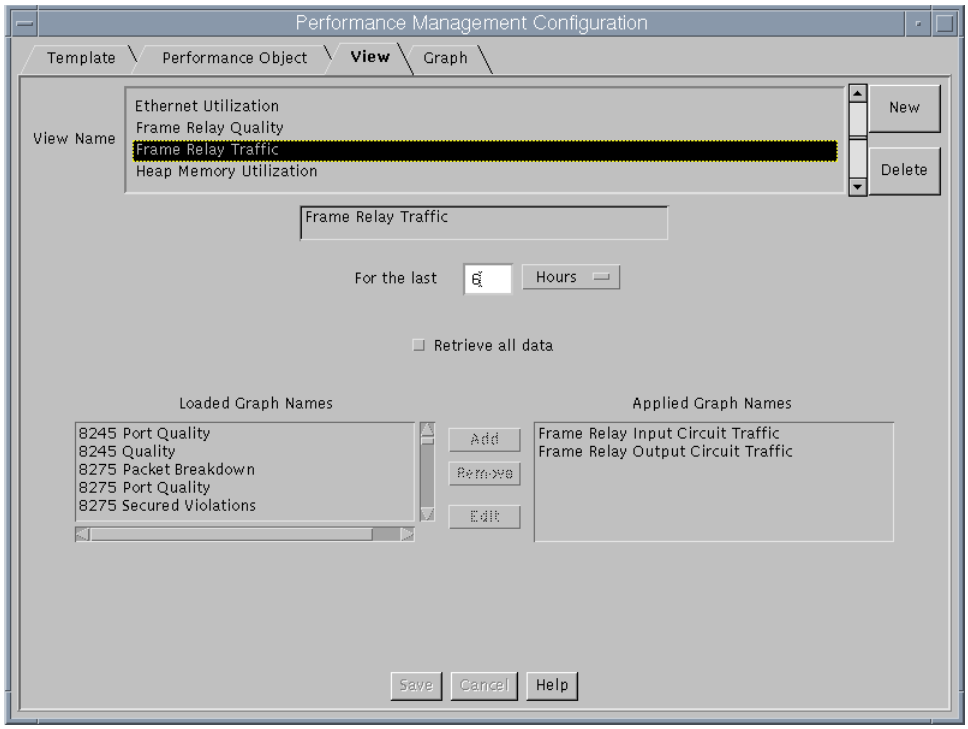


Figure 210. Example View Configuration: Frame Relay Traffic

- Graph - This page is used to create or modify graphs. You may combine any performance objects that exist (and are displayed in the left-hand list box) to create graphs (see Figure 211).

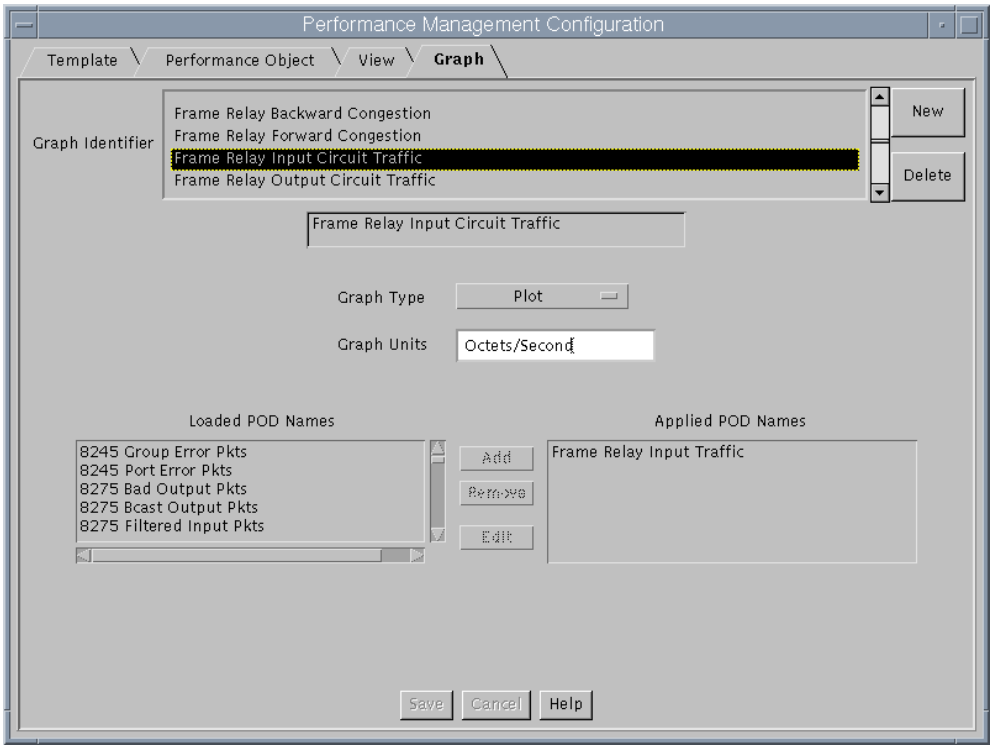


Figure 211. Example Graph Configuration: Frame Relay Input Circuit Traffic

7.4 Navigation for Java Management Application

The JMA can be started by double-clicking on the device icon from the NetView submap. Figure 212 shows the JMA view of the 2210.

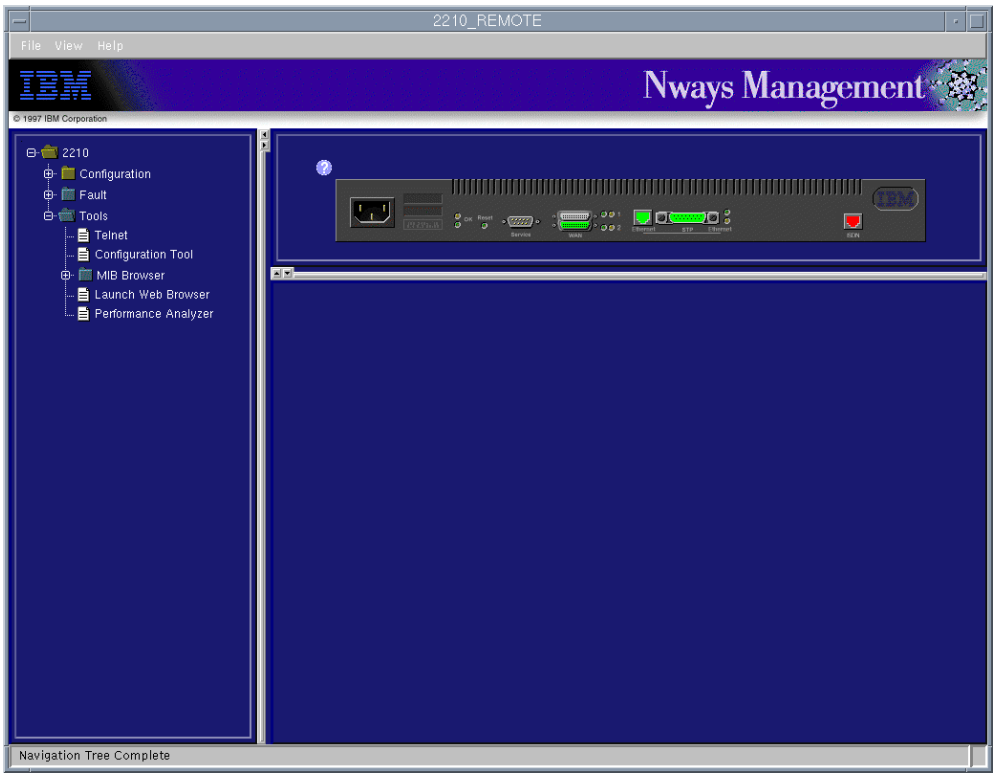


Figure 212. JMA 2210 (JMA Device)

For the generic Java-based device, click on the device icon in the NetView submap then select **IBM Nways Java: Open Java device View** from the **Tools** menu.

7.4.1 The JMA Navigation Tree

The Navigation tree uses several icons to represent the monitored resources:

•Folder - A higher level resource that represents one or more dependent items. The folder at the top of the tree, for example, usually represents the device itself. Other folders at subsequent levels might represent configuration information or fault information. Within each folder are items that make up part of the overall folder of information. The status indicated for a folder is calculated from the statuses of its immediate dependent items. Click on the plus (+) next to a folder to see and take action on the items within the folder.

•Ball - A dependent resource, such as a port on the device, that has a status associated with it.

•Page - A dependent resource that consists of information only, such as configuration information. This resource may or may not allow user changes, depending on the item and the device being managed. This resource has no status associated with it.

7.4.1.1 Navigating

The following list details some of the features that can be performed from the JMA:

- Expand folders by clicking on **+** next to the icon to display dependent items.

- Collapse folders by clicking on **-.**
- Double-click on the folder itself to display the information panel.
- Double-click on a ball to display a detailed information panel about the selected resource and its status.
- Double-click on a page to display a detailed information panel relating to the selected item. Some of the information panels provide the ability to make configuration changes; others are display only.
- Some icons in the navigation tree correspond to hot spots in the device view, and display the same status information. To view status information for those resources, double-click on the resource's icon in the navigation tree or on the hot spot in the device view.
- Right-clicking on items on the device graphic or in the navigation tree produces pop-up menus with special functions. Right-clicking in the navigation tree area itself produces another pop-up menu with more special functions.

7.4.2 Navigation Tree Resource Colors

The status of a resource is indicated by the following colors:

- **Green** - Normal. The object is in a normal operational state.

  At the folder level, Normal indicates either:

  - All dependent items are in Normal status.
  - One or more dependent items are in Normal status and the remaining items have status of Unknown, Unmanaged, or Admin Disabled, as applicable.

- **Yellow** - Marginal. The operation of the object is impaired but the object is still functional.

  At the folder level, Marginal indicates either:

  - All dependent items are in Marginal status.
  - One dependent item is in Critical status and at least one other dependent item is in Normal or Marginal status.
  - At least one dependent item is in Marginal status and no dependent item is in Critical status. The remaining dependent items are in Normal, Unknown, Unmanaged, or Admin Disabled status, as applicable.

- **Red** - Critical. The object is not functioning.

  At the folder level, Critical indicates that two or more dependent items are in Critical status.

- **Light Blue** - Unknown. The object status cannot be determined.

  At the folder level, Unknown indicates either:

  - The folder has no dependent items that have status.
  - All dependent items have status of Unknown.
  - The status of dependent items are not all the same, and none of the dependent items status are Normal, Marginal, or Critical.
  - Status has been collected for dependent items at some point, but status collection was turned off for all table rows by unchecking each row individually.

- **Light Grey** - Admin Disabled. The object has been administratively disabled.

At the folder level, Admin Disabled indicates that all dependent items have been administratively disabled.

- **Wheat** - Unmanaged. Status information currently is not being collected on the object. For many dependent items you can specify whether or not to collect status.

  At the folder level, Unmanaged indicates that none of the dependent items have status collection turned on. Either status has never been collected on objects in the table, or status collection was turned off for the entire table by clicking the Status column in the table heading (upper-left corner of the table).

7.4.2.1 Setting Status Collection On or Off

To conserve resources and reduce processing time, you can turn off the collection of status information for some items.

Status collection can be turned on or off only for objects that are rows in MIB tables. To view or change the status collection setting, click on the dependent object in the navigation tree to display the object's status information window.

If status collection can be set, the left column in the table is reserved for that purpose. A check mark in the left column of a row indicates that status collection is on for that object. Turn check marks on or off by clicking in the leftmost column of a row. To turn off all check marks and unmanage the entire table, click on the Status column in the table heading (upper-left corner of the table). When some rows are checked and others are not, the status reported reflects only the checked rows.

Turn checkmark off to stop status collection for that object.

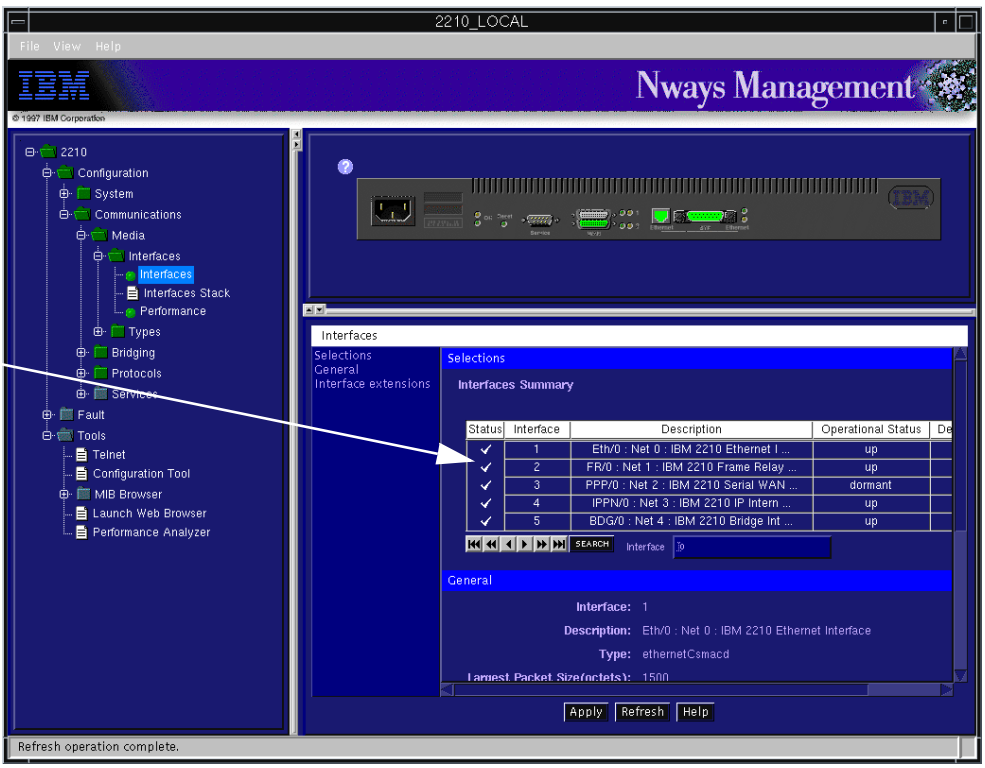


Figure 213. JMA Example: Setting Status Collection On or Off

7.4.3 Starting JMA from a Web Browser

To start the JMA from Web Browser, select either one of the following methods:

- Directly browse the following link
  - http://server/nways/SubSys.html or
  - http://server/nways/RemoteSubSys.html

  where *server* is the Nways Manager Server and nways is the alias name of the Nways Web page directory.

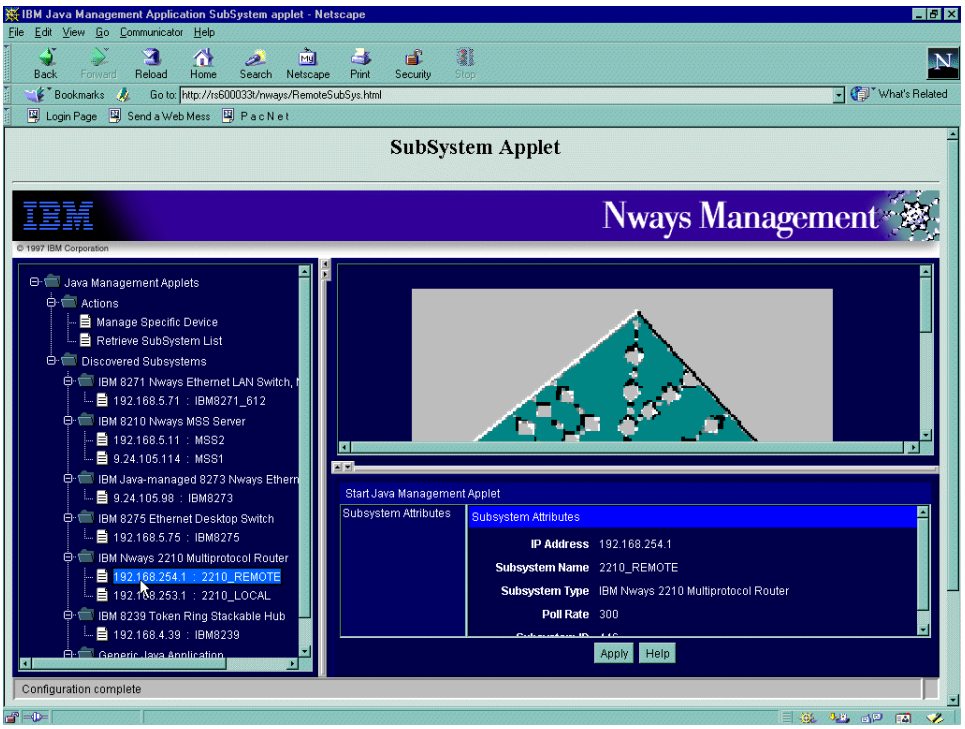


Figure 214. Accessing JMAs Using a Web Browser

Figure 214 shows the subsystem applet running in a Web browser. You can manage the devices by clicking on **Manage Specific Device** from the navigation tree then entering the IP address for the device in the Information area. Alternatively you can click on **Retrieve Subsystem List**, which will display all the discovered subsystems for example, if you want to manage the 2210_Remote from this Web page. Clicking on **Apply** will start the JMA, we selected the 2210_Remote device.

Note: For Web accessed JMA and JMA on Nways Server, all functions are the same except that you cannot launch the Performance Analyses.

7.5 Examples Using the Java Management Applications

This section shows examples of using the JMA and the JPM. In the first example we use the 2210 router.

7.5.1 2210 JPM Example

From the 2210 JMA window, we can perform management functions such as configuring system parameters, monitoring performance information and viewing the status of its interfaces.

Figure 215 shows the 2210 Heap Memory Utilization for a six hour period. This view of system performance is defined as a performance template.

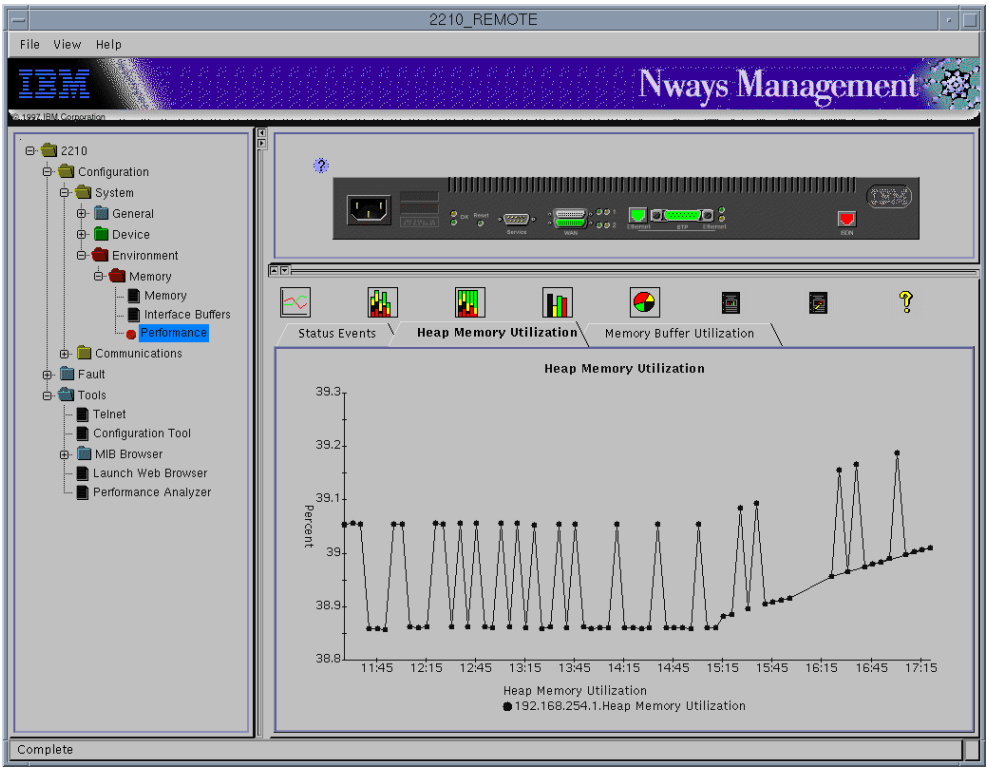


Figure 215. 2210 Heap Memory Utilization

If you go to the device interface on the navigation tree, you can view and control the interfaces as shown in Figure 216. From here you can set the status up or down.

,

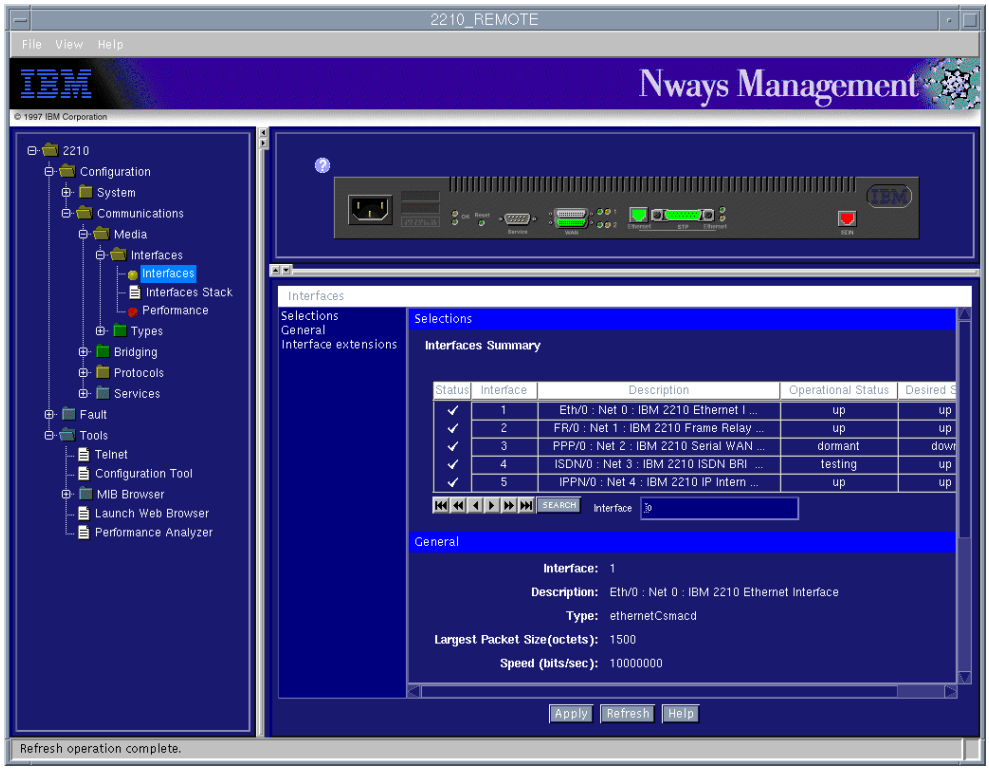


Figure 216. 2210 Interface List

The interface utilization is shown in Figure 217 on page 239.

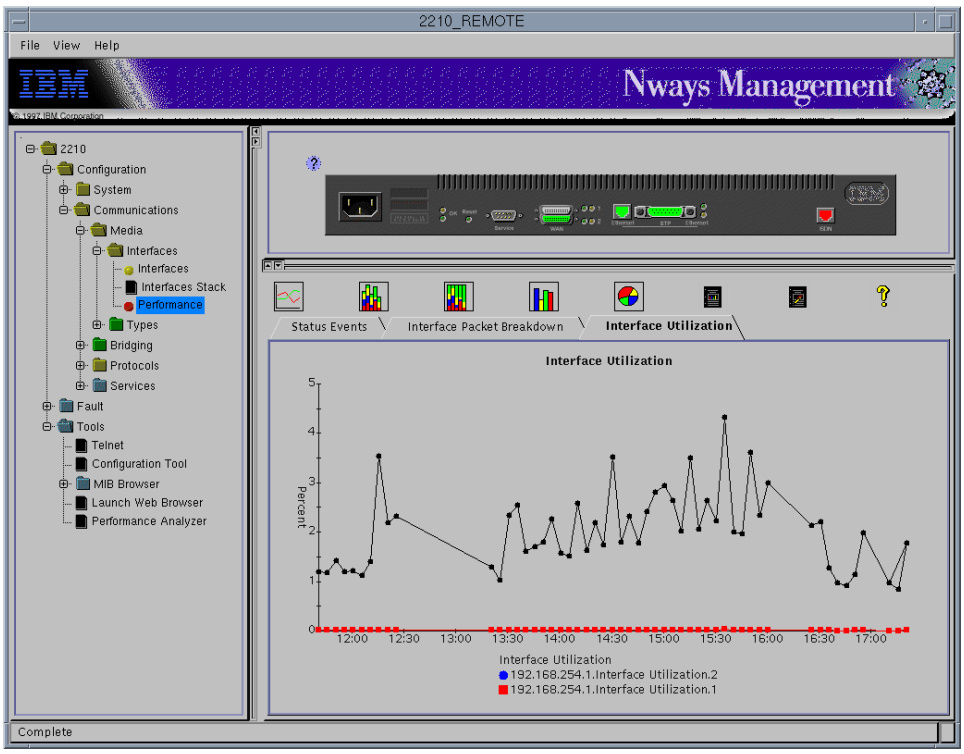


Figure 217. 2210 Interface Utilization

Figure 218 shows the IP Traffic on the 2210 which can be viewed by clicking on the Performance bullet located under the IP folder. There are three graphs defined in this view:

- IP Input Packets
- IP Output Packets
- IP Forward Packets

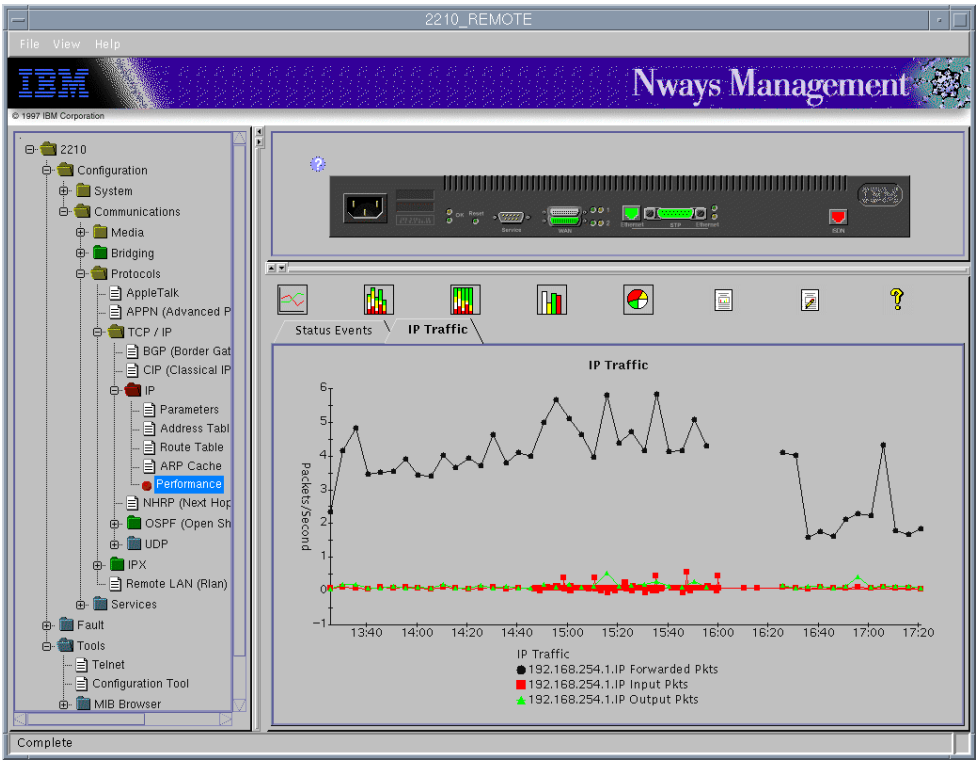


Figure 218. IP Traffic on 2210

You can add more graphs into this view or create another view then add this to the performance bullet by clicking on **Configuration->System->General->Performance Configuration.**

From the performance screen you can select a view that can be used to create a report. This is done by clicking on **add to report** icon. The screen shown in Figure 219 will be displayed. This is explained in more detail in 7.6, “Nways Java Management Reports” on page 251.

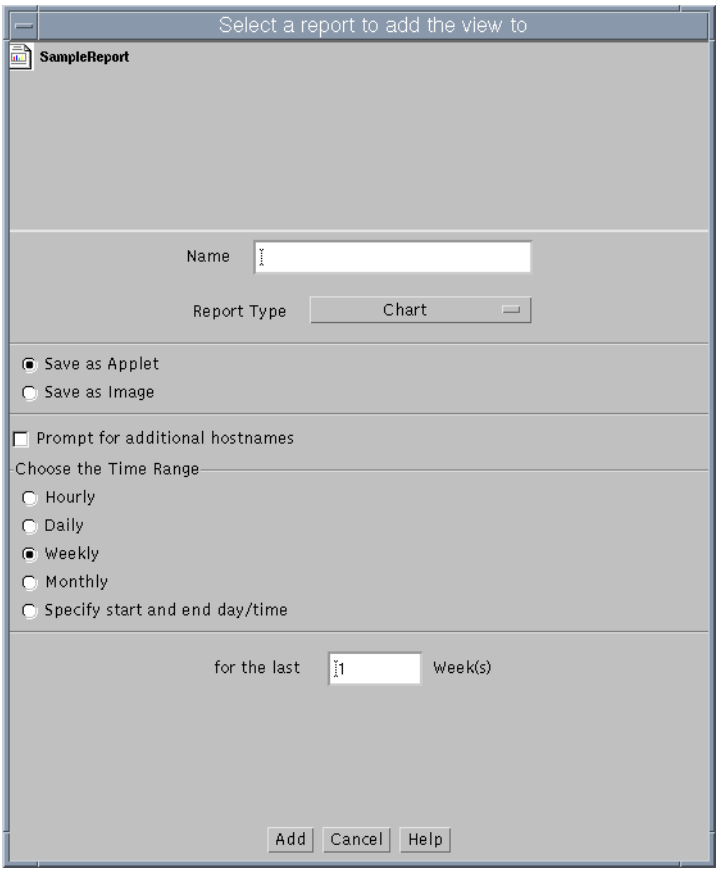


Figure 219. Adding Performance View to Report

7.5.2 8272 JPM Example

The IBM 8272 is currently not supported by JMA but you can use JMA to manage it as a Generic Java-based device. Once the JMA for Generic Java-based device has been started you can perform a number of functions with the exception of device configuration and having the ability to view a graphical display representing the status of the device and its ports.

Figure 220 on page 242 shows the interface status events.

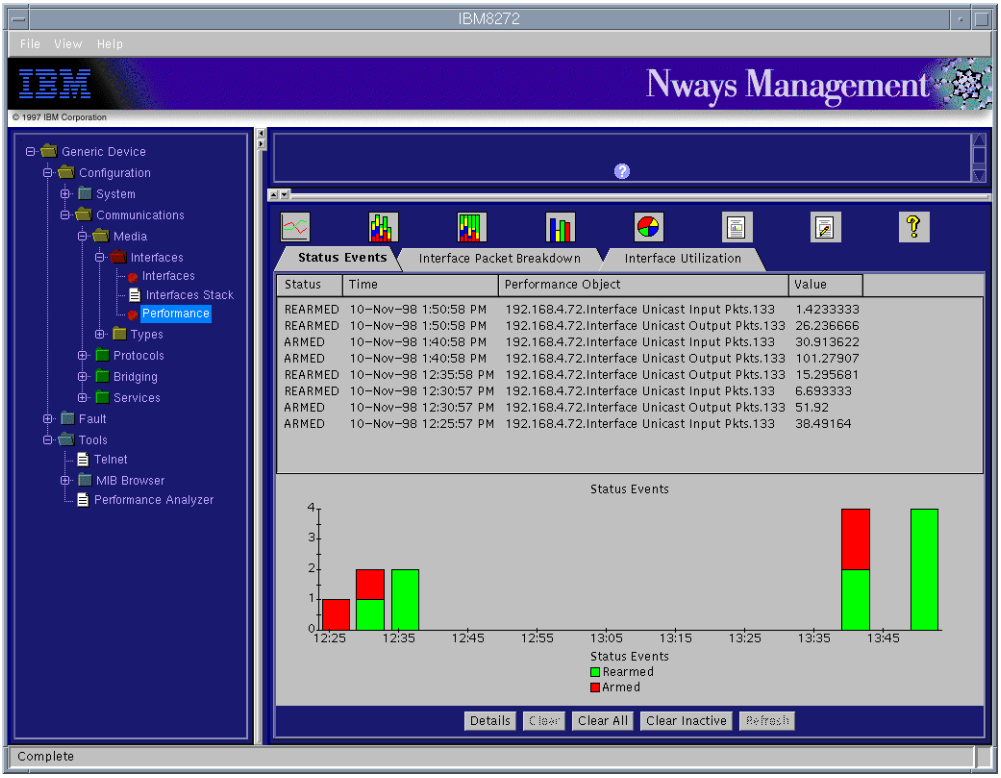


Figure 220. 8272 Interface Status Events

Click on **Interface Utilization** (see Figure 221 on page 242).

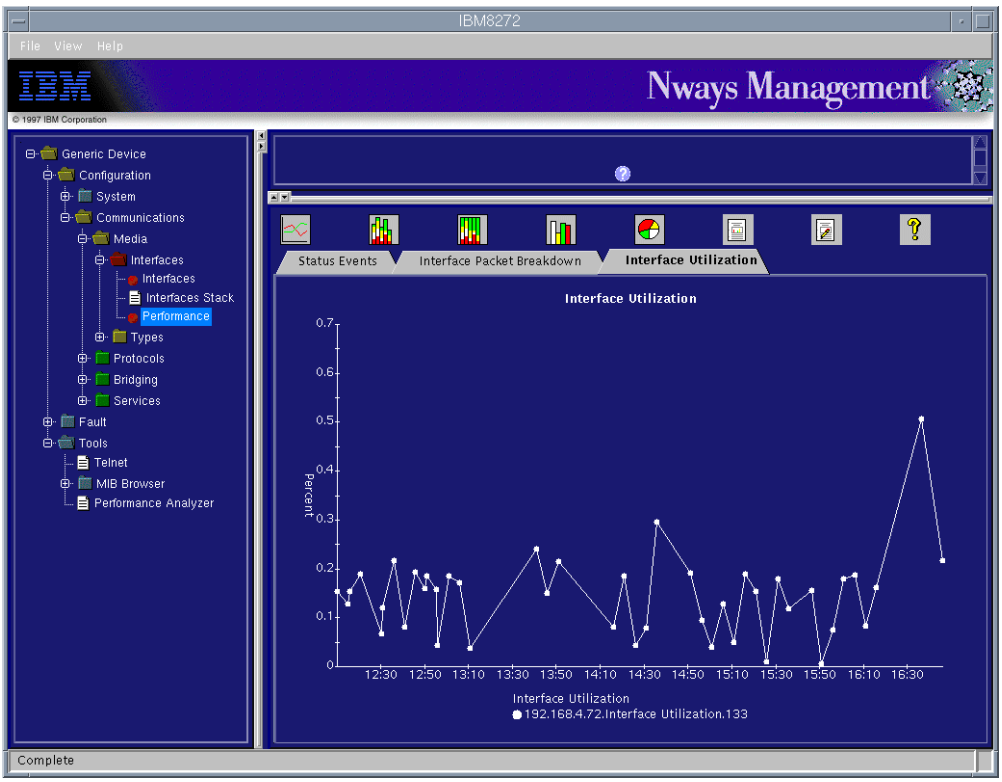


Figure 221. 8272 Interface Utilization

In our network the IBM8272 was connected to the backbone via ATM UFC, so there are navigations of ATM and LANE available for viewing. You can configure the Performance Configuration to add performance objects and the View to ATM template so that ATM performance can be monitored. Figure 222 shows performance of the LEC traffic already defined in the performance template.

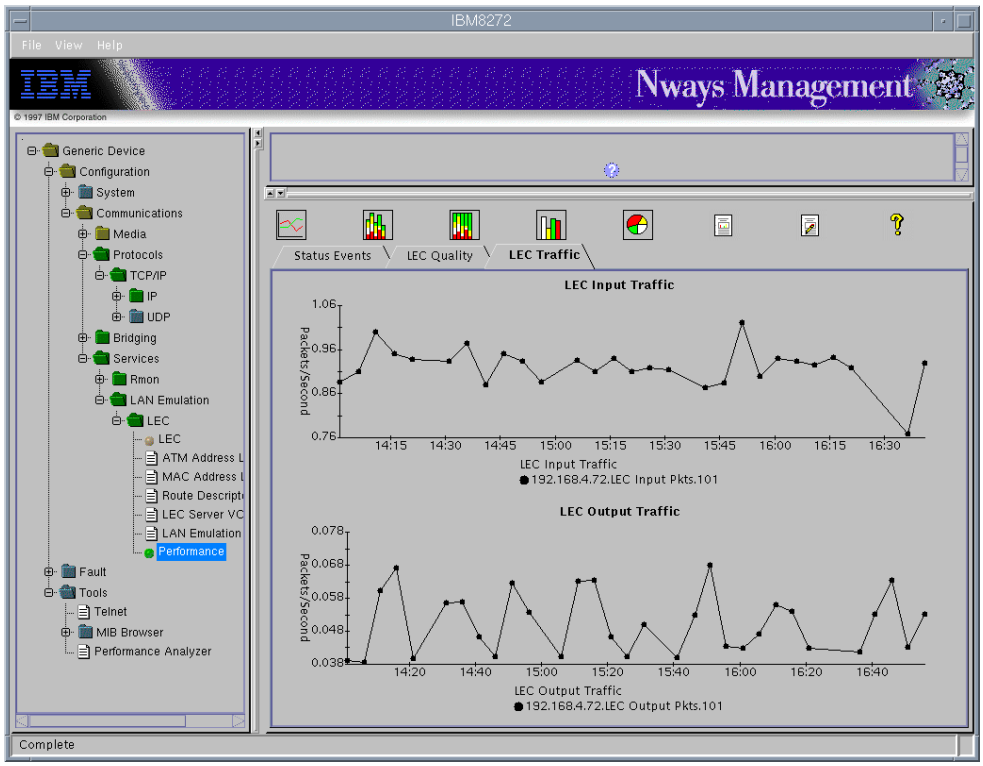


Figure 222. LEC Traffic on 8272

7.5.3 8260 JMA Example for ATM

ATM management can be performed via the ATM Campus submap on NetView. Here you can manage ATM logical views, ELANs, the LES, etc. You can also mange the performance of an ATM interface from the JMA by treating those ATM devices as generic Java-based devices. For example, we started the JMA for 8260 CPSW by opening the ATM Campus submap from NetView Root map then select the **CPSW**, the choosing **IBM Nways Java: Open Java Device** from the **Tools** menu (see Figure 223).

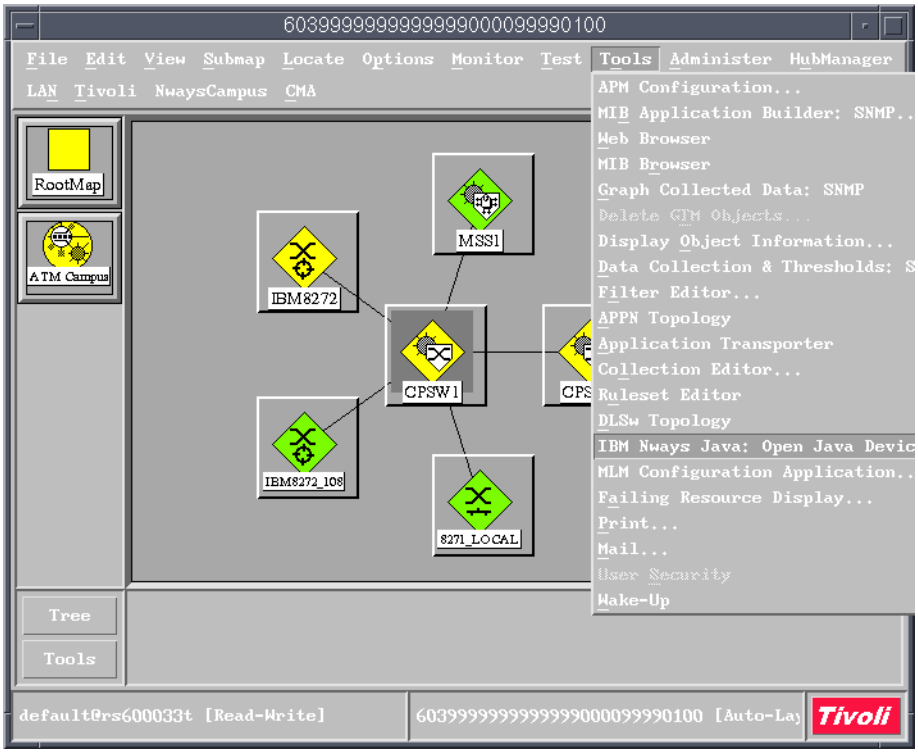


Figure 223. Starting JMA for 8260 ATM Switch

Once the JMA starts we are able to manage the interfaces on the 8260 including the ATM interfaces. You can configure the performance configuration to add performance objects and views.

Figure 224 shows the navigation tree of CPSW and that there are navigations for ATM and LANE available. You can use these navigations to view and manage the ATM interfaces.

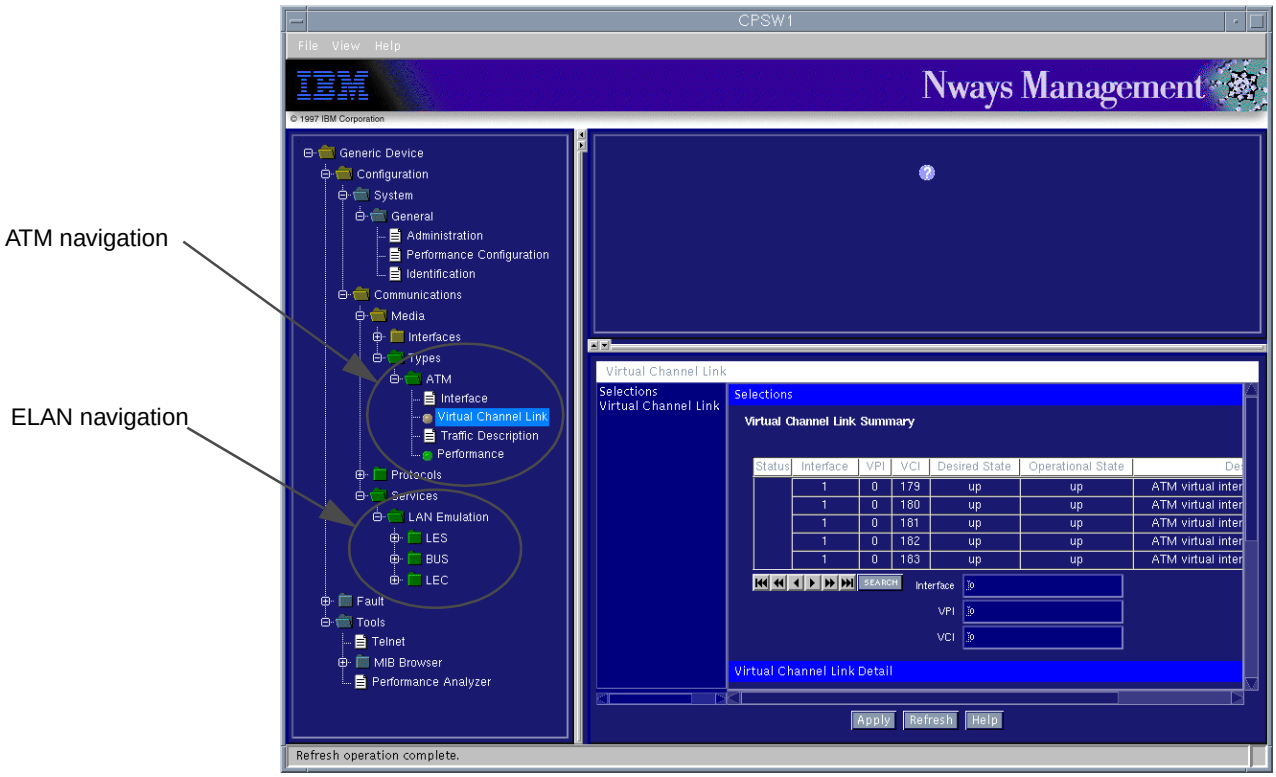


Figure 224. ATM and ELAN Navigation Tree

7.5.4 Frame Relay Performance Example

The 2210_Local and 2210_Remote devices are connected via frame relay. By default, the performance management tool includes some performance objects for Frame Relay but they are not assigned to a specific template. We configured the template as follows:

- From the 2210_Remote JMA select **Configuration-> System-> General-> Performance Configuration**.
- Select **Resource Identifier = framerelay.model.FrameRelay.**
- Add the following performance objects to Applied POD Names:
  - Frame Relay Backward Congestion
  - Frame Relay Forward Congestion
  - Frame Relay Input Traffic
  - Frame Relay Output Traffic
- Add the following views to Applied View Names:
  - Frame Relay Quality
  - Frame Relay Traffic
- Click on **Save.**

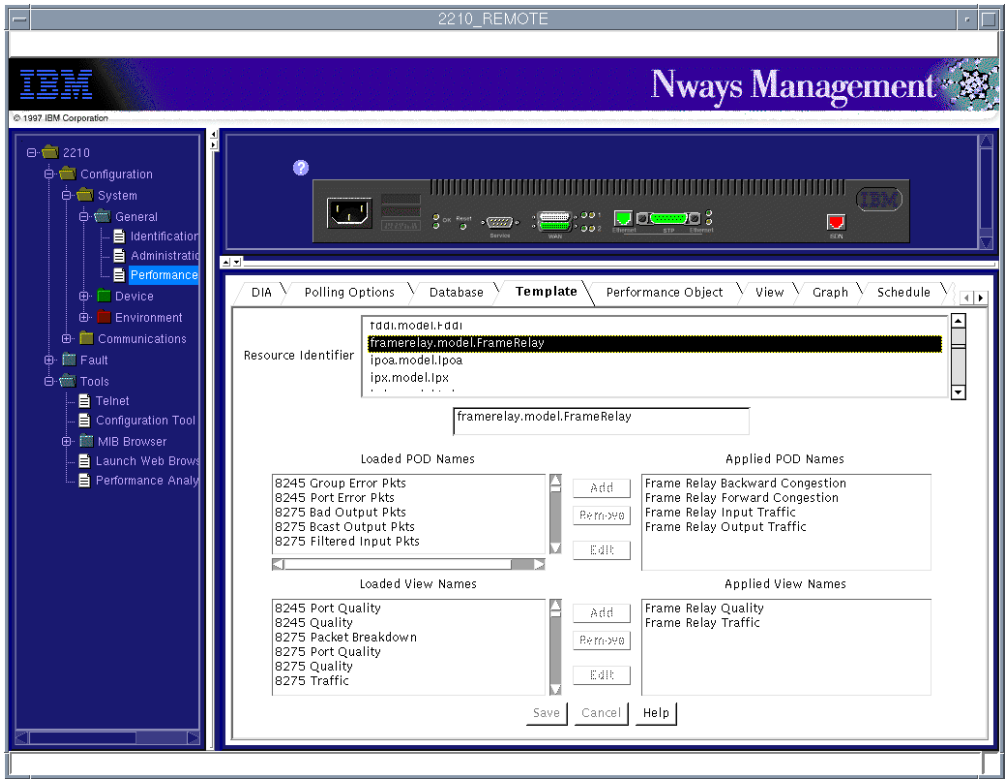


Figure 225. Configuring Performance for Frame Relay

Initially no data will appear as the frame relay data has just started to be collected. When the JPM had performed collection of the data elements we selected the Frame Relay performance option. The quality graph and frame relay traffic are shown in Figure 226 on page 247.

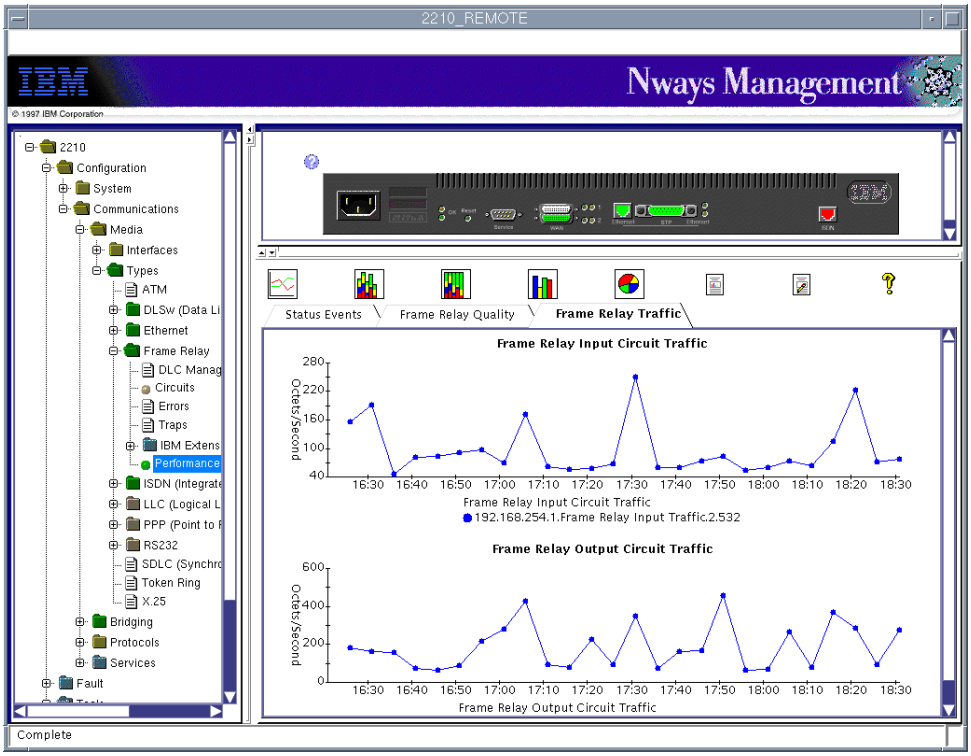


Figure 226. Frame Relay Traffic Performance

7.5.5 Using the Performance Analyzer

The Performance Analyzer application gets all of its statistical data from the Nways Manager Performance Database by default. You need to configure Nways Manager to store its performance data to a database, (see section 7.3.3, “JDBC Database Configuration” on page 225).

You can start Performance Analyzer from the JMA or the Web browser. If you are using DB2 as the database to store Nways Manager performance data and you plan on using the Performance Analyzer from a Web browser, then you need to enable remote access to the DB2 database. Remote connections to the database are enabled by invoking the db2jstrt command. For example, to allow connections on port 50000, enter:

```
db2jstrt 50000
```

Putting this command in a script or batch file that is executed on system restart will help avoiding retyping this command each time the database machine is restarted.

To start the Performance Analyzer from JMA:

- Click on **Performance Analyzer** on the Navigation tree.
- Click on **Apply** to start (see Figure 227).

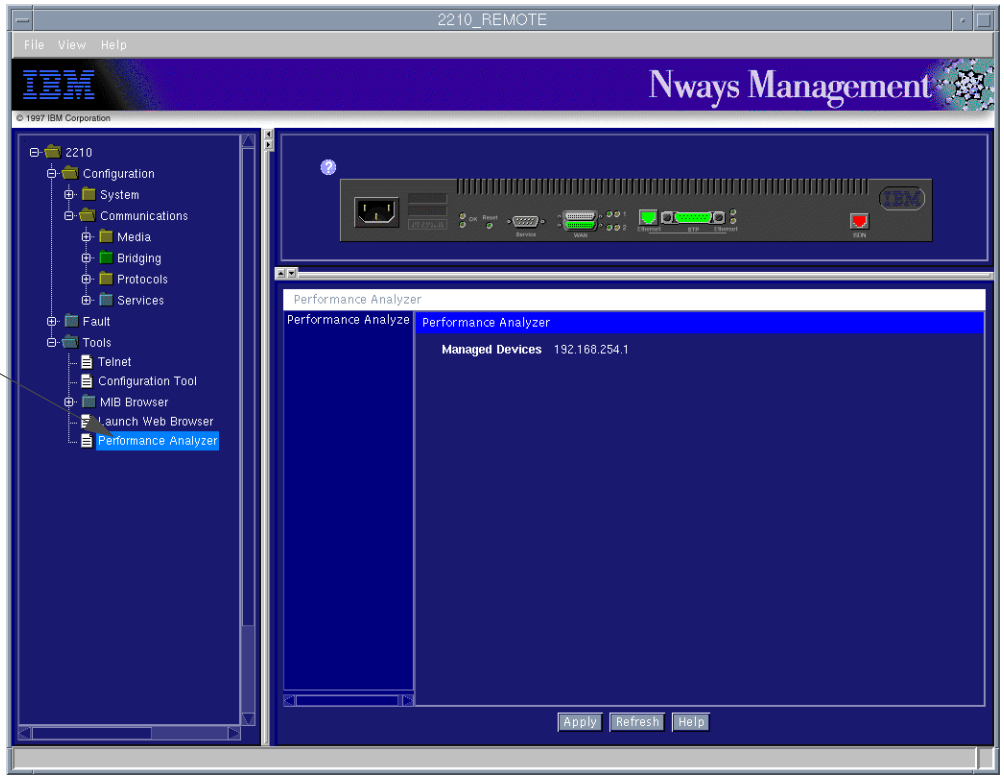


Figure 227. Launching Performance Analyzer from JMA

The Performance Analyzer will appear as in Figure 228 on page 248

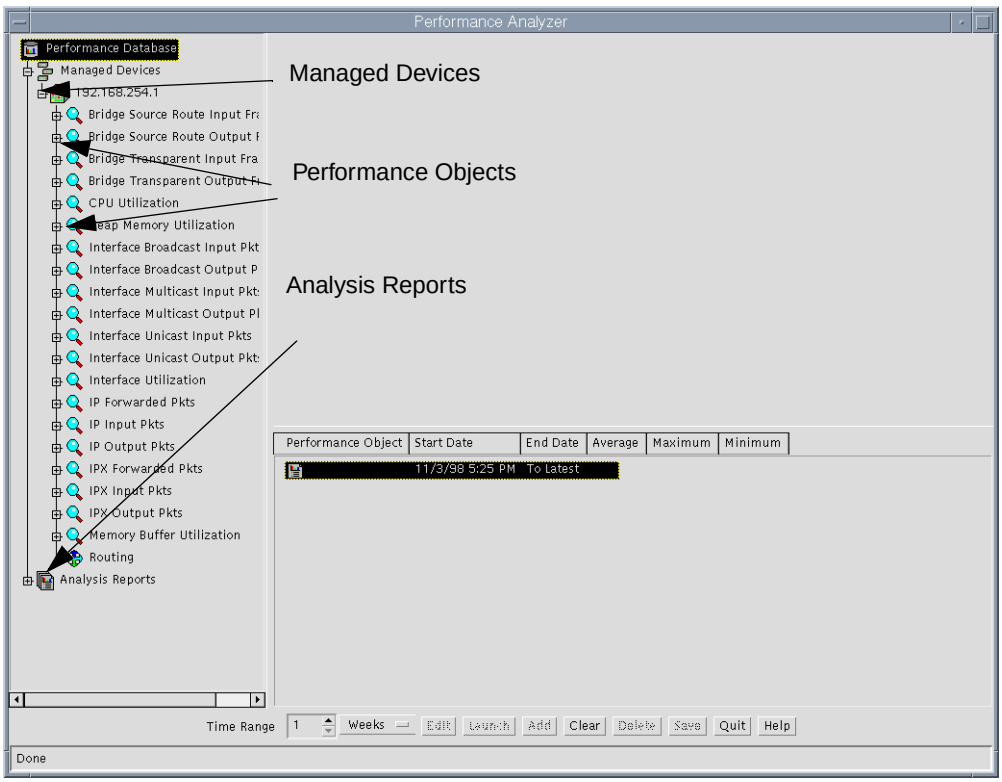


Figure 228. Performance Analyzer for 2210_Remote

The Managed Devices branch of the Navigation tree contains an icon for each device in the Nways Manager Performance Database. If the Performance Analyzer was launched from a Java-based management application, you will only see that device under the Managed Devices tree.

Under each managed device, you will see a magnifying glass icon representing a performance object. A performance object is an SNMP MIB variable or expression that Nways Manager is polling for that device.

Under each performance object, you will see each instance that was discovered for this device. Single-instance (scalar) performance objects will only have a single instance ("0") while multi-instance (tabular) performance objects can have several.

The Analysis Reports branch of the navigation tree contains an icon for each user-created report.

For a router device, there is an icon named Routing at the bottom of the Performance Objects tree. Figure 229 shows the results when you double-click on this icon.

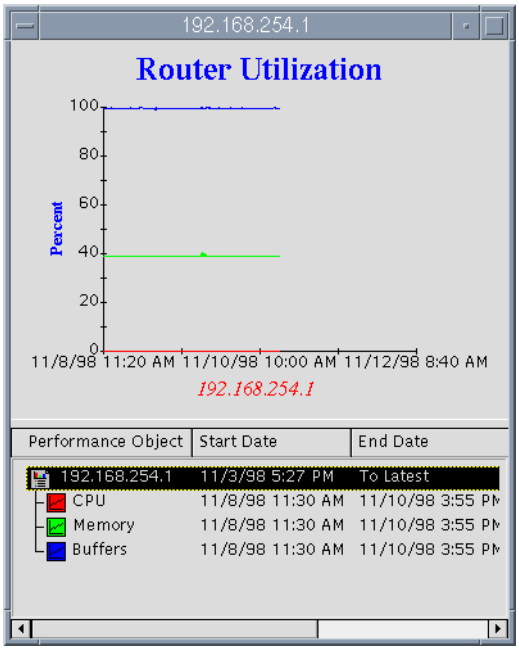


Figure 229. 2210_Remote Router Utilization

From Performance Analyzer you can play or create a graph for the analysis report. Here you can do the following:

- Setting the Time Range

  The Time Range control gives you the ability to manage the amount of time (from the current time into the past) that you want your graph to cover. Graphs with larger-than-needed time frames can be slow to retrieve data from the database and the graph can become cluttered, so be sure to choose the smallest time range that meets your needs.

- Clear the Graph

The Clear button is used to clear all elements from the graph and to reset the graph times to the range indicated by the Time Range control. Notice that the graph will not accept new Time Range values until it is cleared.

- Add Elements

  Now that your graph is initialized, you can begin to add graph elements to it. A graph element can be added by double-clicking on a performance object instance or by selecting one or more instances and clicking the **Edit** button. The selected instances will be added to the graph with the instance details displayed in the legend below the graph.

- Modify Attributes

  You can modify the attributes of a graph or of a graph element. You can modify graph attributes by double-clicking on the top row of the legend below the graph. You can modify graph element attributes by double-clicking on the desired element in the legend.

- Manipulate a Graph

  This section describes the actions that you can perform on a graph.

- Zooming

  You can zoom in on a particular section of a graph by holding the left mouse button down and dragging a selection box around the desired part of the graph.

- Translating

  You can move the graph around both of its axes by holding down both the Shift key and the left mouse button and dragging the mouse in the direction you want the graph to move.

- Resetting

  To reset a graph to a default view of the data (X axis from first to last point, Y axis from the minimum to the maximum value), simply press the **R** key. Notice that the reset key will only work if the graph itself has focus.

- Exploding

  You can explode a point in time on a graph by holding down the Ctrl key and selecting a graph point with the left mouse button. A graph dialog will appear with the values for all of the graph elements at that specific point in time.

  You can toggle between a pie and bar chart view of the data. The same zooming, translating, and resetting options are available, but now an explode operation (Ctrl-Click) will display the value of the selected element as well as its percentage when compared to the other elements.

- Saving a Report

  After creating a graph, you can save your changes to a report. Clicking on the Save button will bring up the Save Analysis dialog. Enter a unique name (up to 18 characters with no spaces) and click Yes to store the graph in the performance database as a report. A new report icon will be created under the Analysis Reports branch of the Navigation tree.

- Launching a Report

  You can launch a report that you have created by selecting a Time Range and then double-clicking on a report icon (or selecting one or more reports and

clicking the Launch button). If you want to make changes to a report, simply select the report and click Edit to load the report as a graph. Make your changes to the graph and click Save to store the graph back as a report.

Figure 230 shows the Analysis report of 2210 IP traffic, which has three elements displayed on the graph.

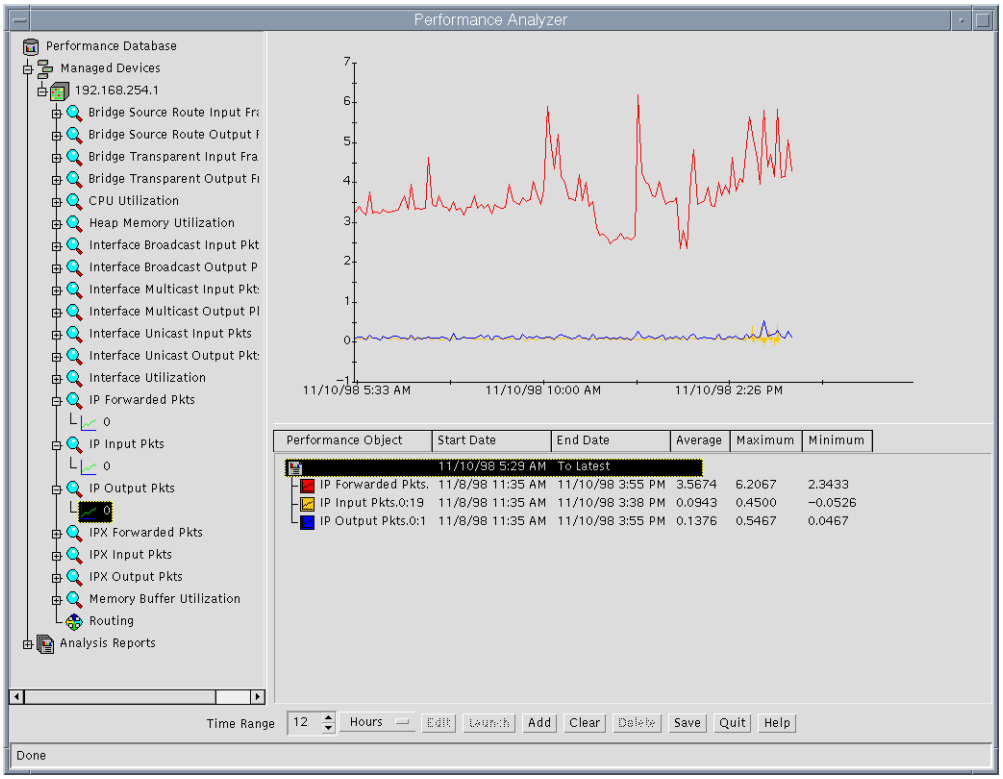


Figure 230. Adding a View to the Performance Analyzer

7.6 Nways Java Management Reports

Java Performance Manager's reporting capability provides access to the historical data that is stored in the JPM database without having to navigate through the JMA. It provides this access through Java applets that are imbedded in html pages made available through a Web server on the Nways manager workstation. There is one type of report that provides graphical displays of stored historical data, and two types of reports that provide text-based displays. To simplify Web access to the reports, a Report Catalog html page is available: /usr/CML/JMA/java/websvr/reports/ReportCatalog.html that provides links to all reports, is automatically created and updated by JPM.

7.6.1 Creating Chart Reports

The simplest way to create a report is to click on the **Add View To Report** button while viewing a graph in the JMA. When the report creation dialog comes up, type in the name for the report you wish to create (JPM automatically adds a html link to the created file), and select a time span for the report. You can create a report that is generated based on the number of hours, days, weeks, or months.

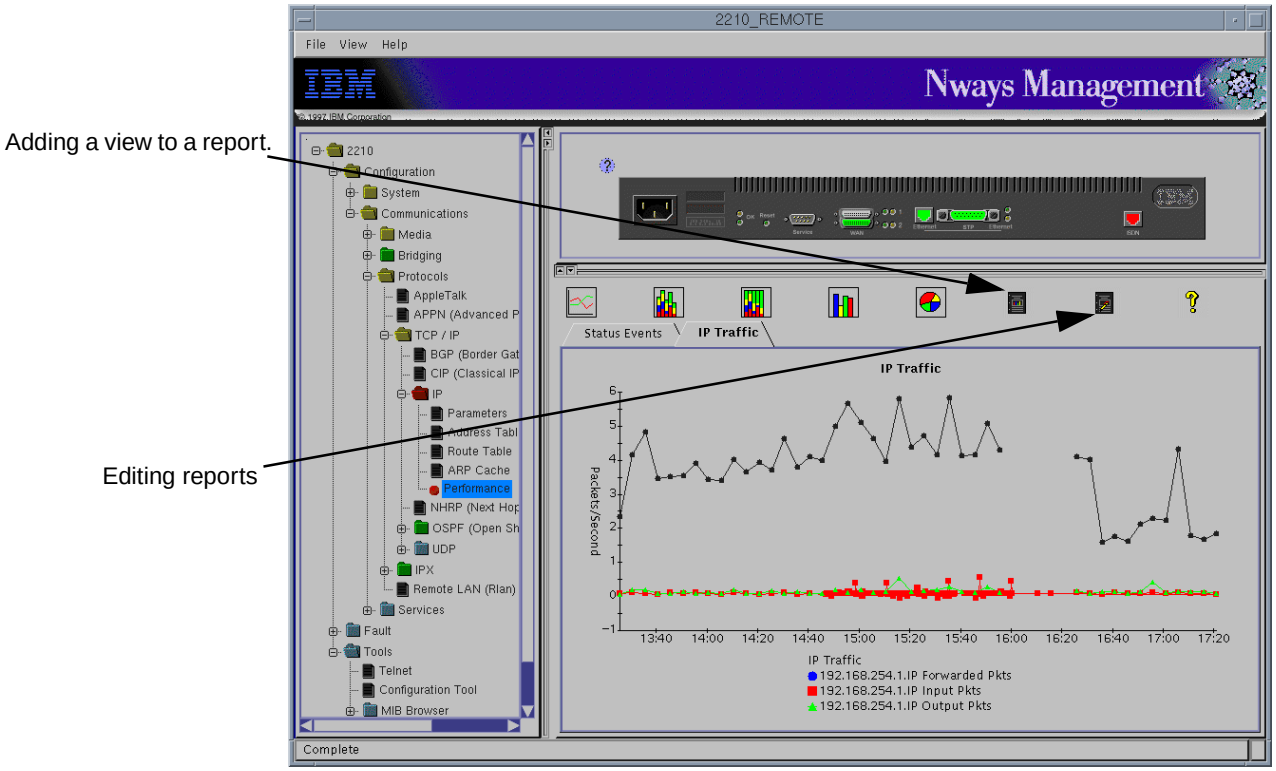


Figure 231. IP Traffic on 2210: Add to Report

Click on **Edit Report** (see Figure 232 on page 253).

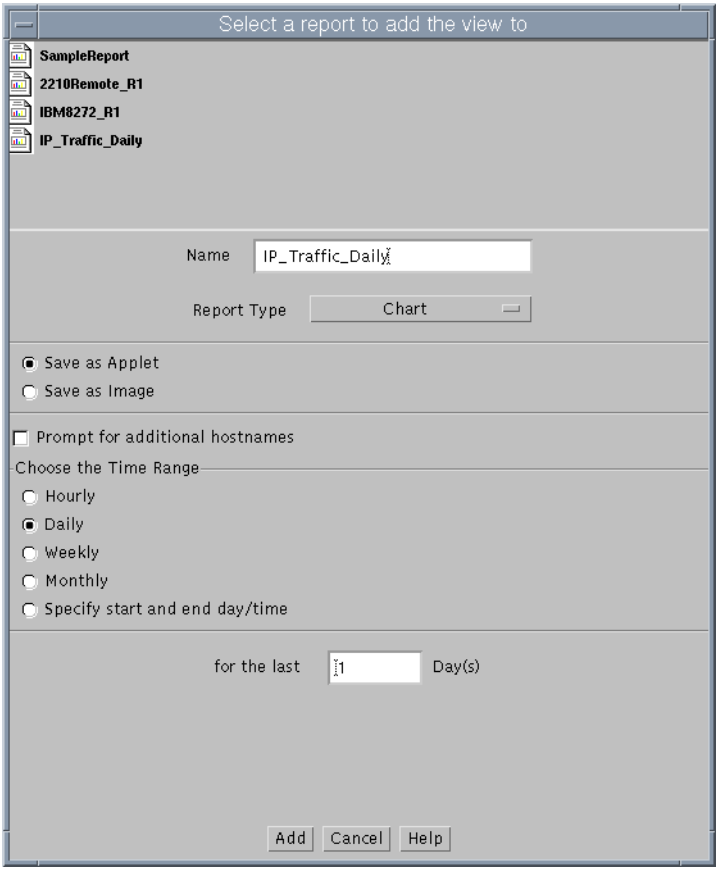


Figure 232. Creating a Chart Report

To create a simple report that displays the information in graph format, leave the default selections for the Report Type and save as an applet, and leave the **Prompt for Additional Hostnames** button unchecked.

Performing these steps will create an HTML file with APPLET tags and parameters. An applet is a Java program that runs inside a Web browser. The JPM chart applet communicates with the JPM server to retrieve the historical data identified by the parameters and displays the data in a chart.

A report created with default parameters through the **Add View To Report** will display information from only the agent that the JMA is open for, and for all instances of the tabular MIB variables. The next section describes how to create reports that have different parameters.

7.6.1.1 Report Parameters

It is possible to create reports that display selected rows of tabular MIB data (such as interfaces), or which combine historical data from multiple agents on a single graph. This section shows you how to code parameters in HTML files to create these varieties of reports.

To modify the reports created by JPM use any text editor, or click the **Edit Reports** button above the JPM graph after clicking on the **Performance** bullet on the JMA navigation tree.

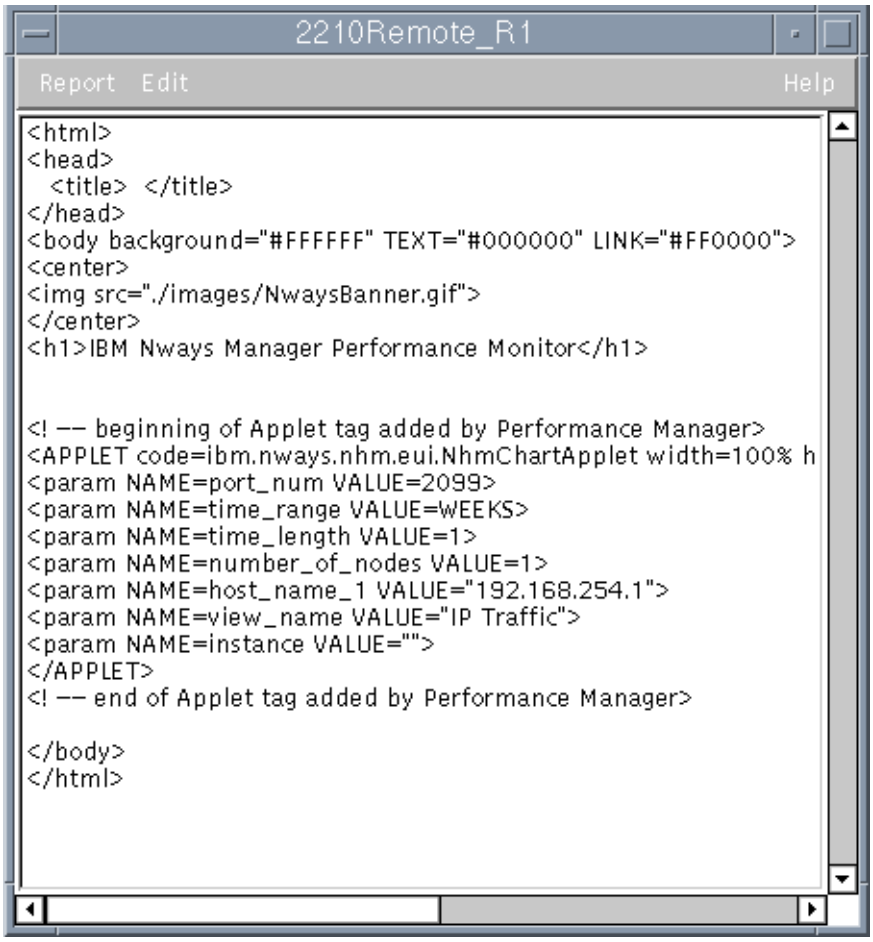


Figure 233. Editing Report from JMA

To create a report that has a single instance of a tabular MIB variable for a single agent, specify a value for the instance parameter which is created by default in the report file. This value has the format MIB_variable_name=value. For example, to create a report that shows the interface utilization of interface 3, first use JPM to create a report that displays Interface utilization for all interfaces, then modify the parameters as follows: (Do not change any of the other parameters).

```
<param NAME=number_of_nodes VALUE=1>
<param NAME=host_name_1 VALUE="10.10.3.100">
<param NAME=view_name VALUE="Interface Utilization">
<param NAME=instance VALUE="ifIndex = 3">
```

Some tables require two MIB variables to identify a particular row in the table. For example, to create a report that shows the frame relay traffic for circuit 17 on interface 4, modify the instance parameter as follows:

```
<param NAME=number_of_nodes VALUE=1>
<param NAME=host_name_1 VALUE="10.10.3.100">
<param NAME=view_name VALUE="Frame Relay Traffic">
<param NAME=instance VALUE="ifIndex = 4, frCircuit = 17">
```

To create a report that shows more than one instance (but not all instances) of a tabular MIB variable for a single agent, create a host_name_ and instance_

parameter pair for each instance you wish to view. In this case, you must set the number_of_nodes parameter to the number of instances you wish to see on the graph.

```
<param NAME=number_of_nodes VALUE=2>
<param NAME=host_name_1 VALUE="10.10.3.100">
<param NAME=view_name VALUE="Interface Utilization">
<param NAME=instance_1 VALUE="ifIndex = 4">
<param NAME=host_name_2 VALUE="10.10.3.100">
<param NAME=instance_2 VALUE="ifIndex = 5">
```

To create a report that shows instances of MIB variables from more than one agent, create a host_name_ and instance_ parameter pair for each agent you wish to see. Also, change the number_of_nodes parameter to the number of (host, instance) pairs you create for example:

```
<param NAME=number_of_nodes VALUE=3>
<param NAME=host_name_1 VALUE="10.10.3.101">
<param NAME=view_name VALUE="Interface Utilization">
<param NAME=instance_1 VALUE="ifIndex = 4">
<param NAME=host_name_2 VALUE="10.10.3.102">
<param NAME=instance_2 VALUE="ifIndex = 1">
<param NAME=host_name_3 VALUE="10.10.4.101">
<param NAME=instance_3 VALUE="ifIndex = 9">
```

7.6.2 Creating Text Reports

There are two types of text-based reports that may be created by selecting the **Add View to Report** button on the JMA chart screen: Single Node Analysis report, and a Multiple Node Analysis report.

- A Single Node Analysis report presents a statistical analysis of all performance objects (variables) associated with the selected view (the view that is currently being displayed). The mean, standard deviation and recorded high and low values are displayed in a table.
- The Multiple Node Analysis report presents a statistical analysis of a single performance object across one or more agents. The mean, standard deviation, and recorded high and low values are displayed in a table.

To create a text report, click on **Add View to Report** while viewing a performance graph in a JMA that contains performance objects that you wish to analyze. Choose a name for the report, and change the Report Type to either Single Node Analysis or Multiple Node Analysis.

7.6.3 Viewing Reports

You can view the reports with a Web browser that supports Version 1.1 of the Java Development Kit (JDK). Start the Web browser go to the page:

`http://`*`server/nways/`*`reports/ReportCatalog.html`

Where server is the Nways server and nways is an alias name of the Nways Web page directory. The reports can be selected from this page.

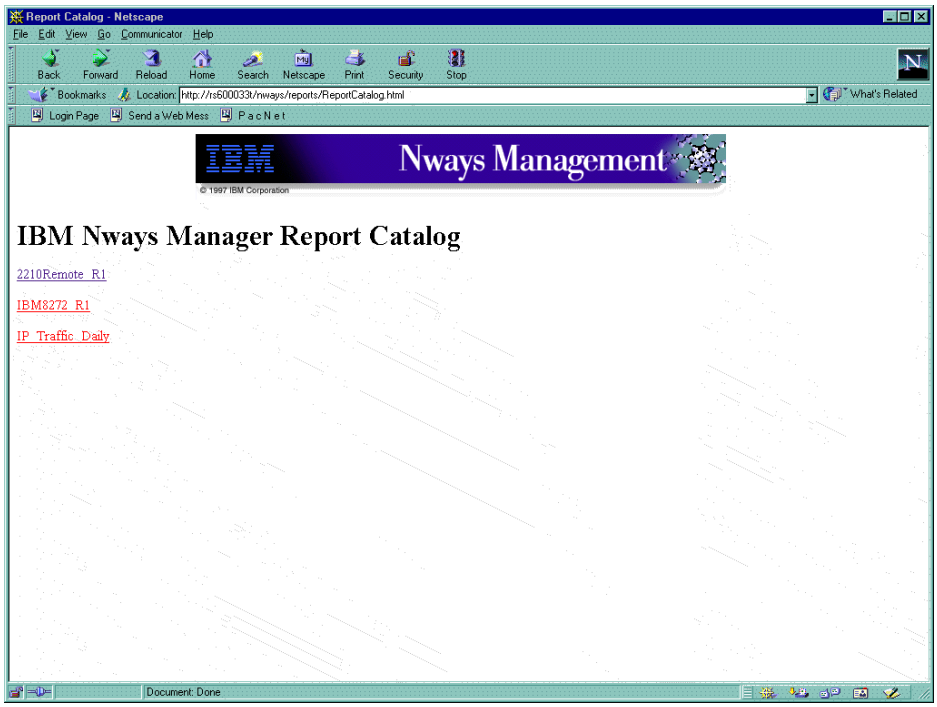


Figure 234. Nways Report Catalog Page

When viewing a report, the time period that the report displays is governed by the parameters you selected when the report was created (the time_range and time_length parameters in the HTML file). The starting period for the time range is dependent on the units specified by the time_range parameter. For a unit of HOURS, the time range starts at the beginning of an hour; for a unit of DAYS, the time range starts at the beginning of a day (12:00 midnight); for a unit of WEEKS, the time range starts at the beginning of a week (Sunday by default, but this may be changed under the Report Options tag of the DpAdmin tool).

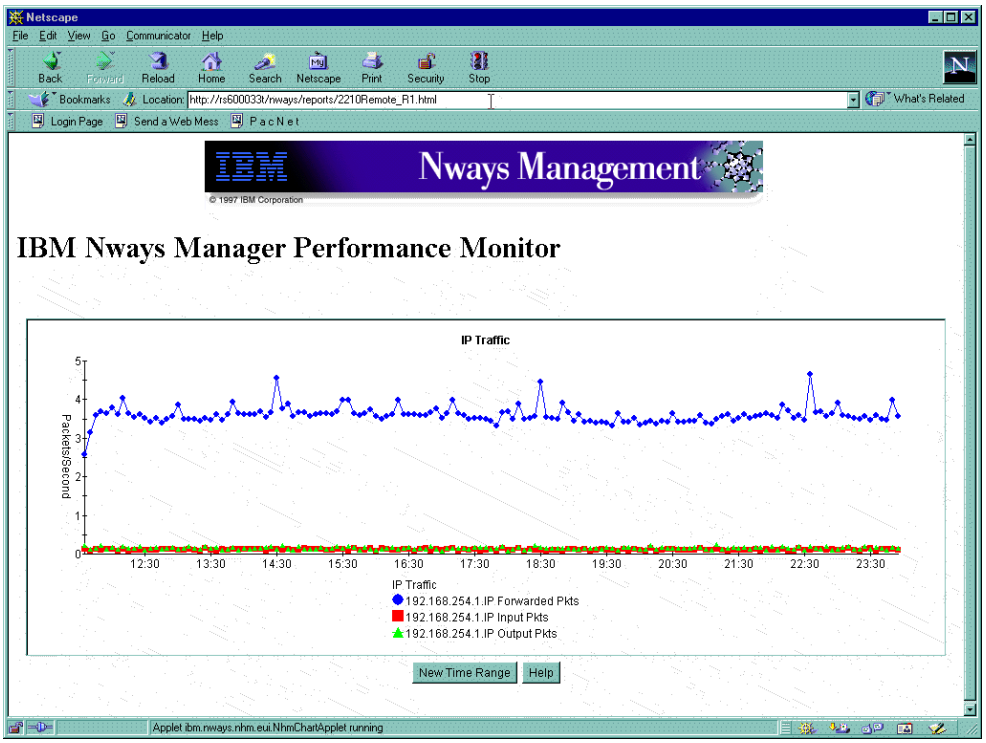


Figure 235. Viewing Report from a Web Browser

When viewing a report, you may change the time span that the report covers by clicking on **New Time Range.** Here you can specify a range as a certain number of hours, days, weeks, or months, or you may give an exact starting and ending times.

7.6.4 Disable the JPM

There maybe a reason to disable the JPM, as this starts automatically when the JPM is initiated. To disable the JPM perform the following steps:

Shut down the JMA Server (close Workgroup Manager on NT or issue the command ovstop JMAintegrator).

Edit the JdmServerProperties.txt file (in java\bin on NT or /usr/CML/JMA/java/properties on AIX)

Change the section that contains the line:

```
ibm.nways.perfhook.PerfService          \
```

```
# The services property identifies the service classes to be started
# when the JDM server is started.
#       ibm.nways.jdm.TrapCatcher              \
services=ibm.nways.jdm.RemoteModelFactoryManager \
        ibm.nways.jdm.modelgen.InstrContextFactoryMgr    \
        ibm.nways.jdm.SnmpService              \
        ibm.nways.jdm.browser.BrowserService    \
        ibm.nways.perfhook.PerfService         \
        ibm.nways.jdm.traceroute.TraceRouteService \
        ibm.nways.perfhook.ModelListener
```

To be:

```
# The services property identifies the service classes to be started
# when the JDM server is started.
#       ibm.nways.jdm.TrapCatcher              \
#       ibm.nways.perfhook.PerfService         \
services=ibm.nways.jdm.RemoteModelFactoryManager \
        ibm.nways.jdm.modelgen.InstrContextFactoryMgr    \
        ibm.nways.jdm.SnmpService              \
        ibm.nways.jdm.browser.BrowserService    \
        ibm.nways.jdm.traceroute.TraceRouteService \
        ibm.nways.perfhook.ModelListener
```

Now save the file.

Restart the JMA server (start Workgroup Manager on NT or ovstart JMAintegrator on AIX)

The effects of this change will be as follows:

- No performance polling is done for newly or previously managed devices.
- Performance bullets in the JMA navigation tree will be blue (unknown).
- Clicking on the Performance bullets will result in a blank panel with just the Performance toolbar.
- Several Cannot find PollingService messages will be logged.

7.7 ATM Web Based Management

The ATM Web interface is accessed from a browser. For our environment we used the following:

`http://rs600033t/atm-html/AtmWebMngt.html`

See Figure 236 on page 259.

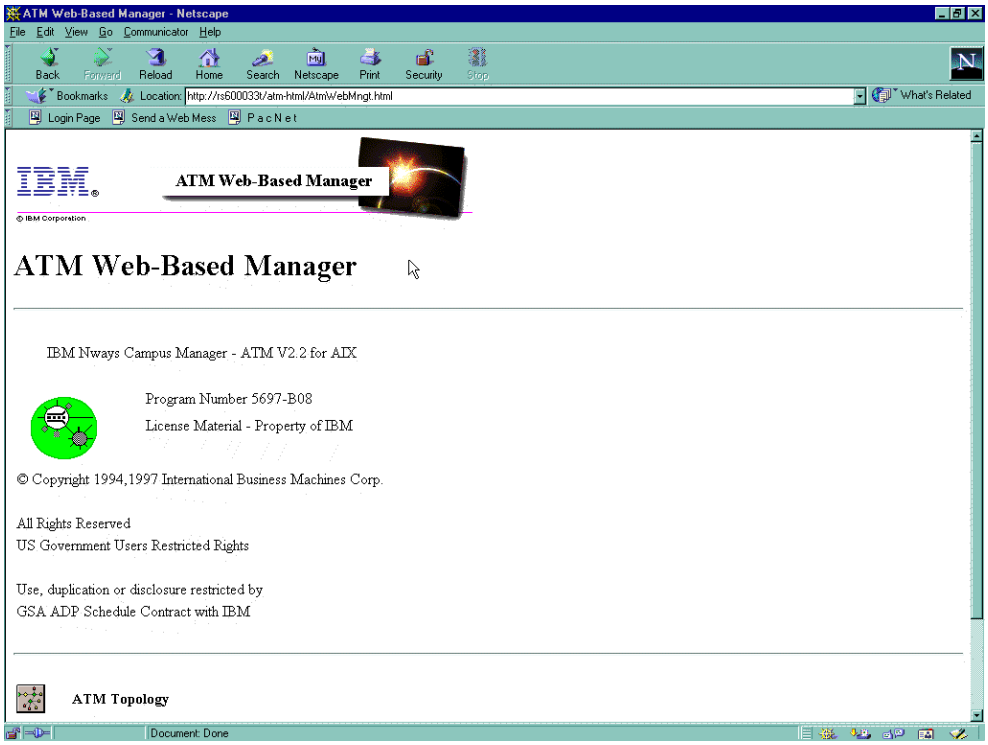


Figure 236. ATM Web Management Home Page

Click on **ATM Topology** (see Figure 237).

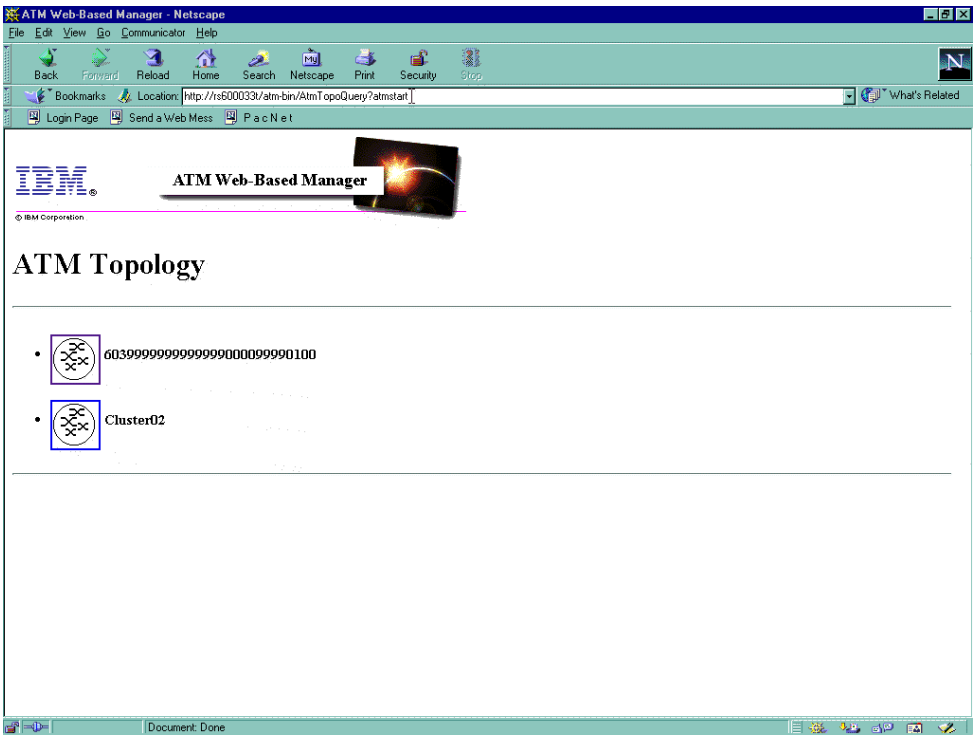


Figure 237. ATM Topology: ATM Cluster/ Peer Group Level View

Here we can see the PNNI configuration and Cluster02 for our environment. If we double-click on the PNNI icon we can see the nodes.

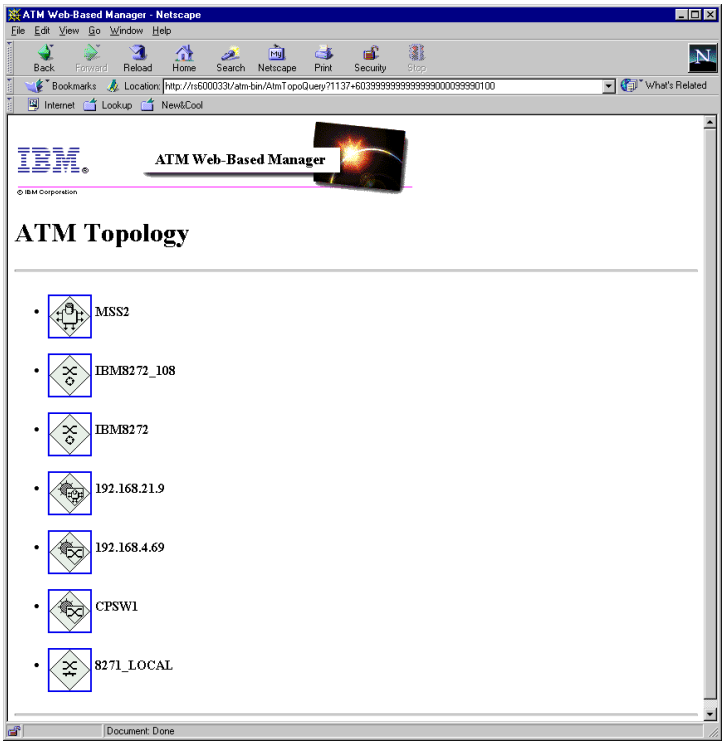


Figure 238. ATM Nodes

Click on any device on this page to access the Web functions (see Figure 238).

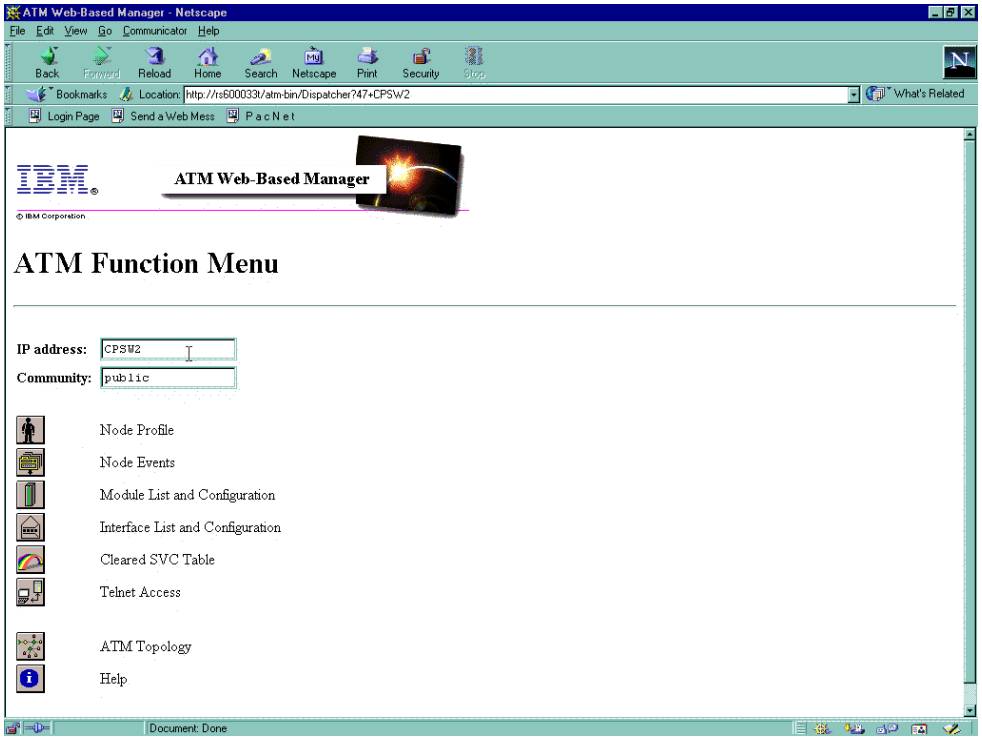


Figure 239. ATM Functions Menu

Click on **Node Profile** to see node information.

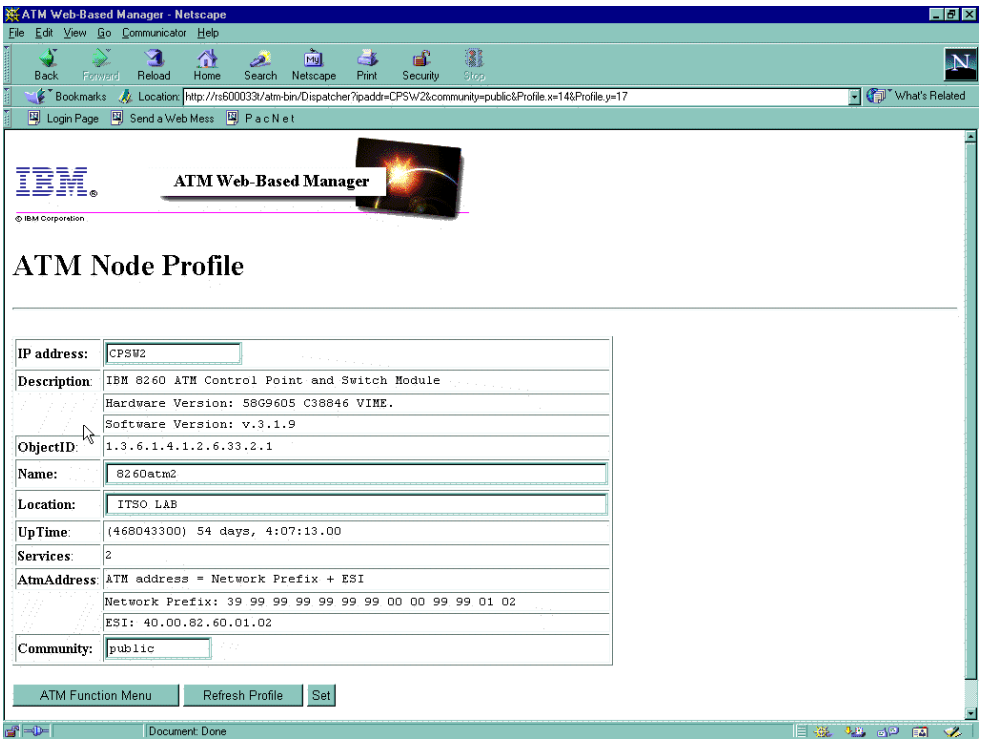


Figure 240. ATM Node Profile from the Web

The cleared SVC table is shown in Figure 241.

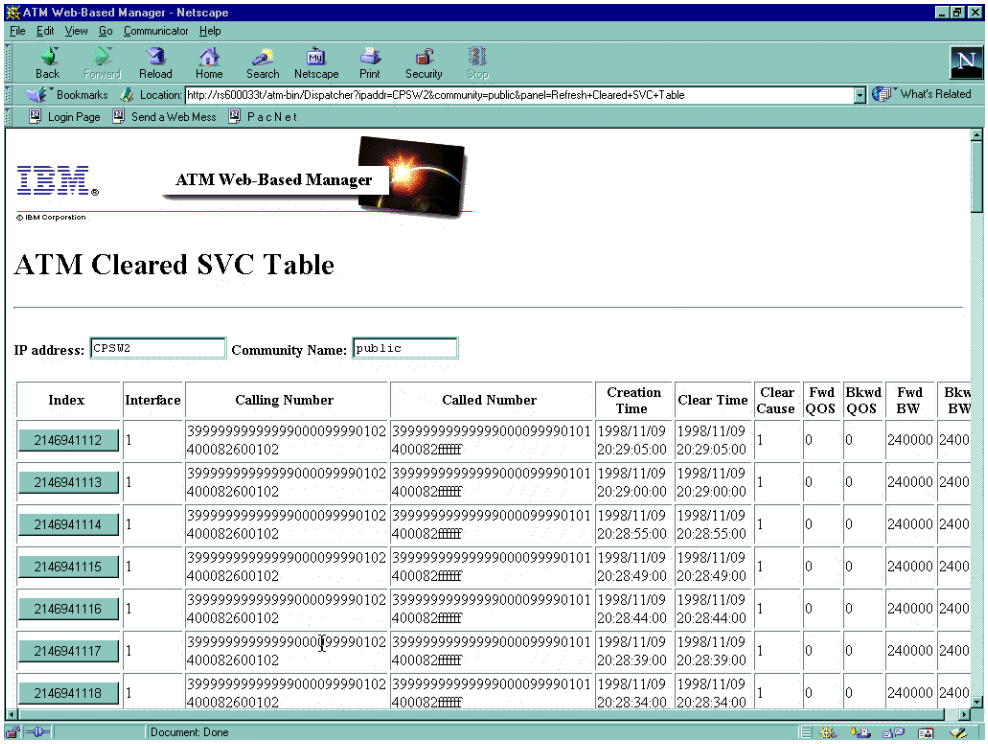


Figure 241. ATM Cleared SVC Table from the Web

7.8 Web Access for HTTP Agents

The trend towards Web and Java-based management is more evident, as more and more products have built-in HTTP agents. The HTTP agent or server allows you to directly manage a device graphically using a Web browser, which is fully platform and/or vendor independent. One such example from IBM is the MSS (multiprotocol switched services).

Some of the newer devices support Java. The Java technology allows Java applets to be downloaded from the network device and executed. These views are dynamically updated for status of the device. One such device from IBM is the 8275-113 Ethernet Desktop switch.

Below, some examples of Web management of both the MSS and the 8275-113 Ethernet Desktop switch are shown.

7.8.1 MSS 8210 Web Browser Interface Example

The Web browser interface of MSS allows configuration and basic management of the MSS server using any Web browser that supports HTML. Before the MSS server can be accessed over a Web browser, an IP address should be configured, and IP connectivity must exist between the Web browser and the MSS server.

There are two ways of launching the Web browser:

- From the JMA view of the MSS
- Directly from the Web browser

For the 8210 we can select **Launch Web Browser** (see Figure 242).

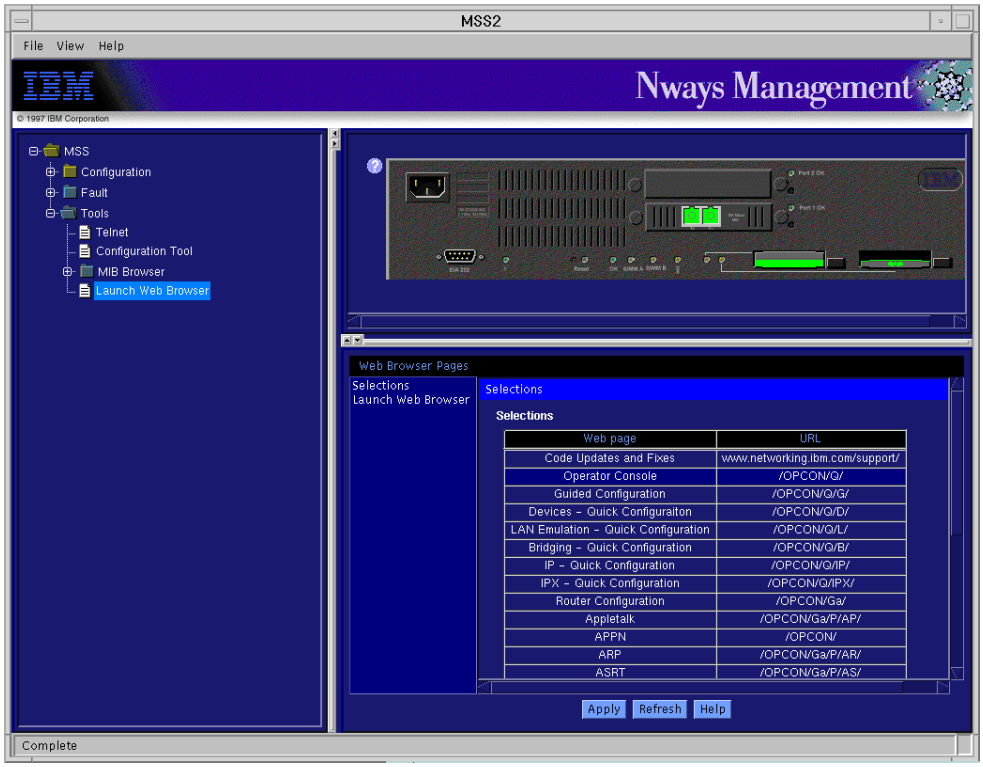


Figure 242. Launching the Web Browser from a JMA View of MSS

In the bottom right-hand side of Figure 242, the JMA view contains several URLs to provide specific functions.

Our MSS was set up so that we had to enter a user Id and a password (see Figure 243).

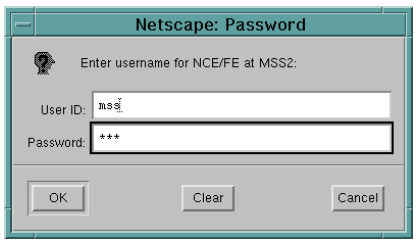


Figure 243. MSS Server Login Validation

Below is the MSS home page accessed by launching Netscape from the AIX desktop, with the URL set to MSS2. MSS2 is the hostname as defined in the DNS and resolves to the IP address.

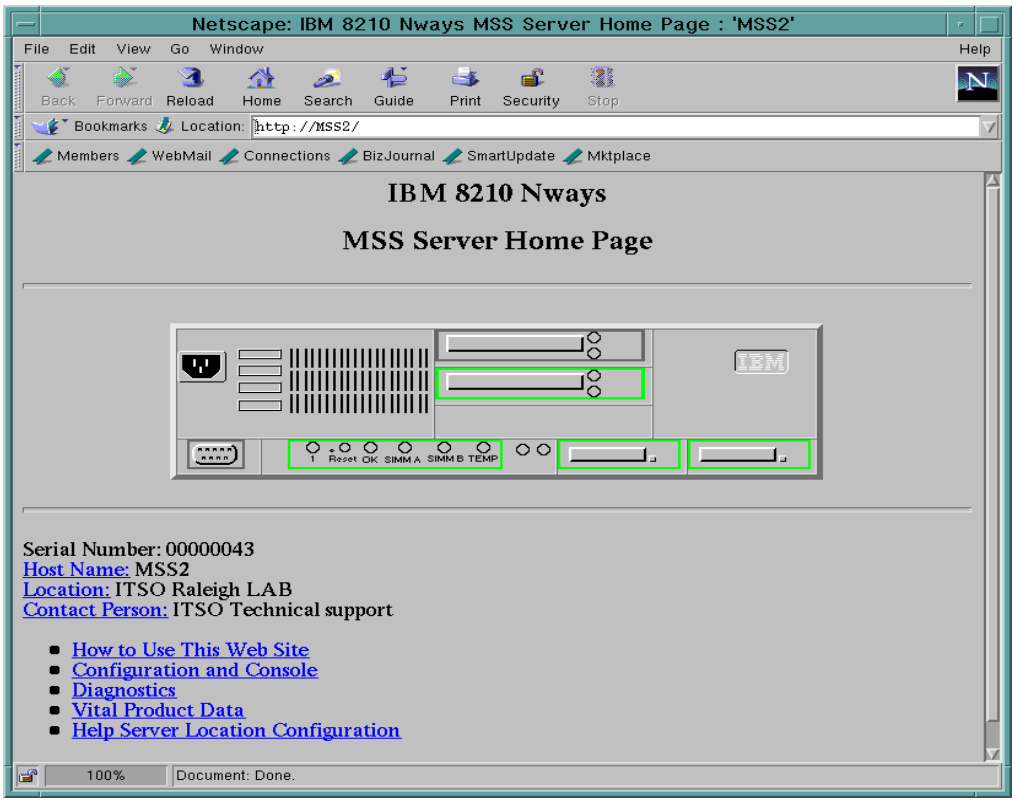


Figure 244. MSS Server (8210) Home Page

Click on **Configuration and Console** to see Figure 245.

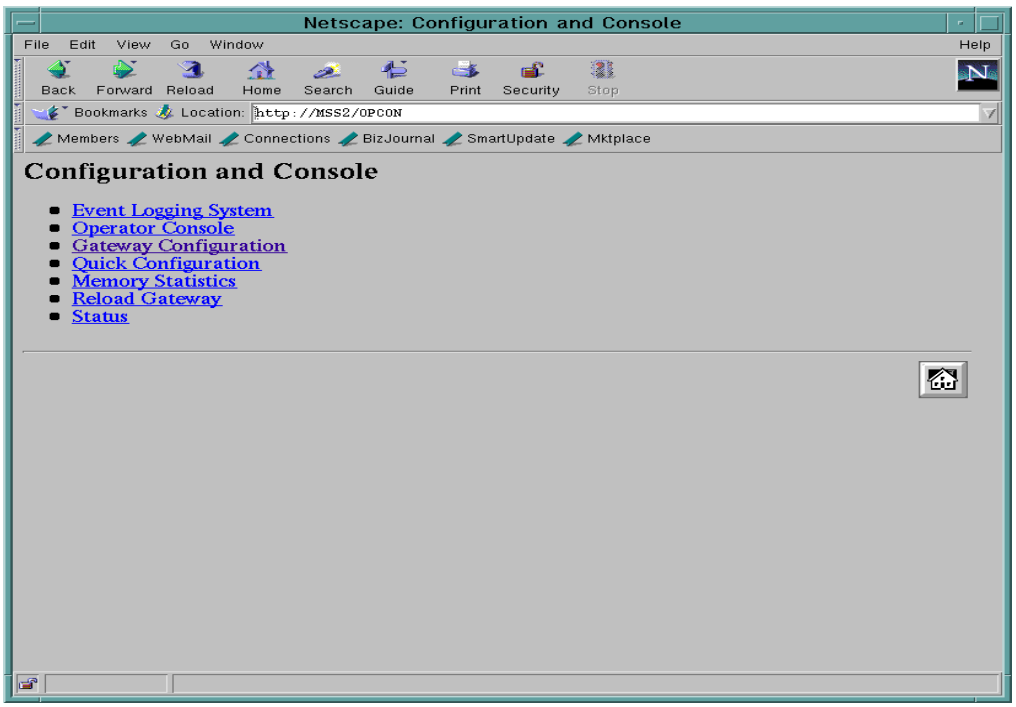


Figure 245. MSS Configuration and Console

Figure 245 shows the options available under the Configuration and Console page. This is a re-organization of the text based version accessed via the console. The major difference is that it has been converted to forms. This simplifies the configuration and monitoring tasks compared to that of the command line version using a text-based console.

On the right-hand side of the page, there is an icon that if selected will return to the MSS home page.

Note

1) The web caching feature of the Web browser should be disabled to avoid the Web browser from using a cached Web page, which may not represent the actual configuration or status on the MSS.

2) Only a single user may use the Web browser interface at any time. Otherwise modifications one user makes, will affect the actions of another user.

Figure 246 shows the configuration of a LEC interface of the MSS server.

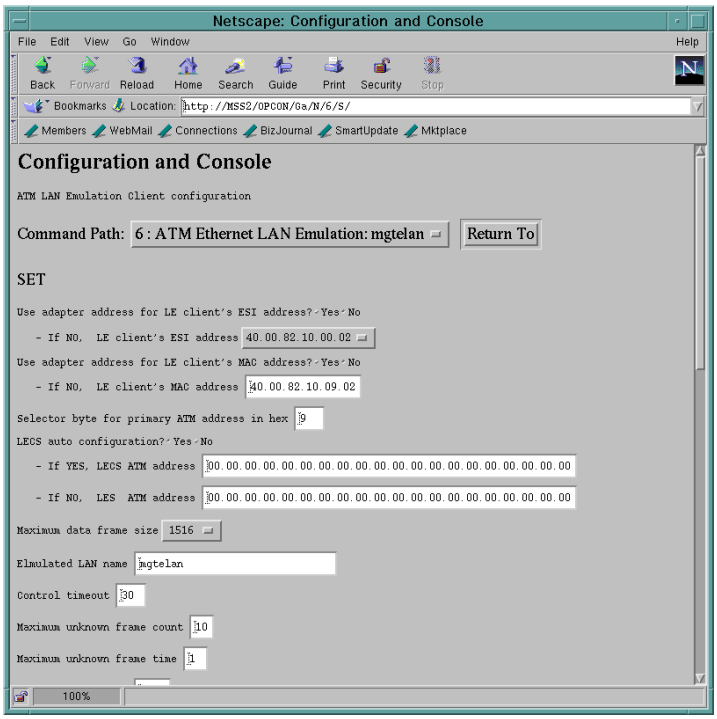


Figure 246. Example: Configuring One of the MSS LEC Interfaces

Figure 247 shows the Reload Gateway function that will restart the MSS server after a configuration change.

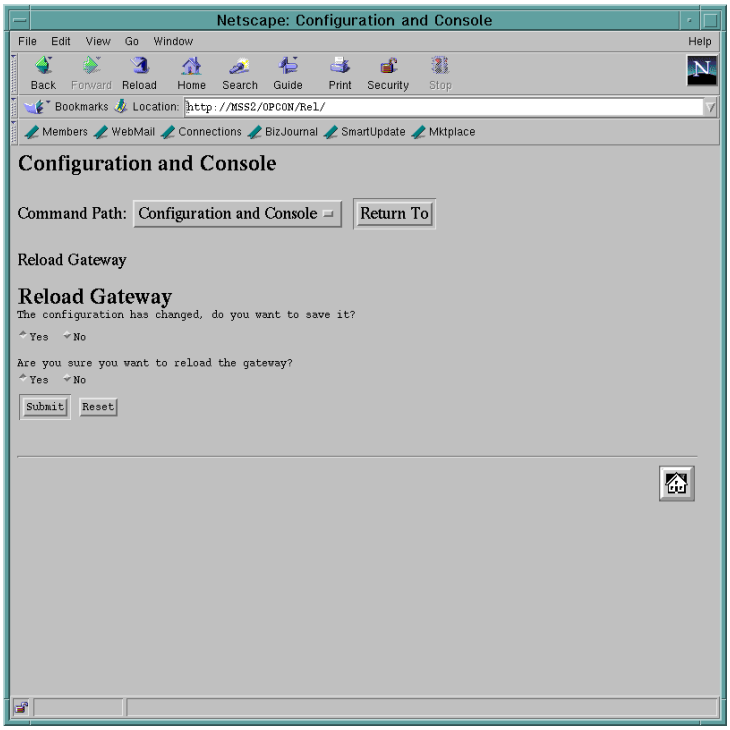


Figure 247. Restarting the MSS Server

The LEC status for the ELAN is shown in Figure 248 on page 266.

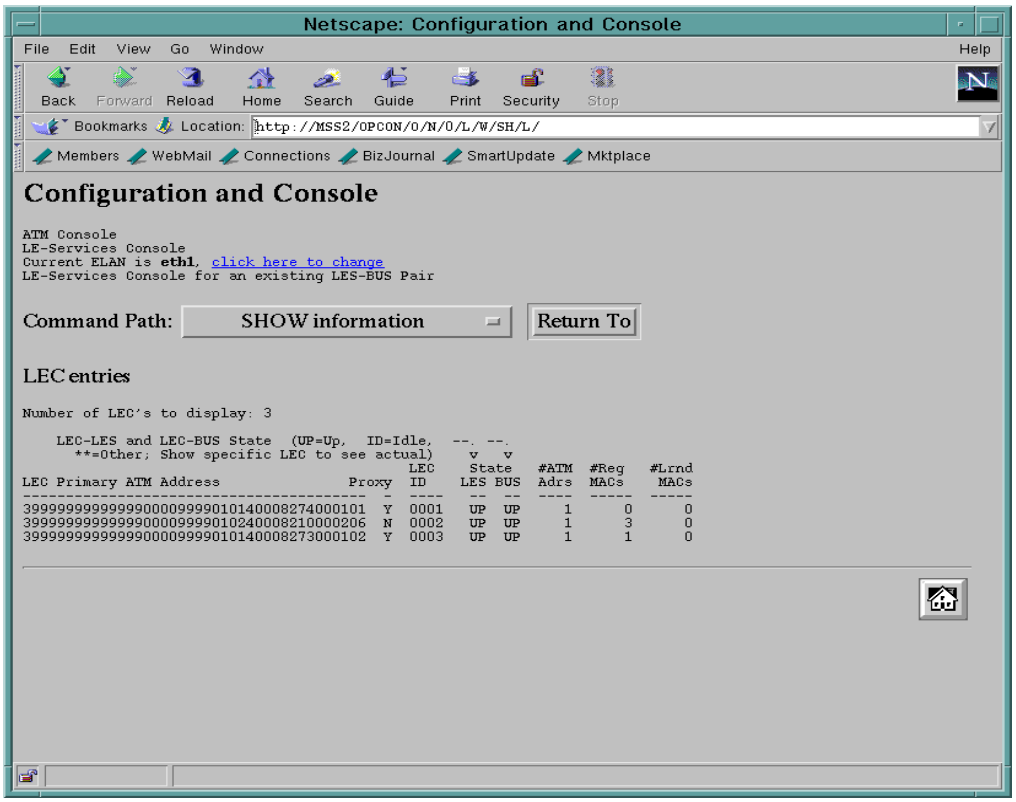


Figure 248. LES/ELAN Status: LECs Within an Elan

Figure 248 shows the equivalent output of one of the GWCON commands for showing all the LECs that have joined a particular ELAN.

7.8.2 IBM 8275-113 Ethernet Desktop Switch Example

Here we show an example of Web management of the 8275-113 switch. Accessing the 8275 home page is the same as accessing the MSS Home page. Before you can access the Web pages for the switch we are prompted for a user Id and password. The default user Id is ADMIN, which has no password.

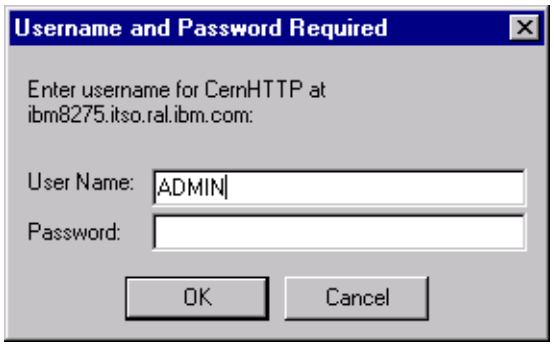


Figure 249. IBM 8275 User Authentication

The 8275 is shown in Figure 250.

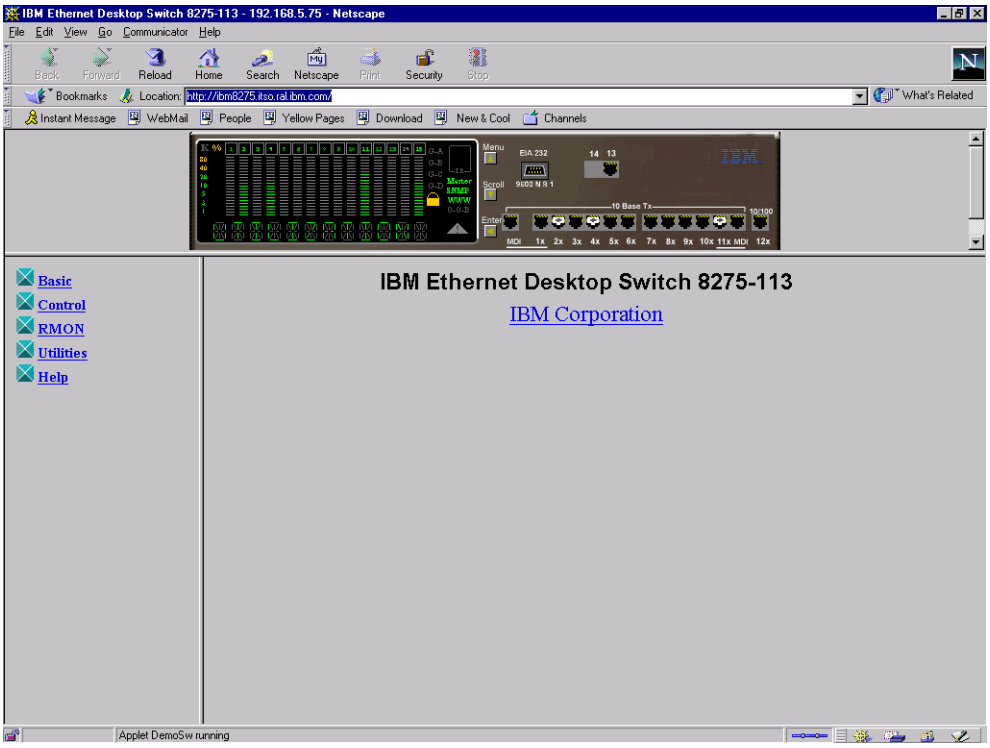


Figure 250. IBM 8275-113 Ethernet Switch Home Page

From this page, the configuration of the switch can be retrieved or updated. Also you can view the status of device and interfaces.

Chapter 8. RouteVision Suite

This chapter covers the RouteVision application, and shows examples of the management options using the 8273 and 8274. We show examples of using the RouteVision software to manage the status, configuration, performance and fault management for the 8274 connected to our network.

8.1 Installation

This section refers to the installation of the RouteVision 3.2 suite of products on the Windows NT platform. At the time of writing, this was the latest version of the product available.

The RouteVision product requires the following operating system and software:

- Pentium II 166MHz or greater processor (or similar)
- 64MB RAM (128MB is recommended)
- High color-capable SVGA video card
- 17" monitor with recommended resolution 1024 x 768
- 300MB free disk space
- Microsoft Windows NT 4.0 with Service Pack 3, or
- Microsoft Windows 95 (OSR 2.1/950B) with DCOM and Winsock2
- CD-ROM drive
- Network interface card
- TCP/IP stack

The installation is run from the CD-ROM or the files copied to the hard drive for later installation. The configuration and customization of RouteVision begin once the installation has completed, but it is important to set up the switches that are to be managed for access from the management station.

To set up the switches to be managed, the user must set an IP address on each switch, then set the SNMP Community String to match that which RouteVision will use. The IP address and other system parameters (name, location, etc.) are set from the `syscfg` and `modvl 1` commands under the system submenu. The command is `modvl 1` because the default group on all switches is 1. This can be achieved by using a local console connection to the switch, or by telnet access if a network connection exists. However, the changing of the IP address, if required, has to be performed from the local console, as the telnet session will be lost. By default, the following strings are used on the switch:

- public - read only access (GET SNMP requests only)
- public - read/write access (GET and SET SNMP requests)

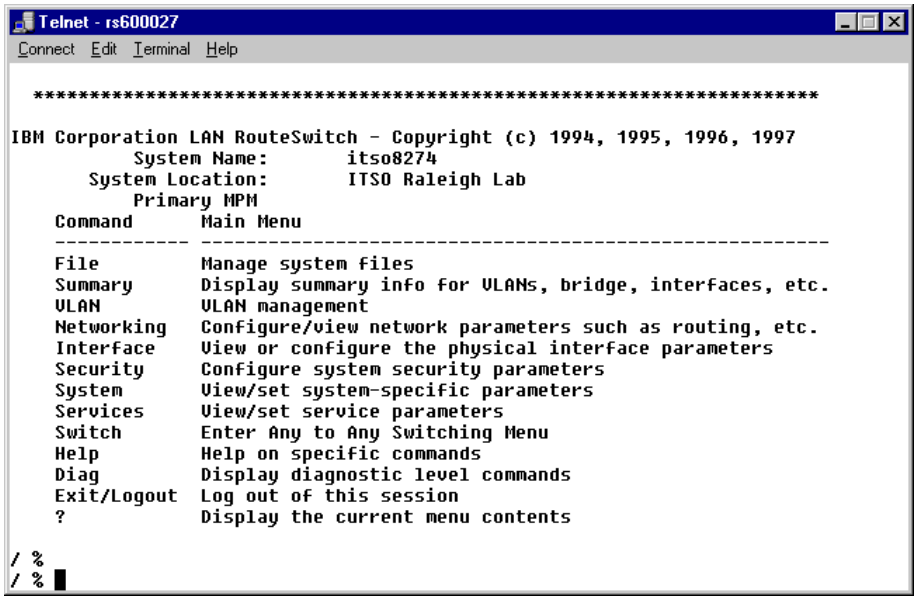


Figure 251. 8274 Console Main Menu

After logging into the 8274 you will be presented with the initial menu. From here type in `system` followed by pressing Return.

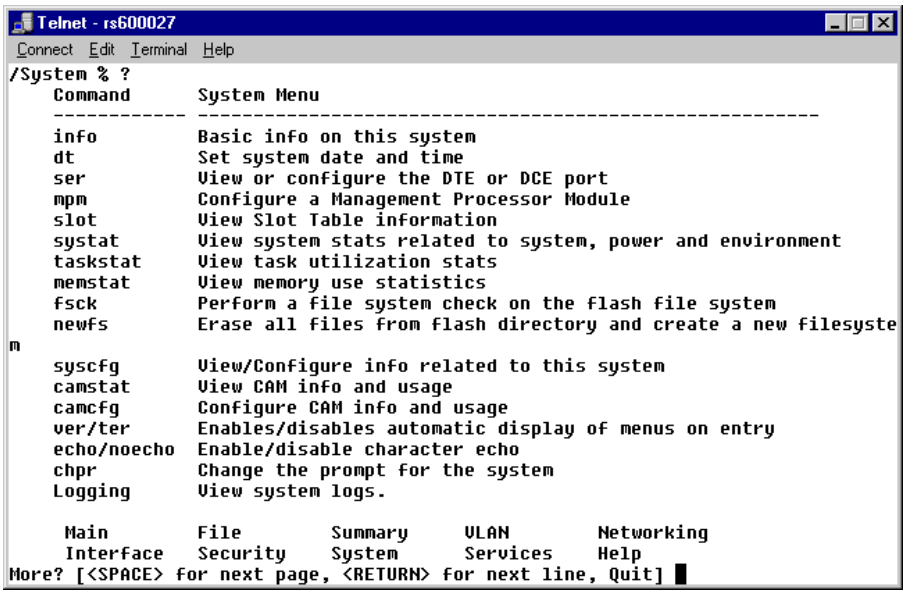


Figure 252. Commands Under the System Submenu

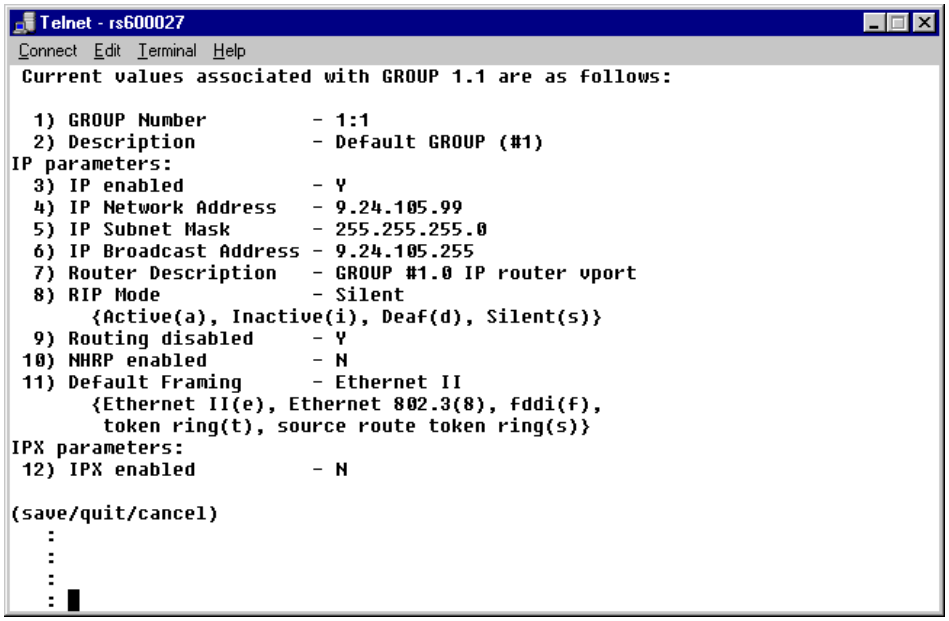


Figure 253. Output from the syscfg and modvl 1 Commands

The Community String can be changed by using the snmpc command from the networking submenu. From the snmpc command users can set the network management stations IP address, as well as set the SNMP trap parameters, such as the TCP port used for traps and the trap mask; where the user decides which traps will be forwarded from the switch to the NMS. It is also possible to configure the Remote Monitor (RMON) settings here, if there are already RMON probes running at that switch. The probes cannot be added from the local console interface.

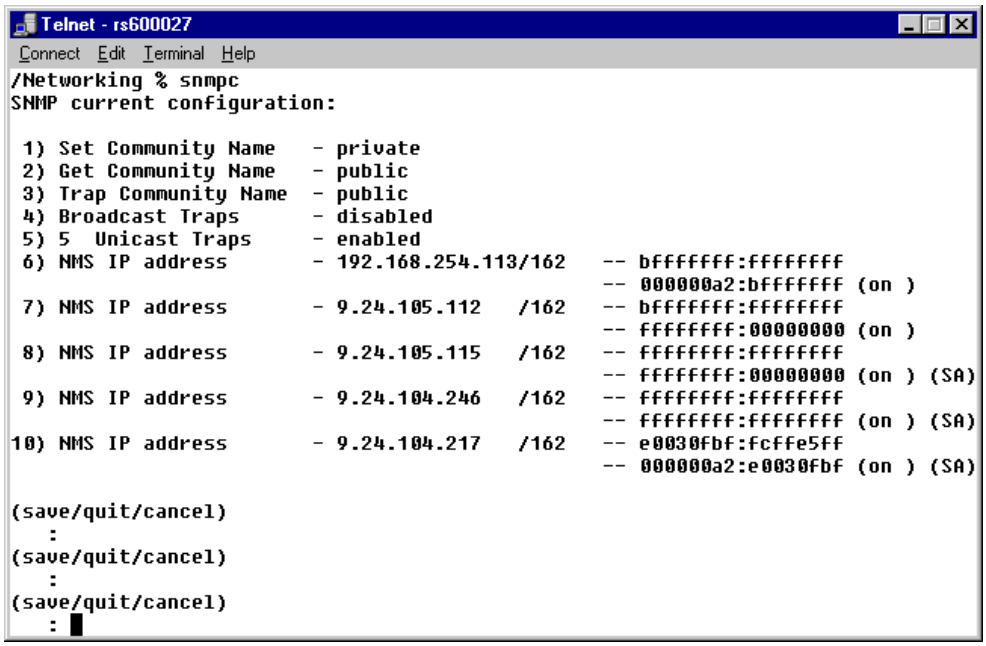


Figure 254. Output from the snmpc Command in the Networking Submenu

From the command line, to see the RMON probes defined type in the command probes.

```
/Networking % probes
                                RMON Probe Summary
Entry  Slot/Port  Flavor    Status    Time     System Resources
1001      3/   1   Ethernet  Active 35 hrs 13 mins    280 bytes
1002      3/   3   Ethernet  Active 35 hrs 13 mins    280 bytes
1003      3/   5   Ethernet  Active 35 hrs 13 mins    280 bytes
1004      3/   7   Ethernet  Active 13 hrs 52 mins    280 bytes
```

Figure 255. Output from the probes Command

Another recommendation is to create a common group for all switches that can serve as network management access. This will allow all switches to appear in the same subnet, making administration easier. All switches in this group should include a connection or trunk service for that NMS group.

Further information can be found in the RouteSwitch manuals and the *RouteSwitch Implementation Guide,* SG24-4881.

The installation of the RouteVision code is straightforward, as all the user needs to run is the setup.exe program, which is in the disk1 directory of the product CD. The following window will then appear.

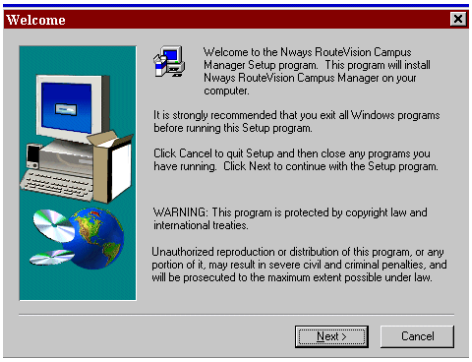


Figure 256. Installation Screen

Once the license agreement window has been negotiated, the user can decide where to install the program. The default option in the installation program is set to C:\Program Files\RouteVision. However, it can be changed by using the Browse button on the panel. It is advisable to change this to a drive with the requisite of 300MB free space, as the products will require this space for databases and storing information (such as performance data, event data, etc.).

You will also be prompted for the installation directory.

Once the directory path has been decided upon, the user can then decide whether to let the program install with the default setting, or choose a customized install. The custom install options let the user decide whether or not to install the help files as well as the program files. The total installation requirement only amounts to 42MB, so it is advisable to install the help files.

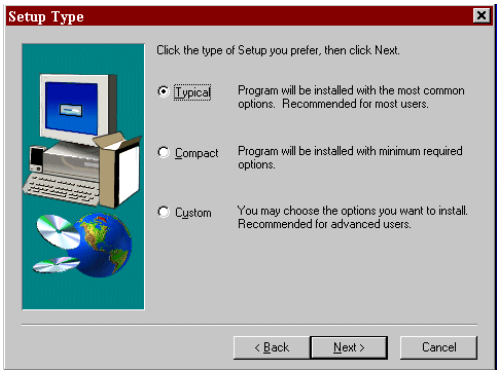


Figure 257. Installation Setup Options Screen

Once the software is installed we can start the discovery.

8.2 Discovery

When you first execute the program, the Discovery application automatically opens. The Discovery application is used to discover existing network regions and learn basic chassis information about the devices that exist on those regions. This information is written into the program's database and is available to all of the program's applications. Discovery continues to poll the devices that it has discovered at user-configurable interludes to ensure that the devices are up and that the database information is still valid.You must use the Discovery application before you can use any other application.

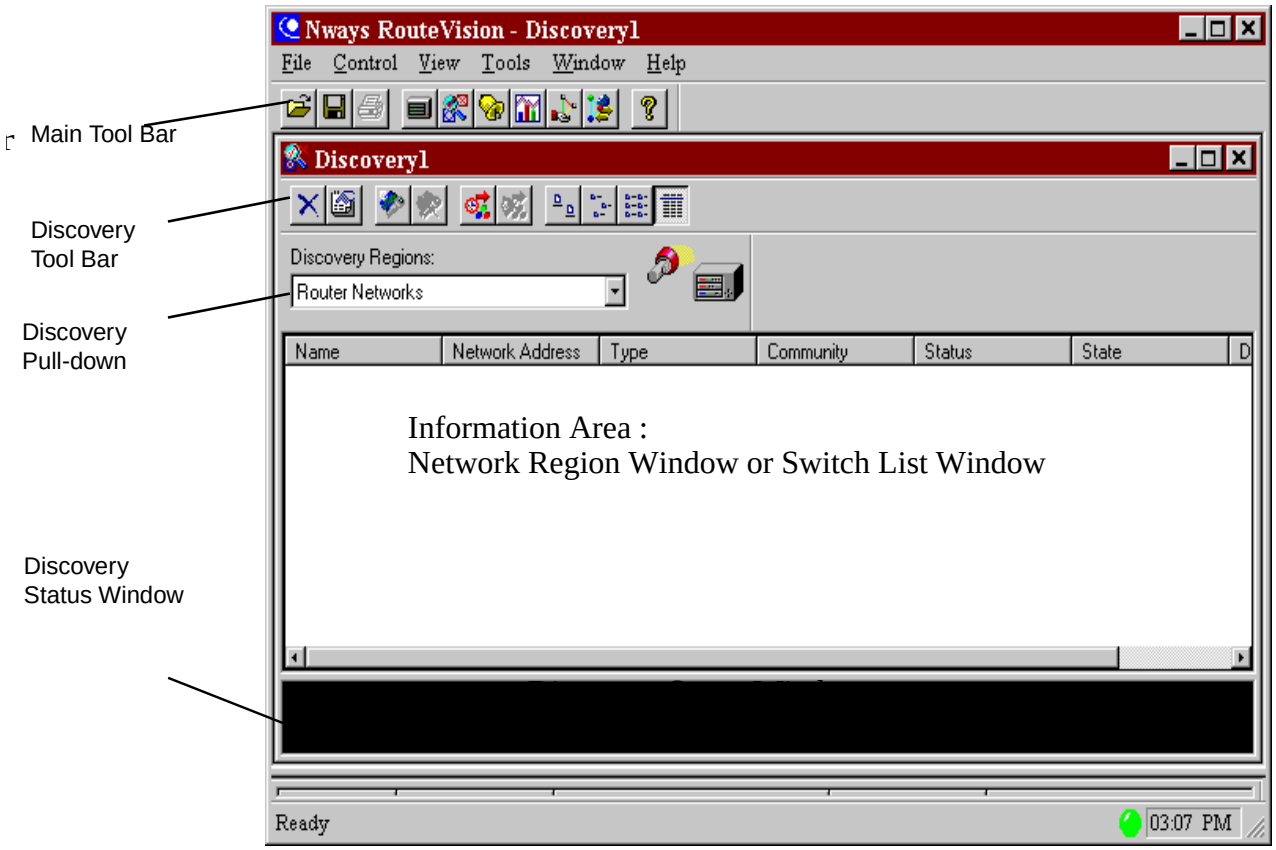


Figure 258. RouteVision Discovery Application Window when First Opened

Discovery can be performed using the Router Networks discovery process, by using the VLAN Advertisement Protocol (VAP) discovery process, by defining a discovery subnet or address range, or by defining individual devices. Once Discovery is complete, you can configure polling individually for each region. In this scenario, the devices to be discovered were defined individually. The Discovery icon on the main tool-bar can also be used to open different Discovery regions, making it possible to segment a network from the management perspective. Each discovery region could then be administered with different polling intervals, etc.

Whatever Discovery method is used, Discovery will not discover third-party devices.

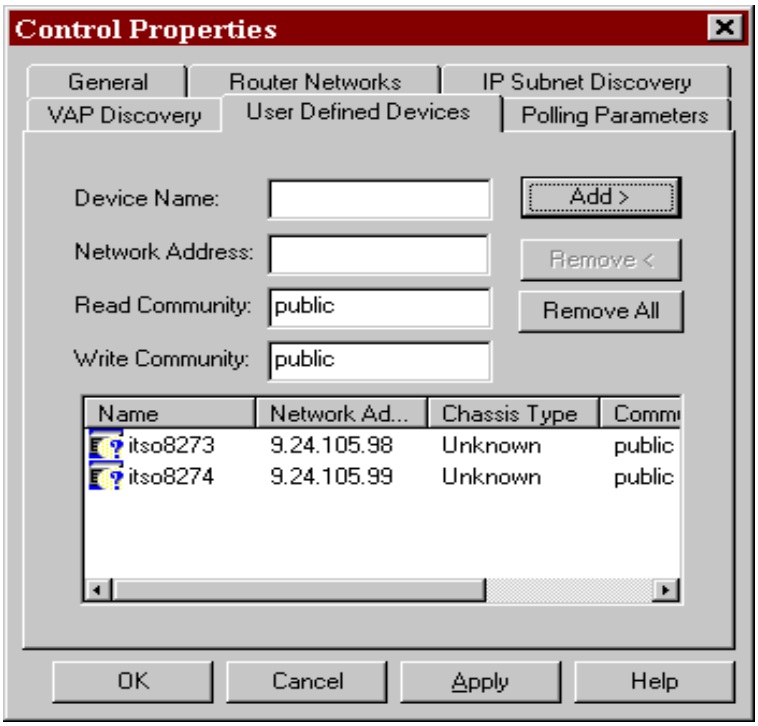


Figure 259. Control Properties Window of Discovery Application

The window above was used to define the individual devices that are going to be managed by RouteVision. Once they have been defined, the polling action can begin. When polling begins for the first time, a box opens that requests a discovery gateway, which is usually the RouteSwitch at the center of the network; the device with the most knowledge of the other devices in the network. In this window, the user also defines the Read Community name, so as to have access to the network information on this device.

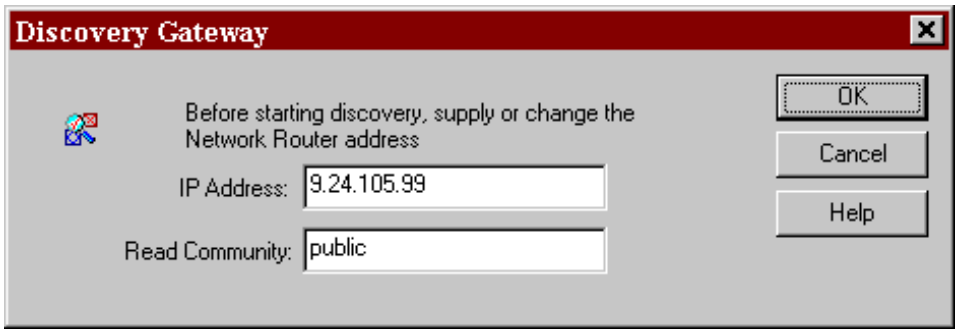


Figure 260. Discovery Gateway Window

From the main RouteVision screen click on the device followed by **Poll**.

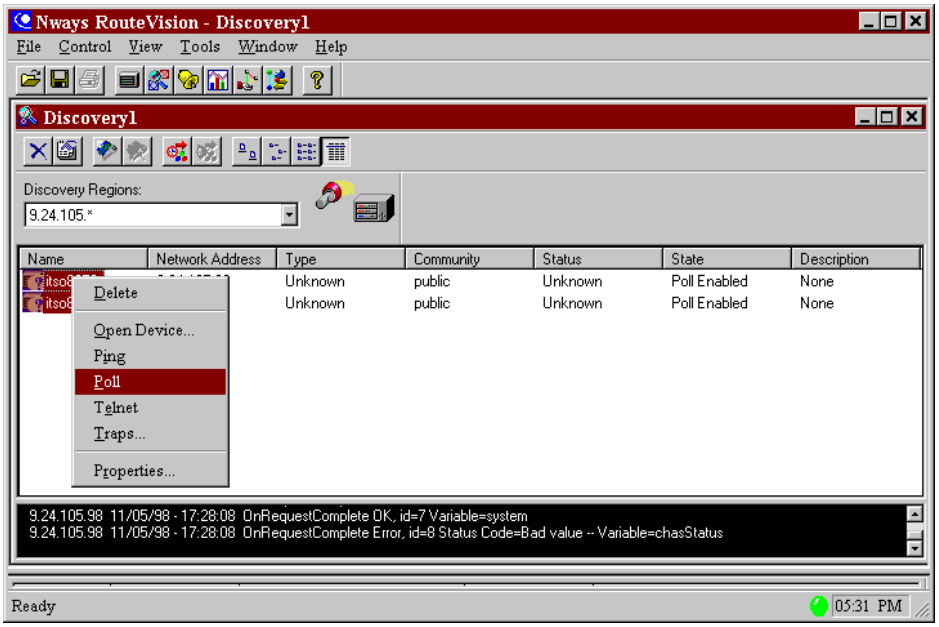


Figure 261. Discovery Polling of Defined Devices

Once the device has been polled its information is displayed, as shown in Figure 262 on page 276.

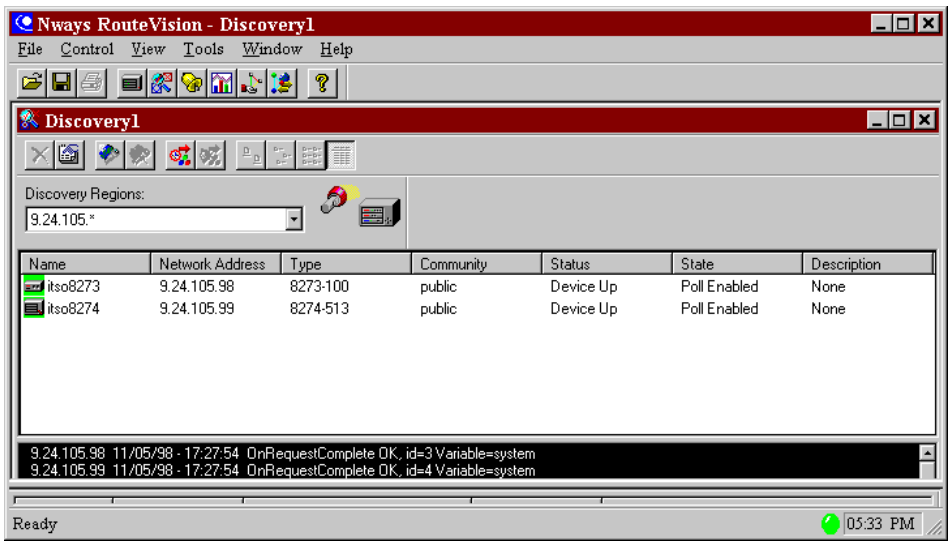


Figure 262. Completed Discovery Window

Once discovered, the user can customize the control properties on a device or region basis, altering the polling interval and time-out values for instance. In this scenario, the polling interval was set to 10 minutes.

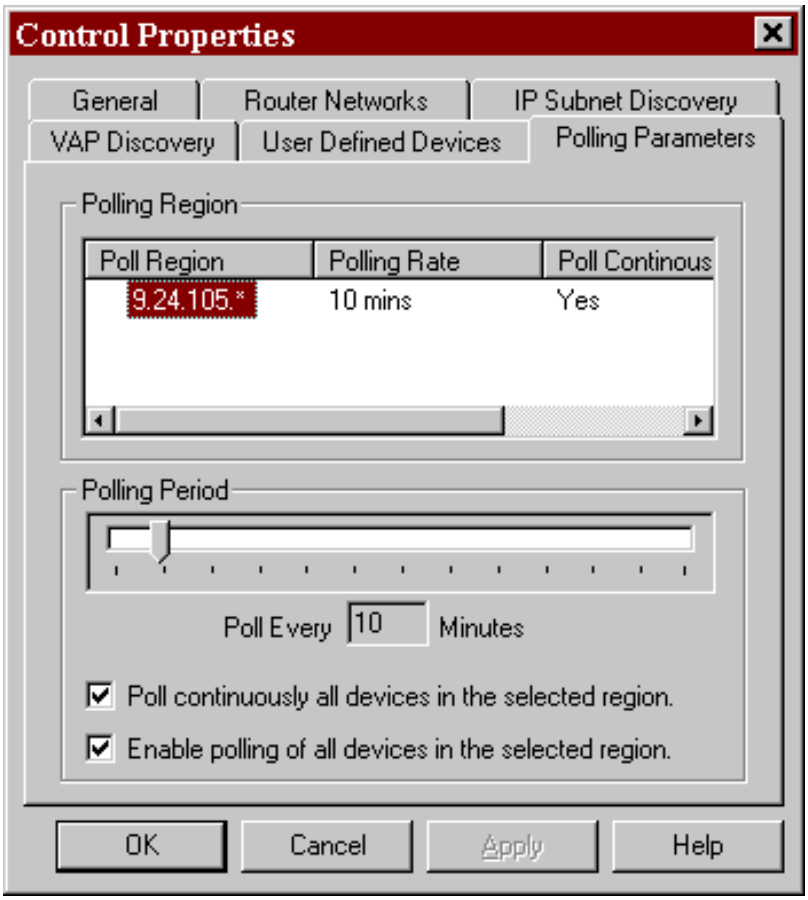


Figure 263. Control Properties Window - Polling Parameters

These intervals are used to automatically update the database information on each polled device. The polling light at the bottom of the screen is an indicator of the status of communication with the devices that have been discovered. This light appears at the bottom of any active screen. Green indicates that the last request for data was successful; yellow indicates that data is being requested from a device; and red indicates that the requested data could not be retrieved.

8.2.1 Integration

RouteVision can be integrated to run in conjunction with the IBM Nways Workgroup Manager for Windows NT and Nways Manager for AIX products. When selecting, for example an 8274, from the relevant view, double-clicking will open the RouteVision application window.

The integration of RouteVision under Nways Manager for AIX is handled by the installation procedure, RouteVision being added to the list of product-specific modules (PSMs) and Java Management Applications (JMAs) that are used to perform device management. The following set of panels shows how to integrate RouteVision on the Nways Workgroup Manager for Windows NT platform.

First, select the relevant device from the network view and click on the **Options** menu pull-down. The option to select is the **Double-Click Action** item.

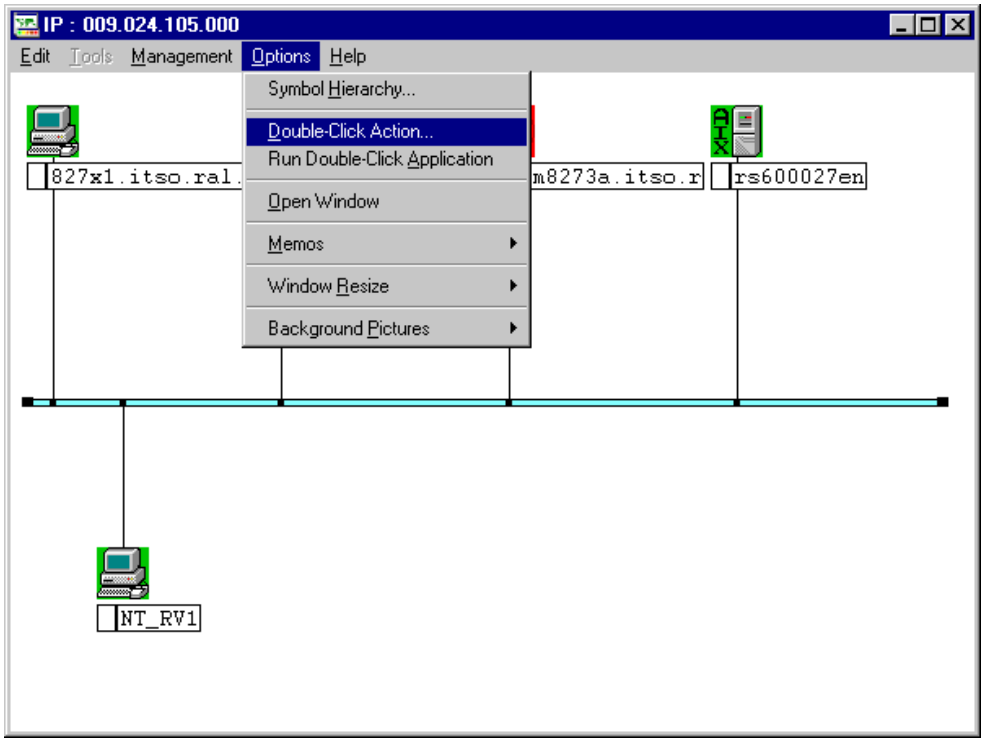


Figure 264. Selecting Double-Click Action from Workgroup Manager Window

This will open up the following window, where the user specifies the action to take. As can be seen, the user needs to specify that an application will run. There is no need to open a window as RouteVision will open its own window. The user then needs to specify the application, which is the RouteVision main task routevision.exe. Alternatively, the user can ask for the device management task only (routemanager.exe), or the SNMP MIB browser function (mibbrowser.exe). Clicking **OK** will set the action up.

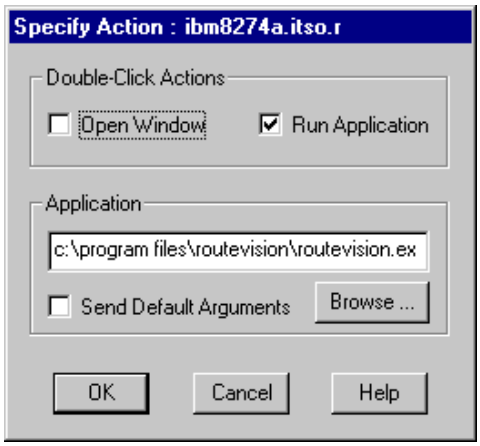


Figure 265. Setting the Double-Click Action

Now, to open the RouteVision application, the user just double-clicks on the 8274. This action only works on the object that it has been set for, which means that the user has to set this double-click action for each RouteSwitch device in

the network. This is required for the 8274, 8276 and 8277 as they have no device management application (either PSM or JMA) under the Nways management platform. The same cannot be said for the 8273, which has a JMA under both the AIX and NT Nways management platforms. Therefore, it may be best to not set a double-click action on the 8273, as it can still be accessed by the RouteVision application when launched against another RouteSwitch device.

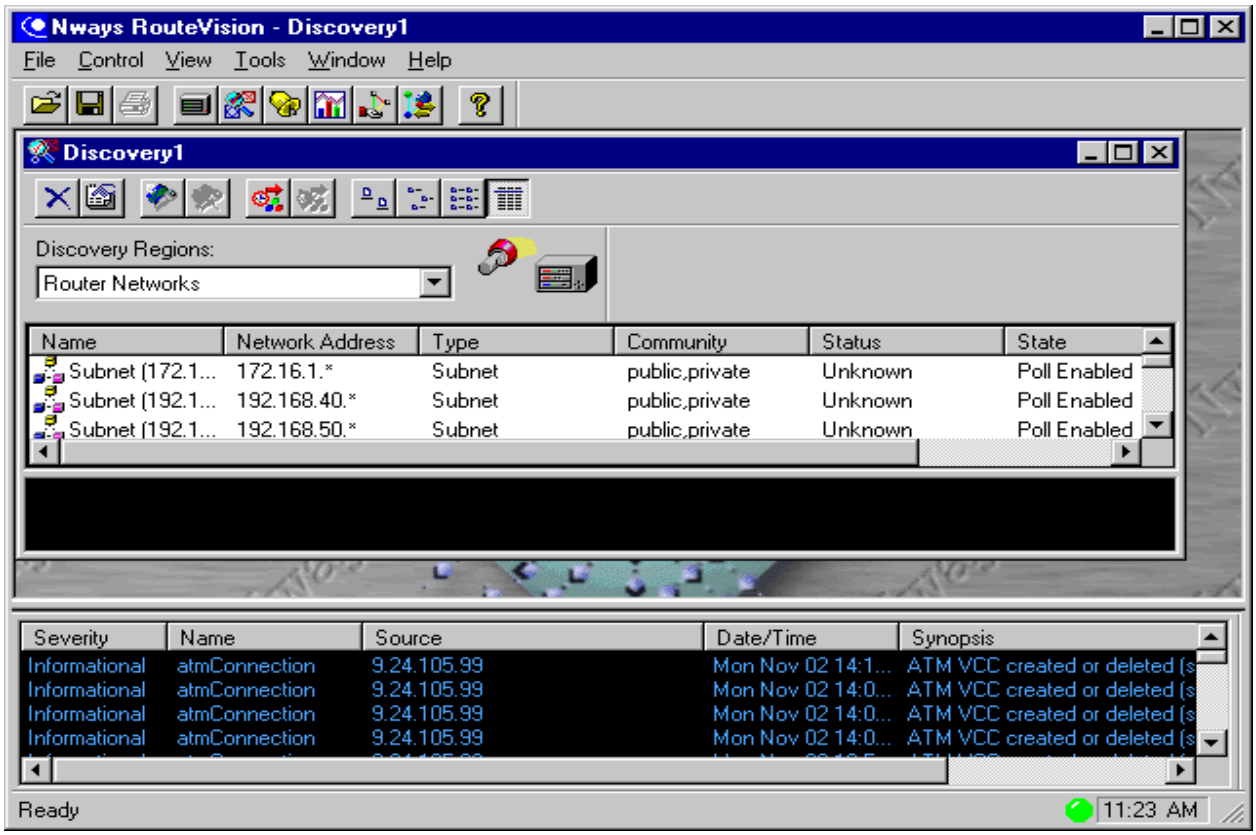


Figure 266. RouteVision Main Window

This window will provide access to all the RouteVision functions.

8.3 Examples of Using RouteVision

This section will provide a brief overview of the management options provided by the RouteVision product suite, using an 8274 as the sample device.

8.3.1 Configuration

The RouteVision product supports dynamic configuration of the RouteSwitch devices. This is performed by accessing the device either through telnet or, more suitably, via the device management window. To access this window, the user can either double-click on a device in the discovery window list or use the right-hand mouse button and select **Open Device** from the context menu that appears. It is also possible to open the device view by clicking on the Devices icon on the main tool-bar and selecting the device to open from the list of discovered devices in the window that appears.

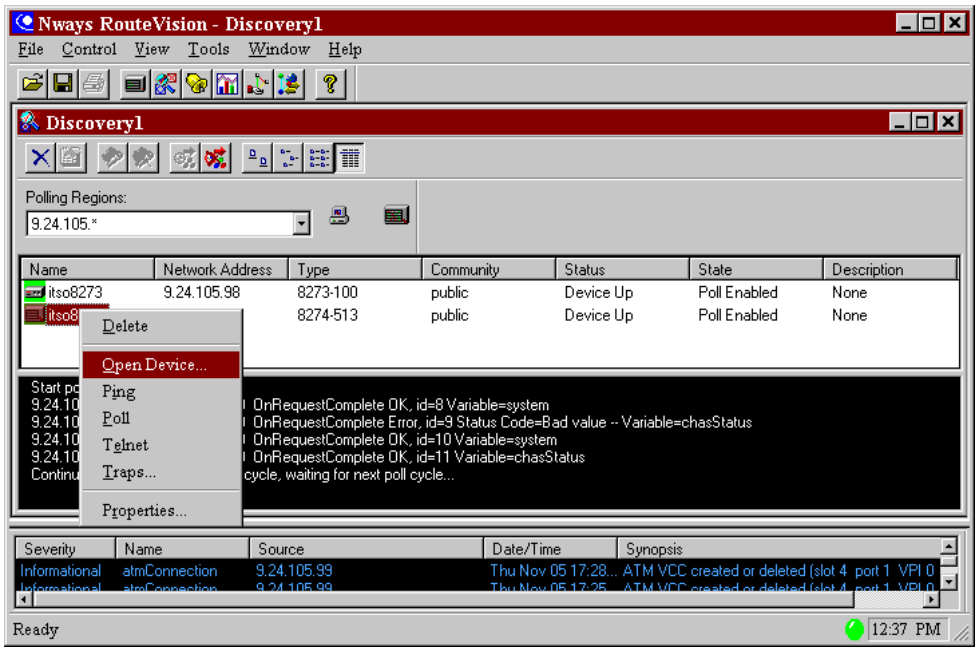


Figure 267. Opening Device View from Discovery Window

This will open up the device view window, as shown below.

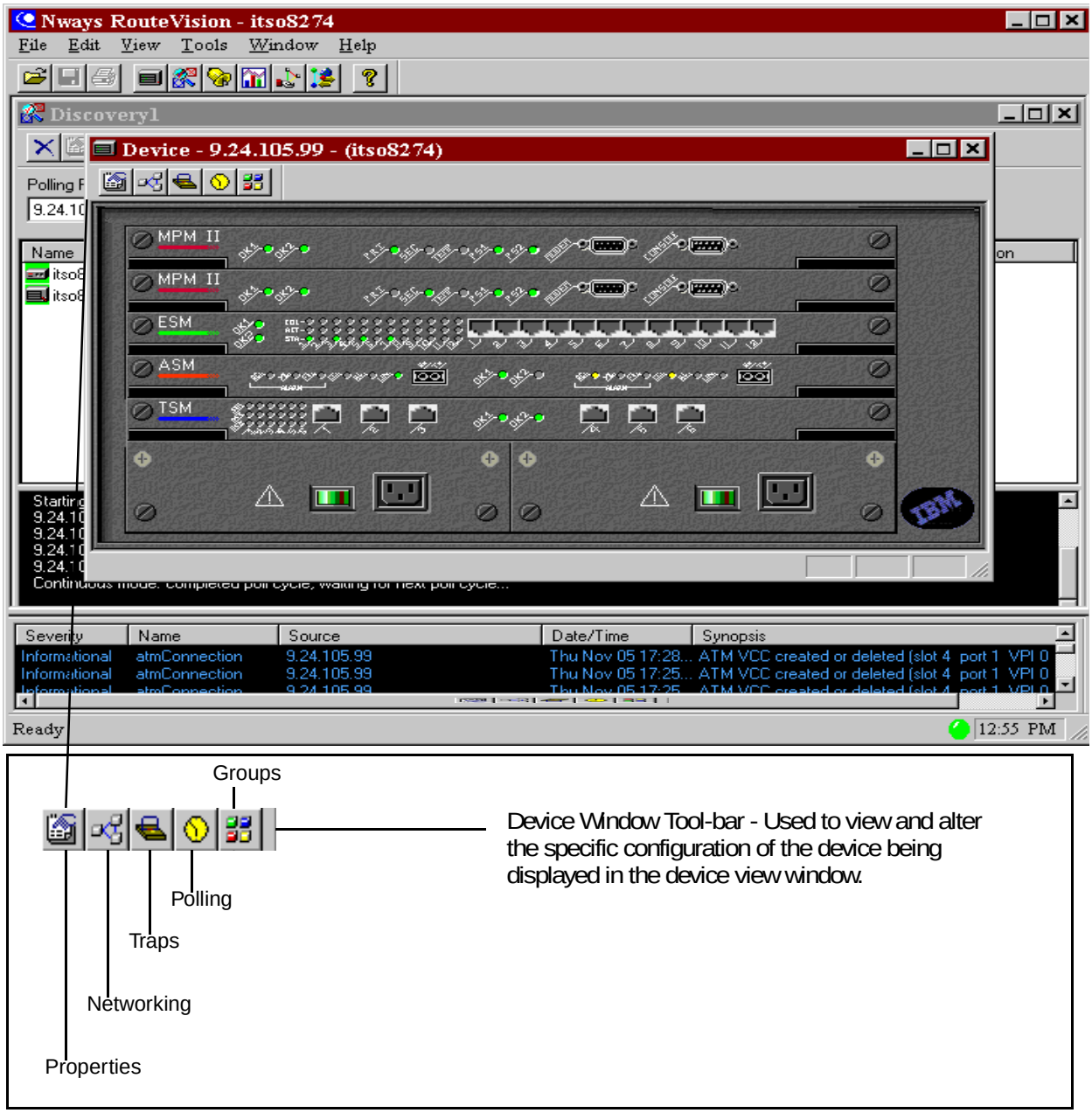


Figure 268. Device View Window

The device view window floats on top of the Discovery window, so it can only be viewed with that window active. From this view, it is possible to manage the 8274, with the ability to monitor and change device status and configuration. The only prerequisite required to make changes is that the management station has the correct SNMP SET Community access name configured.

The Properties pull-down menu item shows the Chassis Properties window for the device, where the basic system hardware configuration is displayed. This window can also be accessed by clicking with the right-hand mouse button on any area of the displayed device except a module. It can be used to display the

physical information about the system. The General, Environment, Information, System and Services windows provide basic information on the device such as its name, IP address, location, power/temperature status, uptime and services supported.

The Module tab has the same effect as the slot command from the console interface, showing module type and description, part and serial number, hardware and firmware levels, LED status, MAC address and manufacturing date.

The Physical Ports tab has the same effect as the `vi` command from the console interface. It can be used to list all of the ports on the device and their media type, interface index number, status and port/slot assignment. There are also some basic statistics available for each port, based on layer 1 (physical layer) activity.

The final tab is the Interfaces tab, which is used to list the interfaces on the box, their operational and administrative state, the interface speeds and the physical address on each interface. There are also some basic statistics available for the physical layer traffic on the interfaces.

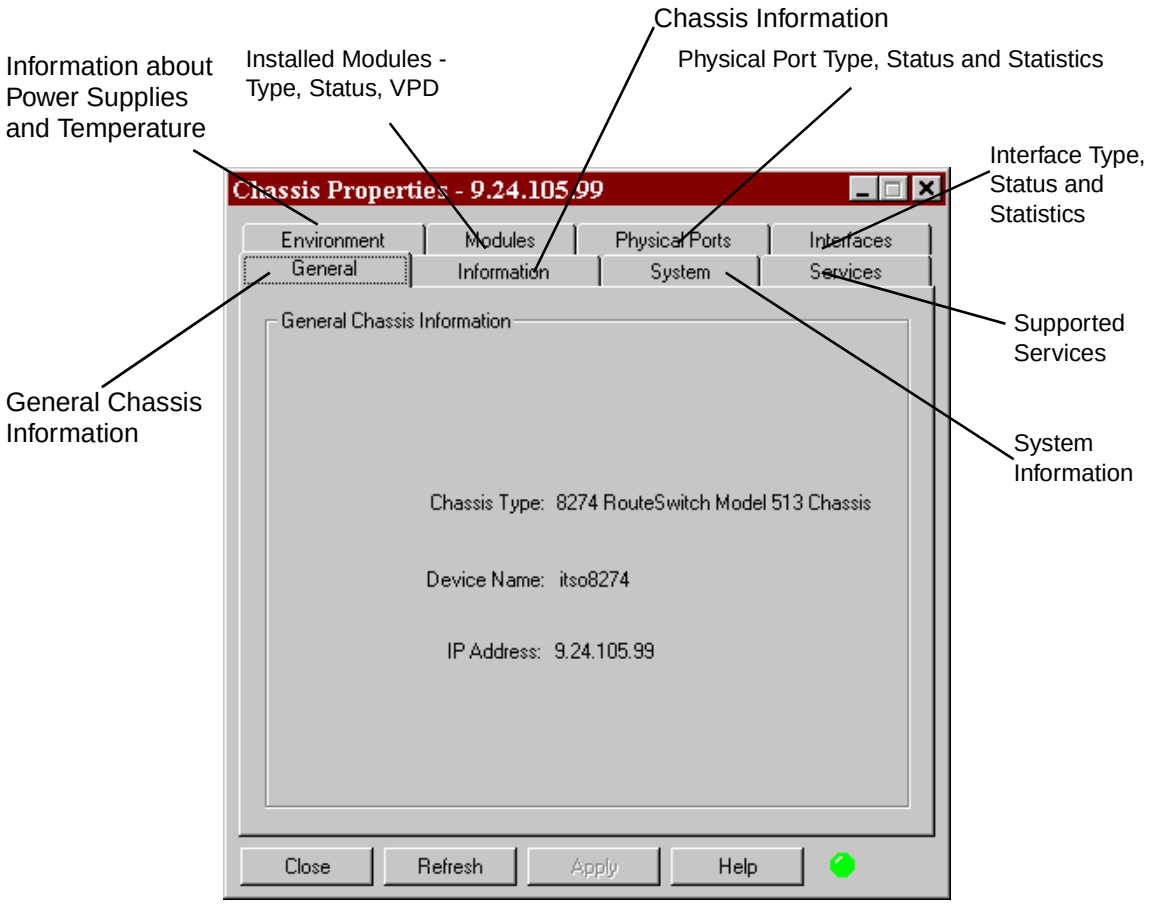


Figure 269. Chassis Properties Window

By selecting a Management Processor Module (MPM) with the right-hand mouse button, it is possible to display the module information as per the Chassis Properties window, but with extra details such as the MPM redundancy status

and the file contents of the flash/simm memory. By selecting any other module with the right-hand mouse button, it is possible to view the module information as presented in the Chassis Properties window. Selecting an individual port on any module with the right-hand button allows the user to view the port configuration. The information displayed includes the general configuration parameters on the port, as well as media-specific information. With the correct community name set, some of this configuration information can be changed from RouteVision.

Ethernet port properties are shown in Figure 270.

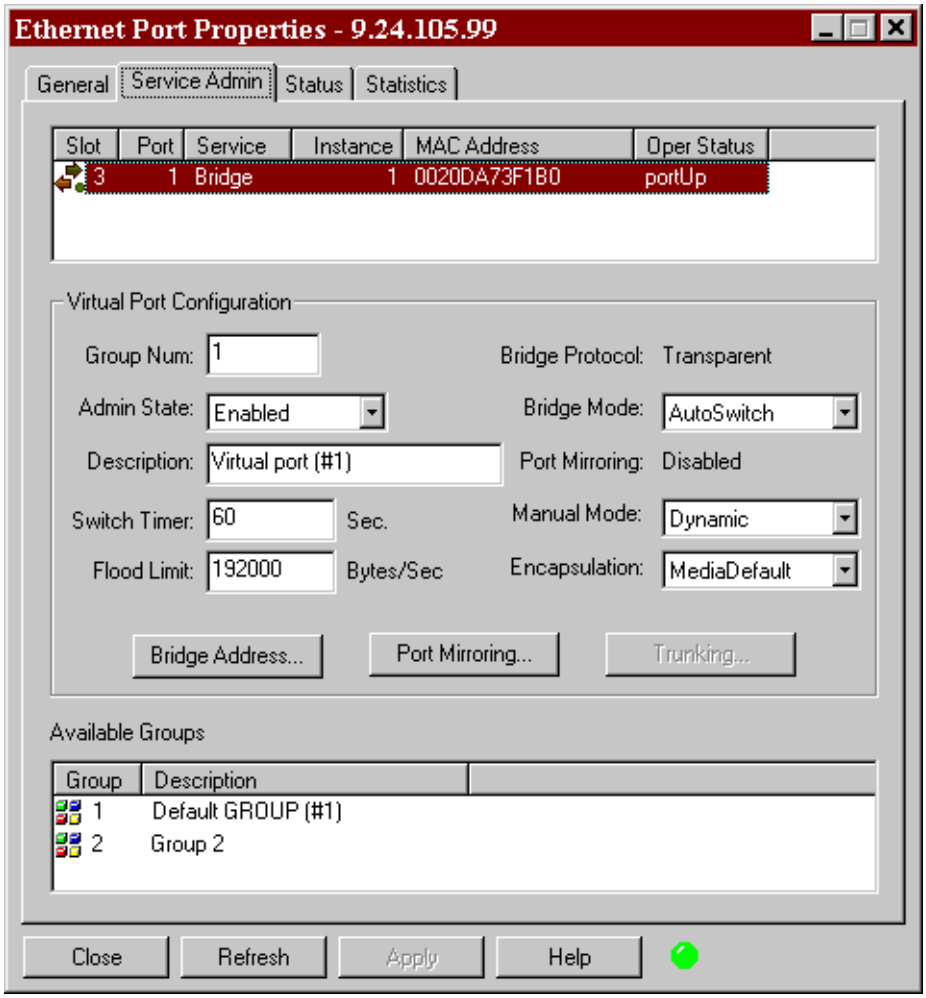


Figure 270. Ethernet Port Properties Window

Token-ring port properties are shown in Figure 271 on page 284.

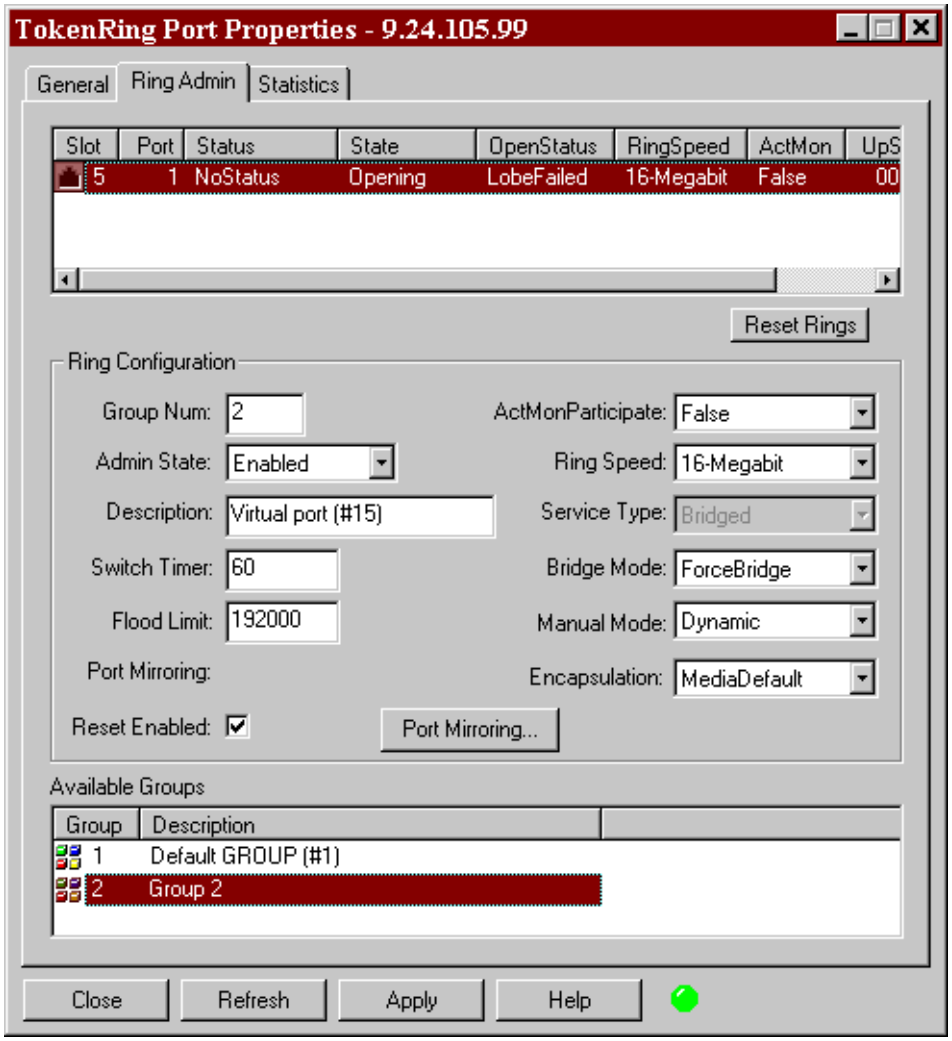


Figure 271. Token-Ring Port Properties Window

The ATM Port window allows the creation of ATM services, connections and LECs, as well as setting the type of ATM Forum-compliant interface to be used, (see Figure 272 on page 285).

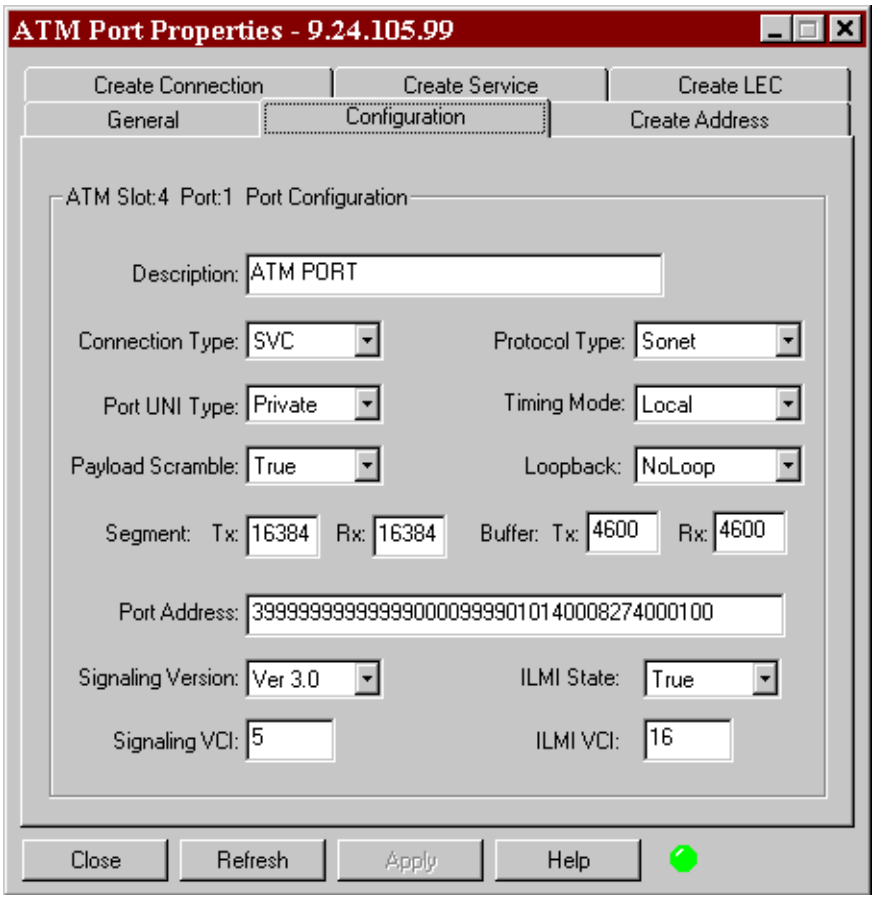


Figure 272. ATM Port Properties Window

By default, all ports are assigned to a pre-defined default group, known as Default GROUP (#1). To allocate new groups and assign ports to them, the user has to start the Group Properties window from the device view tool bar.

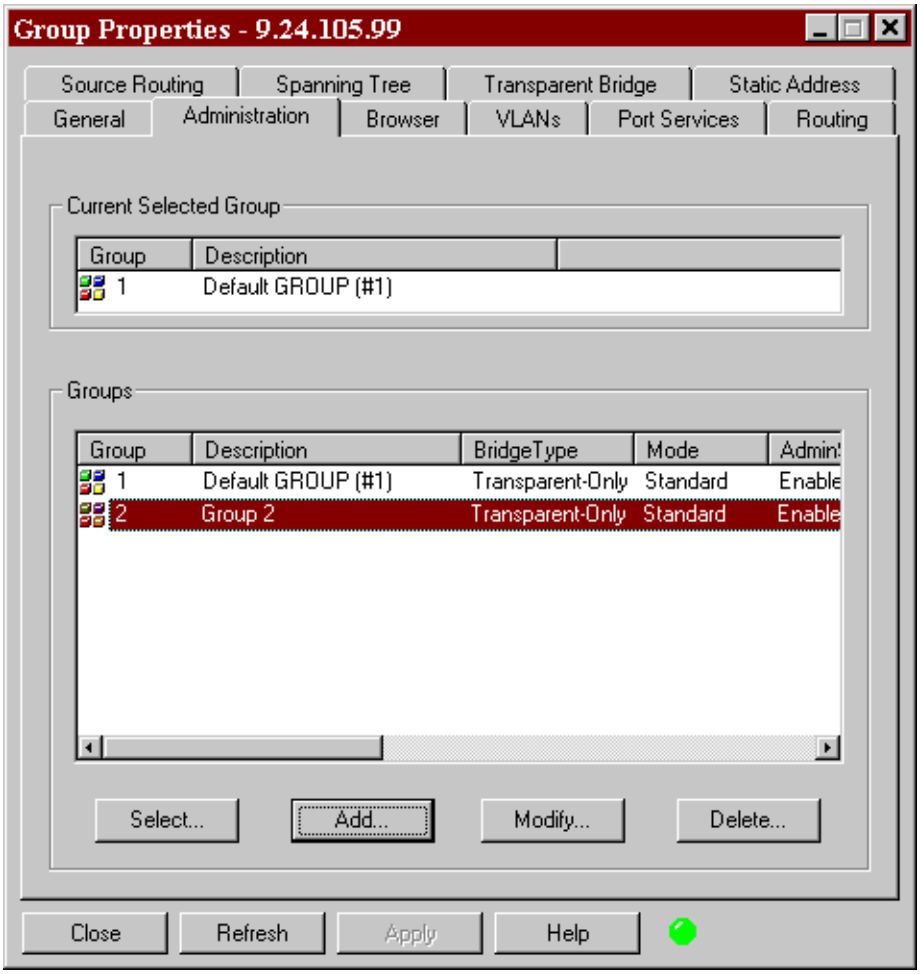


Figure 273. Group Properties Window

This window is the starting point for administration of all the groups of ports that exist on the device. From here, new groups can be created, ports can be re-assigned to different groups, bridging and routing administration can be performed as well as VLAN administration. In fact, RouteVision has to be used to run VLAN monitoring and administration for the RouteSwitch products. There are several proprietary ATM MIBs in the RouteSwitch firmware that IBM Nways management products cannot work with. It is also possible to perform the VLA administration by selecting the **VLANs** icon on the main tool bar.

One other area of configuration that can be accessed within RouteVision is the Services administration function. This is opened by selecting the **Services** icon.

8.3.2 Services

The Services function will perform the creation of maps, to help with network organization and administration. Before Service can be used to manage these functions, there must be a database entry for all device in the network (that is, they have been discovered) and there must also be information on the physical connections between the devices in the network; including slot and port number, IP addresses or names of the devices.

Once this information has been gathered, the user can create maps, then view, modify or delete them. The user also has the ability to create entities in the maps to represent servers, clouds, switches and rings, and can also delete any of these entities. The entities will have certain properties, which can be displayed and changed. The maps are a representation of the physical topology of the network only, but all of the logical connections and services running on the devices in the map can be viewed and modified from this map. Therefore, it is possible to run the configuration of all the network services from this function by first mapping the existing physical connections between devices and then adding any further physical connections followed by the logical connections, services and other logical entities required by the network. It is then possible to create maps of these logical resources, which can then be used to show the network topology from both the physical and the logical aspects. Note that this is possible only with RouteSwitch products. It is not possible to add non-RouteSwitch devices to the map and configure resources on them.

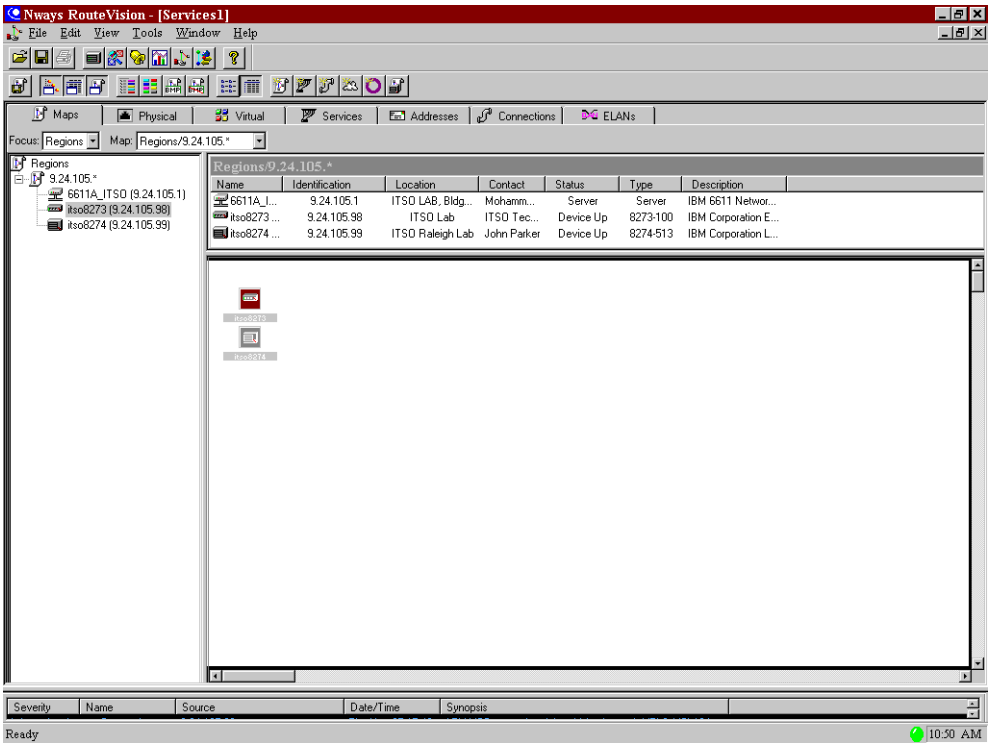


Figure 274. RouteVision Services Window

8.3.3 Performance

There are several locations for performance information within RouteVision. As discussed previously, there are some physical layer statistics available for the physical ports and interfaces on a module, which can be viewed from the device windows. There is also the possibility to view some networking statistics from the **Networking** icon on the device view tool-bar. By selecting this icon, it is possible to show information on the performance of SNMP, TCP, RIP, OSPF, UDP and so on.

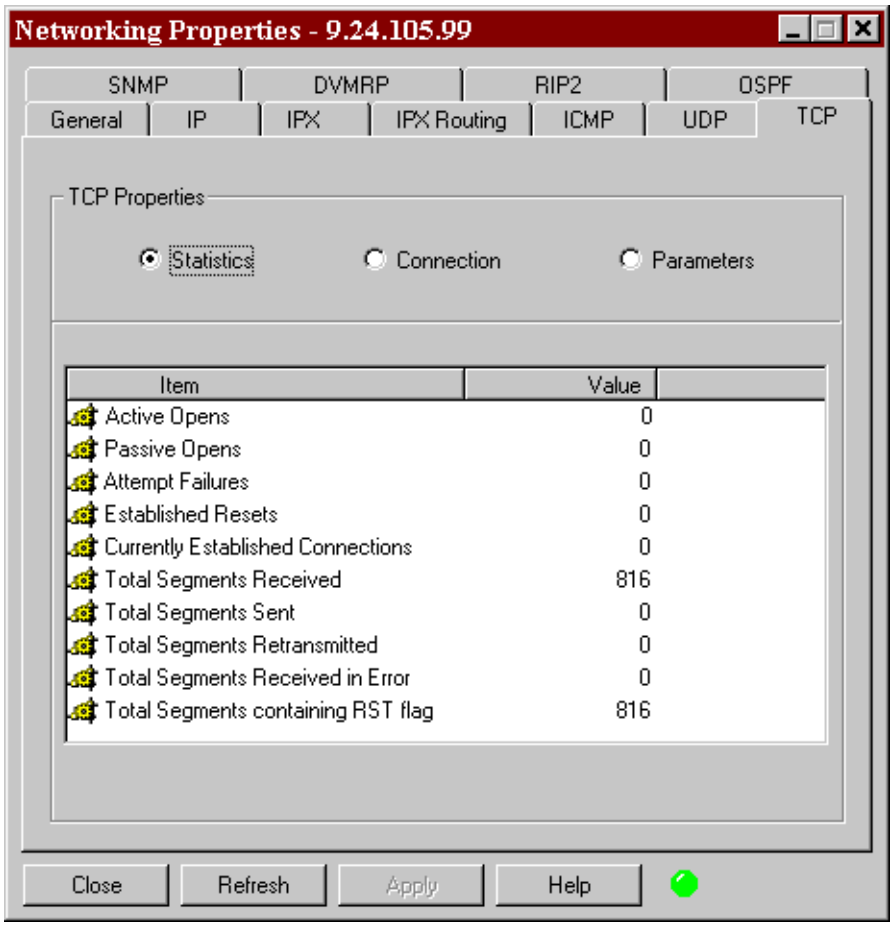


Figure 275. Networking Properties Window

This window is helpful to users trying to troubleshoot IP socket problems, routing errors, IPX broadcast problems and so on.

The Statistics icon on the main tool-bar can be used to launch the main statistics function within RouteVision, which can then be used to create and monitor statistical reporting views of the network and devices.

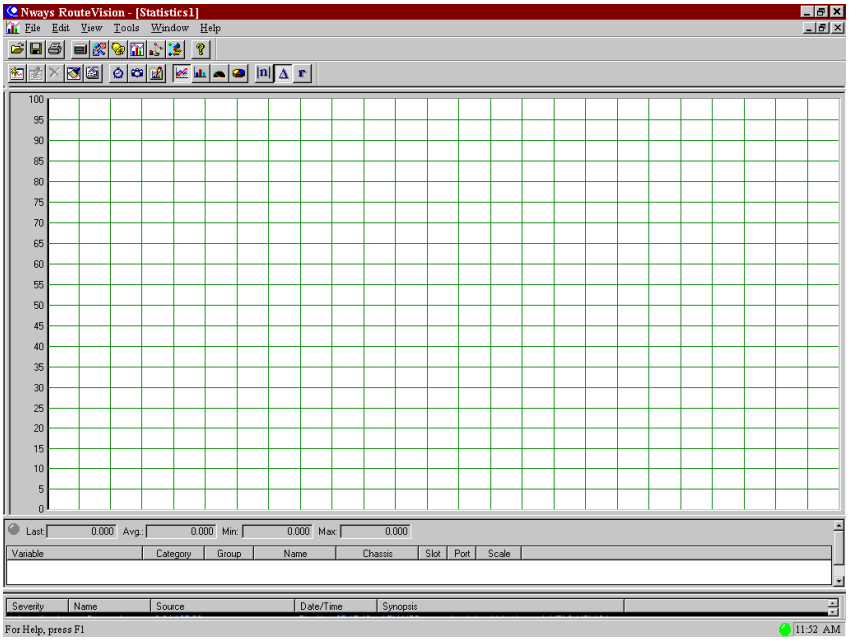


Figure 276. Main Statistics Window

The menu options are shown in the view of the tool-bar below.

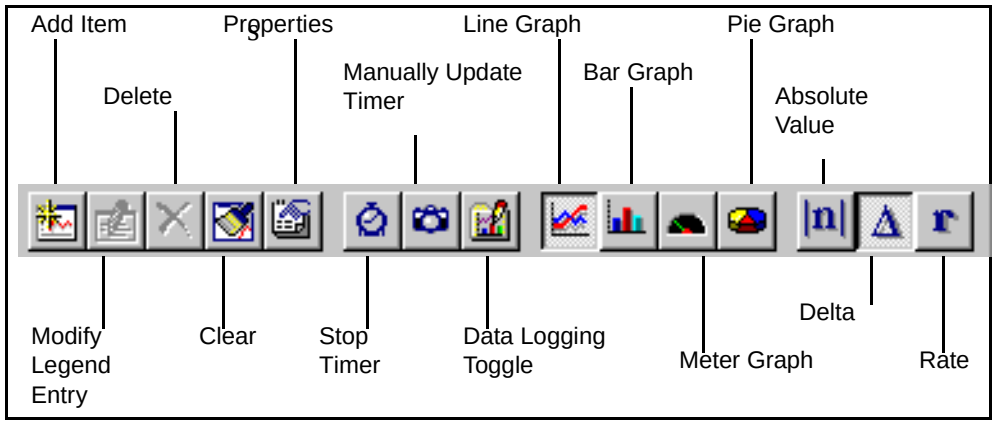


Figure 277. Statistics Tool-bar

The first action to be taken is to add in the devices you want to run statistical analysis on. To do so, click on the **Add Item** icon, which will list all of the discovered devices in the database. There is a second, empty window, on the right of selection list. When a device is selected on the left, then the right-hand window will display the available information from that device. In fact the right-hand window is a listing of all of the supported MIB information on that device.

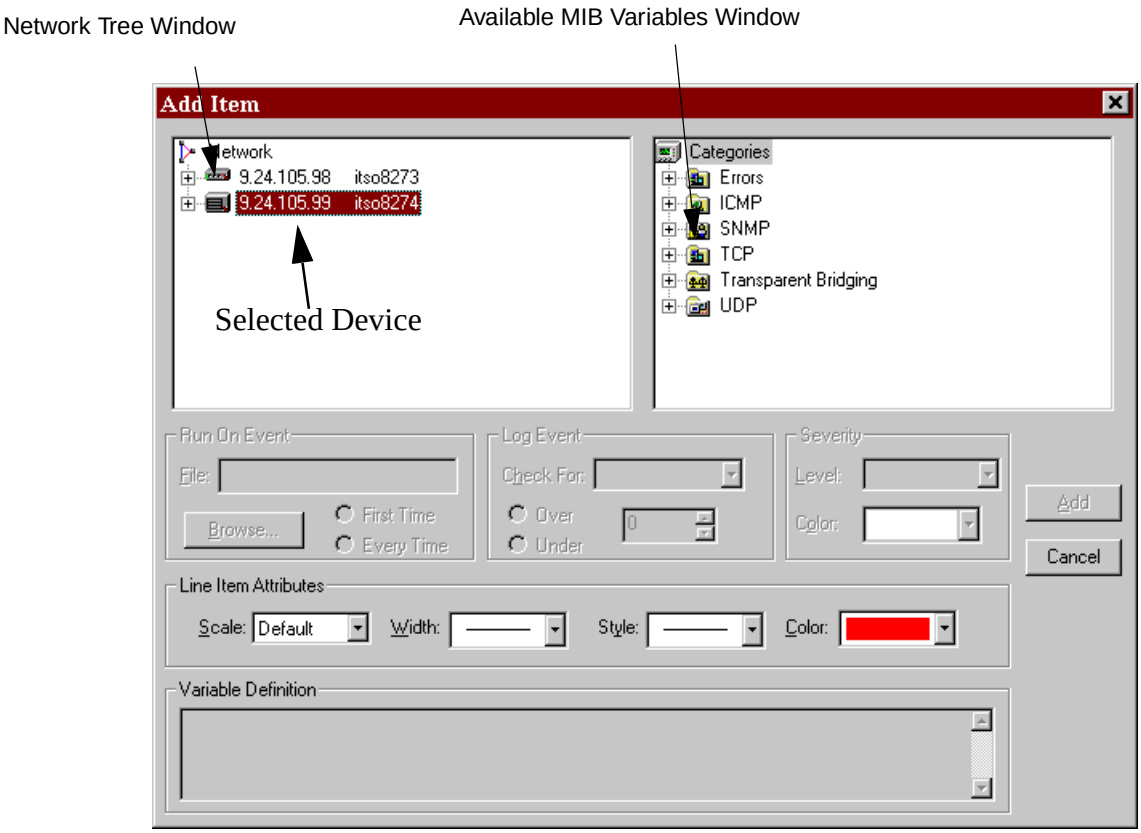


Figure 278. Preliminary Statistics Selection Window

From here double-click on the device (itso8274).

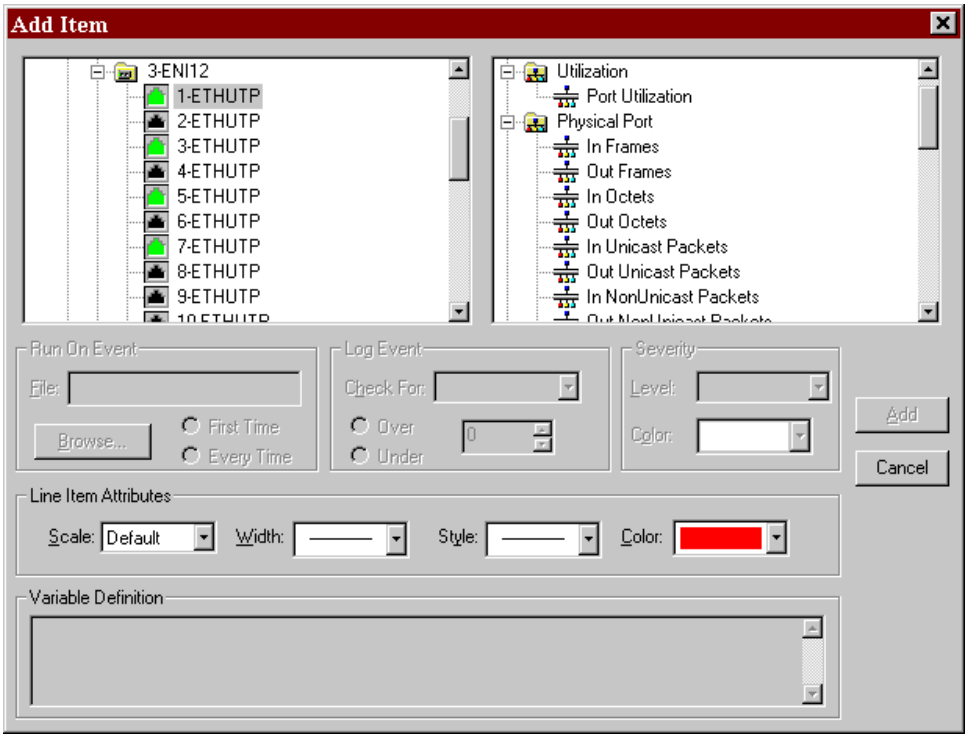
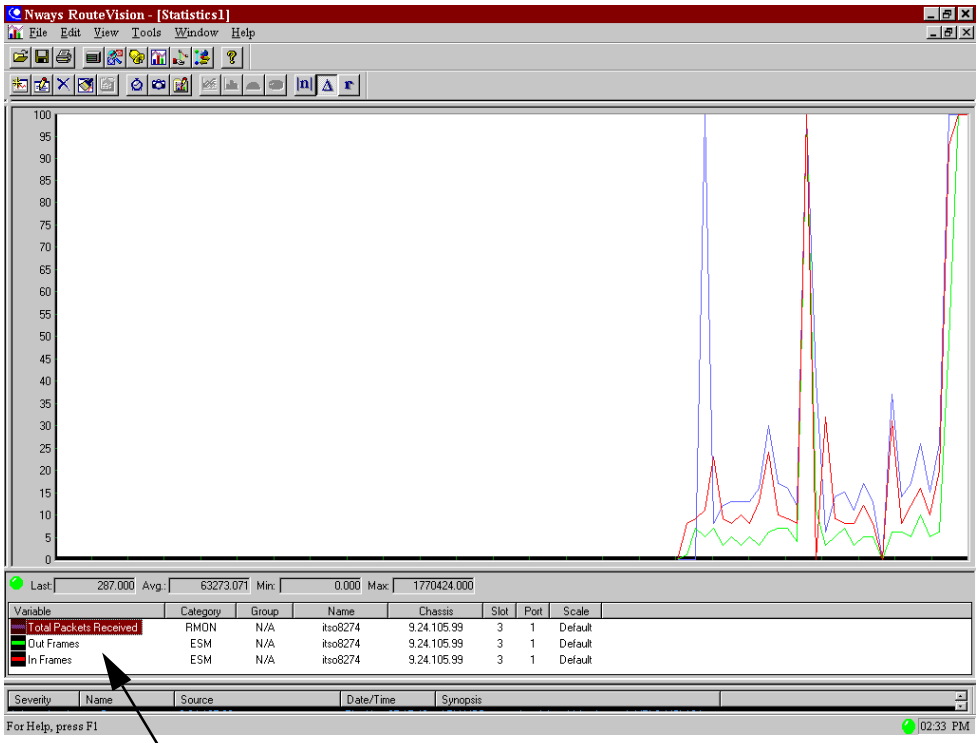


Figure 279. Result of Selecting Specific Resource on the Device

As can be seen above, the user can select a specific resource under the device and then be given a list of the MIB variables under that resource. In this case, an Ethernet UTP Port on a module has been selected, opening up the MIB variables for that port: Ethernet, Physical Port and RMON MIB variables.

Each item that is selected from the variable list can then be added to the Variable Definition window. In the example below the Ethernet In Frames, Ethernet Out Frames and RMON Total Packets Received, produced a graph as below:



List of Monitored Resources

Variable	Category	Group	Name	Chassis	Slot	Port	Scale
Total Packets Received	RMON	N/A	itso8274	9.24.105.99	3	1	Default
Out Frames	ESM	N/A	itso8274	9.24.105.99	3	1	Default
In Frames	ESM	N/A	itso8274	9.24.105.99	3	1	Default

Figure 280. Basic Graph Output

The scale of the map can be altered. The X-axis time divisions represent the polling interval that is being used by the Statistics function. By dragging the pointer from the top left-hand corner of the graph, it is also possible to view up to four different graphs based on the data being collected. Graphs can be shown as line graphs, bar graphs, pie graphs, etc. The data displayed can be the absolute value for the data, the rate of change of the value of the data or the difference in value from the last polling interval.

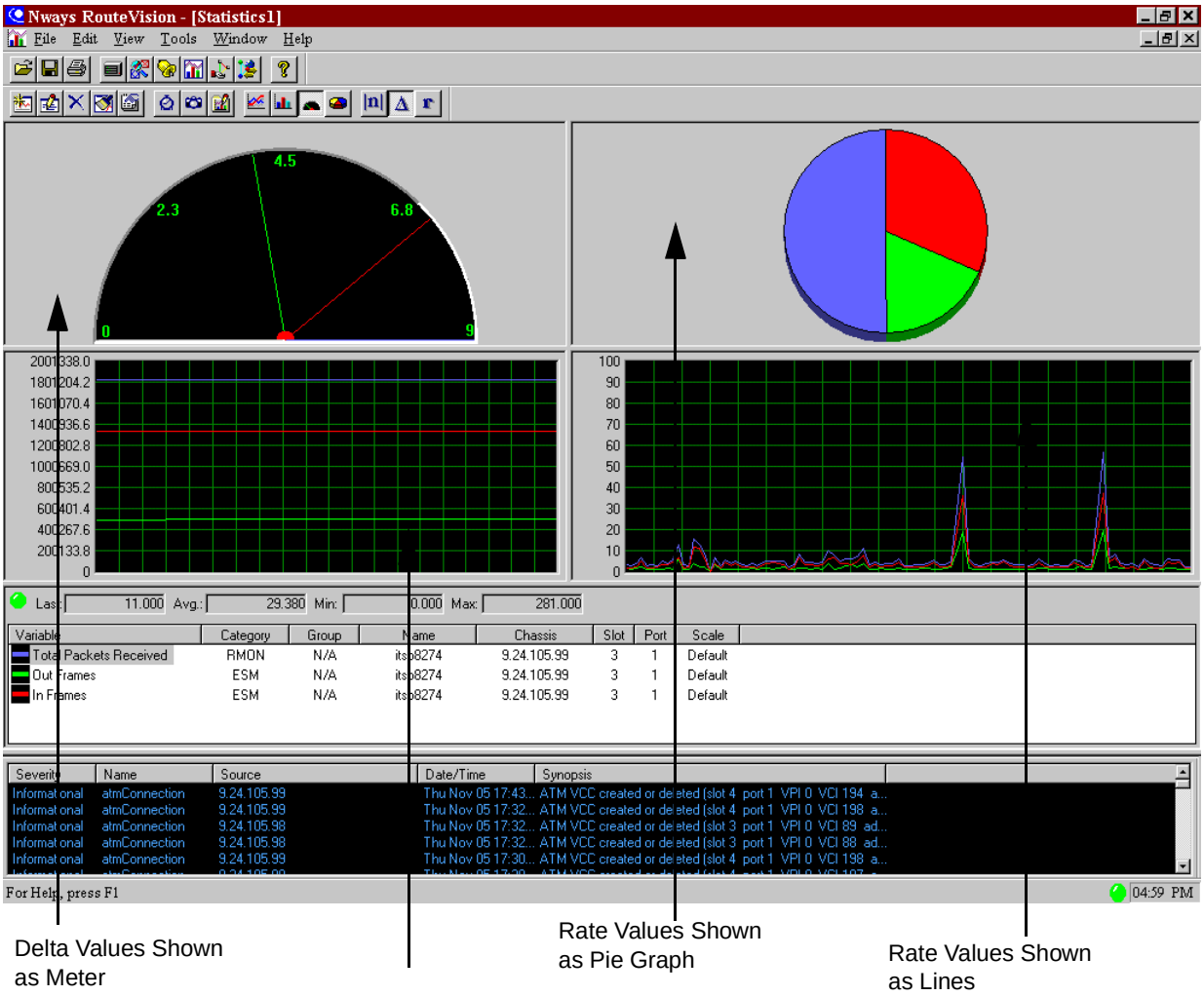


Figure 281. Different Graphing Options for Collected Data

Moving the mouse pointer onto the graph will display the value and time for that part of the graph.

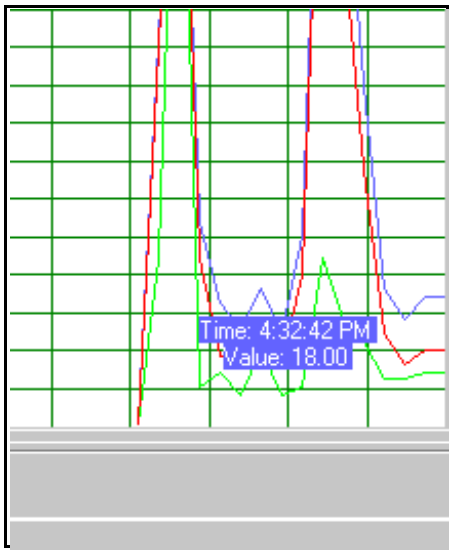


Figure 282. Example of Plotting Point on Graph

Above the monitored resources is the statistics polling light, which will display the overall status of the polling actions taking place. By selecting this light with the right-hand mouse button, it is possible to display the polling status for each monitored resource.

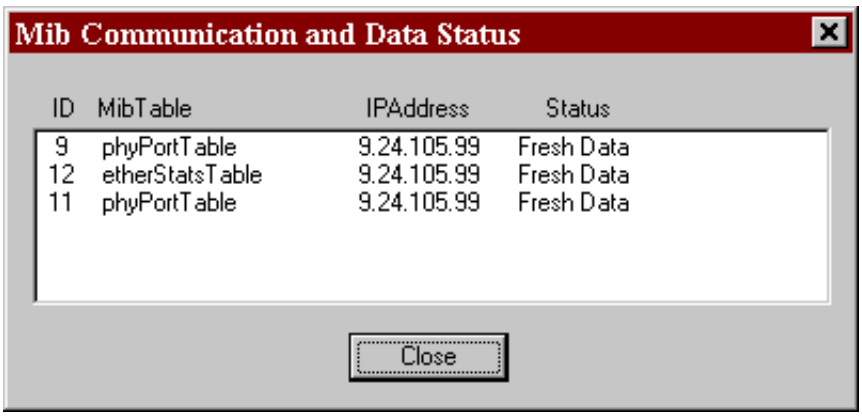


Figure 283. Statistics Polling Status Window

It is also possible to change the polling interval, the initial graph presentation and the logging option for the statistics. The logging option allows the user to collect polled statistical information in a log file for future analysis. These options can be set by choosing the **Edit...Properties** pull-down, or by clicking with the right-hand mouse in the graph output area.

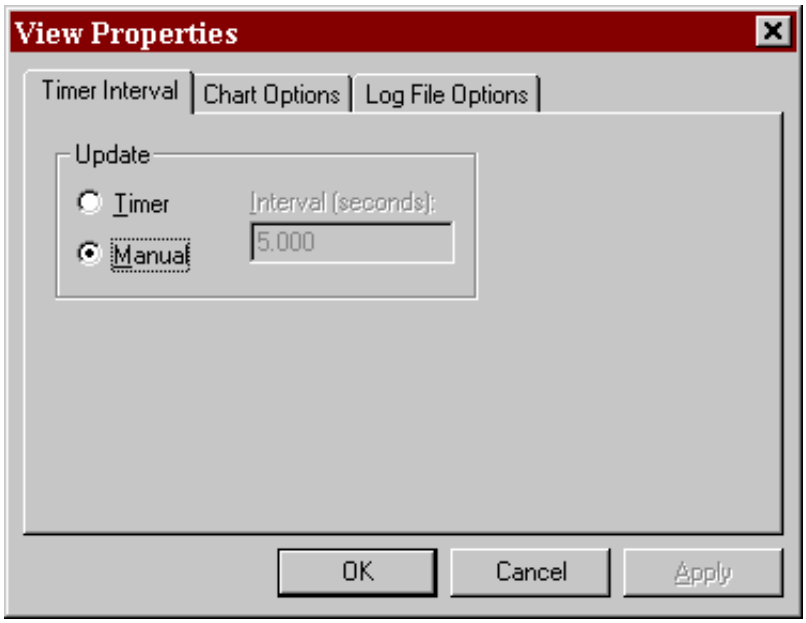


Figure 284. Properties for Graph Polling and Logging

As the majority of the network devices in the scenarios are not RouteVision-compatible, it was decided not to use the RouteVision Statistics applications to measure performance. The 8274 supports RMON so it is possible to use the Nways LAN ReMon product instead. This product can communicate with any RMON (or RMON2) agent, so can be used to monitor traffic across most of the network segments. As RouteVision can only measure performance on RouteSwitch devices, it would only be used to measure performance on items that cannot be monitored by Nways LAN ReMon.

8.3.4 Faults

The RouteVision product runs a Fault window at the bottom of any open RouteVision window. It displays the traps that have been sent to the management station by the devices that have been configured to do so. To set up trap forwarding from the RouteSwitches, the `snmpc` command has to be run prior to the installation of RouteVision (see Appendix 8.1, “Installation” on page 269). It is advisable to configure the management station with global systems administration access to the devices, which means setting the Special Access value to yes via the `snmpc` command.

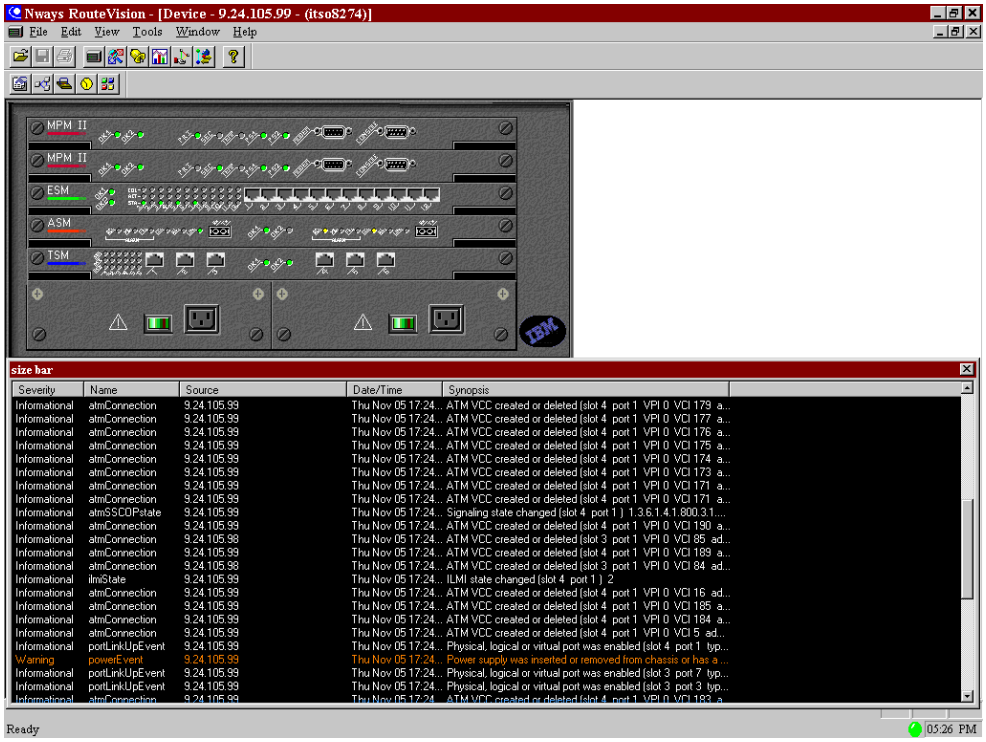


Figure 285. Trap Window Position

To configure the trap reception for the management station, the user must open the Trap Control table for each device being controlled by the management station. This is achieved by clicking on the **Traps** icon in the device view window, or by clicking the right-hand mouse button on the device chassis. This will open up the device configuration to show which traps have been defined to be sent to which management station. A management station with SET Community access privilege and the global system administration access can then re-define which traps are sent to which station. This is a much easier way to administer trap reception than by trying to set the trap words using the snmpc console command.

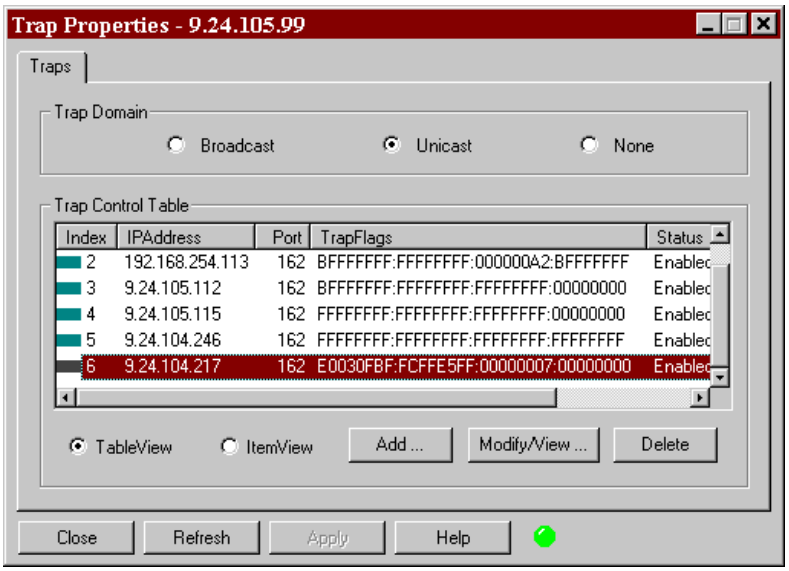


Figure 286. Trap Properties Window for 8274

As can be seen above, the Trap Domain has been set to Unicast this means that the devices listed individually as trap receivers will be the *only* devices to receive traps. The broadcast address will not be used, thereby reducing the traffic in the network. To re-define the traps that will be sent to a specific station, the user must highlight the station address in question and then click on the **Modify/View** button.

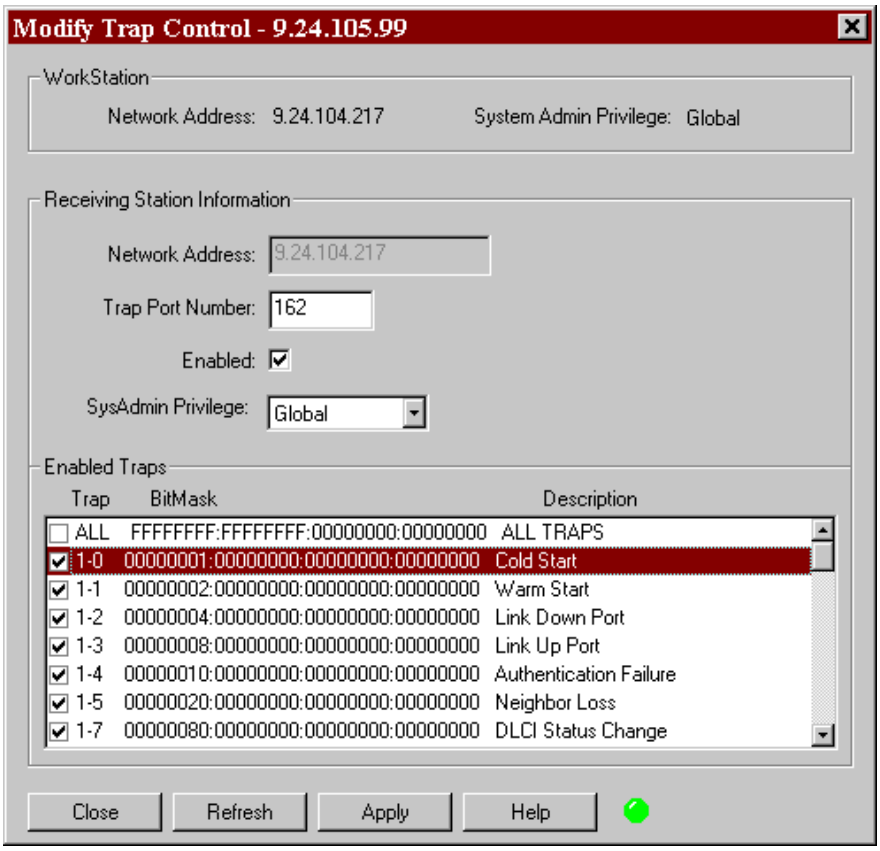


Figure 287. Trap Configuration for 8274

In the window, the user will see a tick mark next to all of the traps that are to be transmitted to the management station. It is also possible to modify the Broadcast Trap Entry if the management station has global access, but in this scenario the Broadcast Trap Entry is disabled. By default, the Broadcast Trap Entry will transmit defined traps to all users in the default VLAN 1 in default GROUP 1, as that is where the broadcast address points to.

Further trap customization can be performed by clicking with the right-hand mouse button in the trap window to activate the Trap Properties window for the management station.

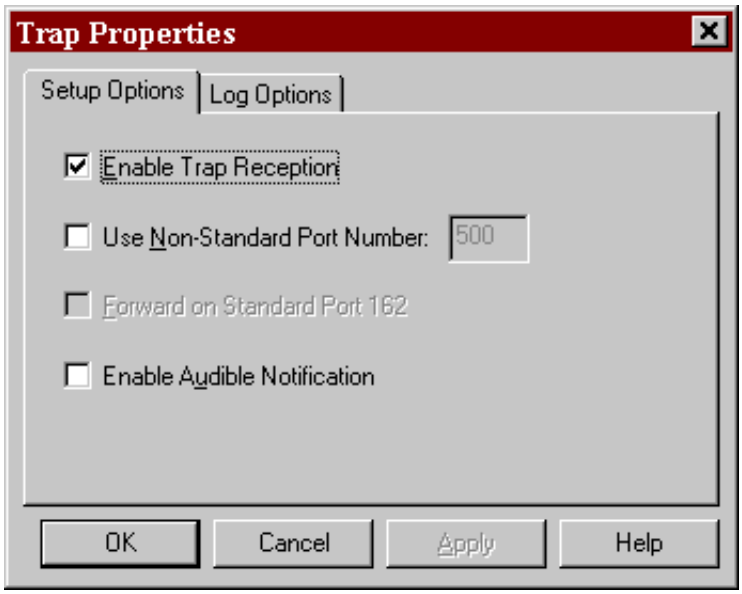


Figure 288. Trap Properties

From here, the user can enable or disable the reception of traps from the network, as well as change the reception port. It is also possible to activate or de-activate the logging of received traps and set the wrap limit on the log file.

There seems to be no options to change the severity of received traps, or to change the color they display in. In the scenarios used, it was decided to use the Nways management and NetView event handling functions to deal with traps from the RouteSwitch devices as there is a greater degree of control within NetView and Nways management, plus there is the ability to forward traps to a focal point or trouble-ticketing system. Both the Nways management and NetView products can understand the RouteSwitch MIBs, so it is possible to receive and process the traps that are sent to them.

Traps are often referred to as *unsolicited* events. In other words they are not the result of a polling action but are generated by the SNMP agent in the device and forwarded to the defined destination stations for processing. *Solicited* events can be created on a management station and applied to a specific device, which is then polled for data on a set time interval. The returned data is analyzed, and the decision to create an event based on the pre-set thresholds is taken.

In RouteVision, the event customization screens are almost identical to the screens used for statistical analysis. This is because the management station is still polling the device for data on a defined set of MIB variables, but this time we are setting a threshold on these variables over which an event will be created.

The Events window can be opened by selecting the **Events** icon on the main tool bar.

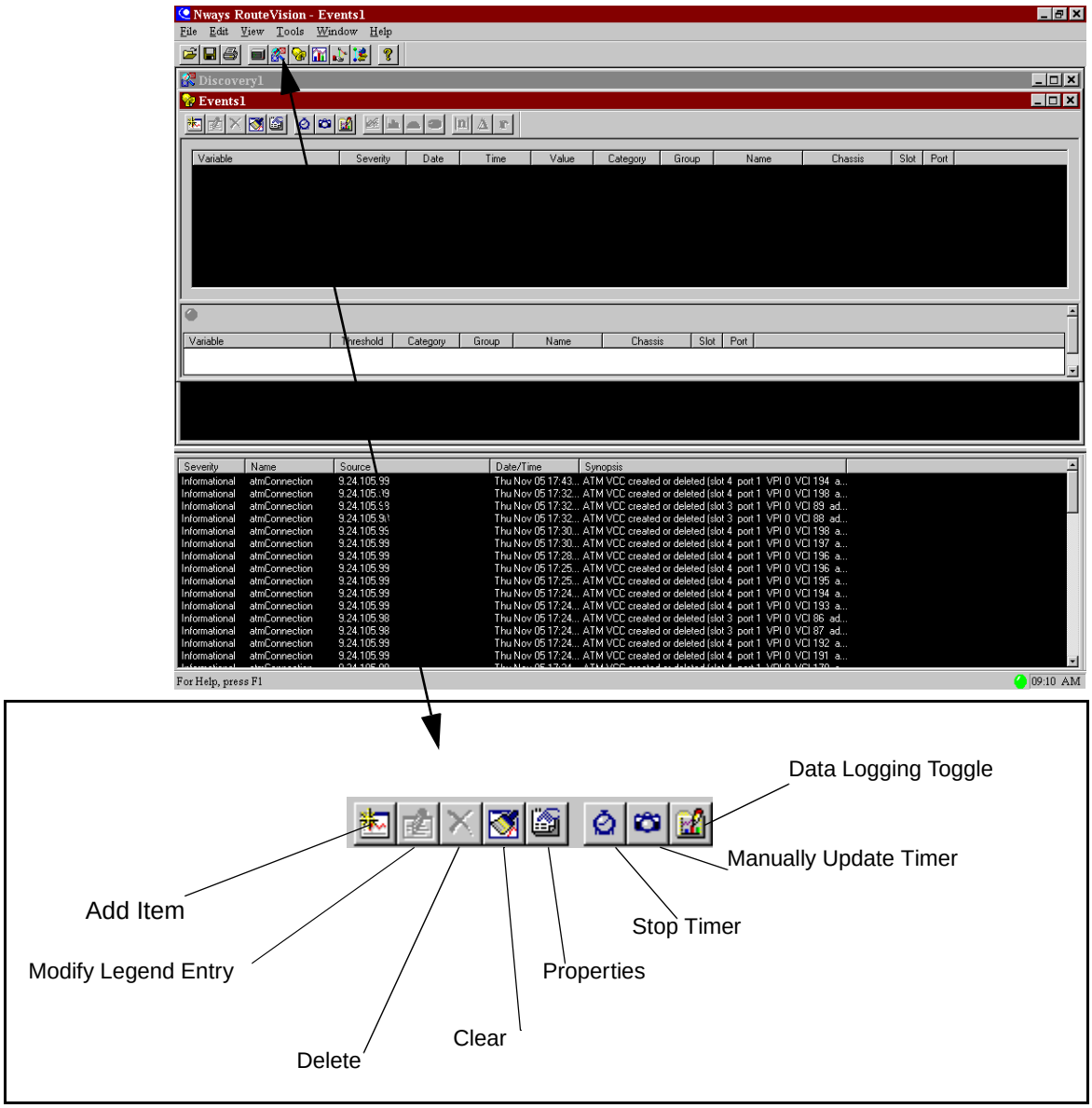


Figure 289. Events Main Window

In order to configure event monitoring, the user must take the same action as when configuring statistics monitoring. First of all, open the window view of the available devices with the **Add Item** button.

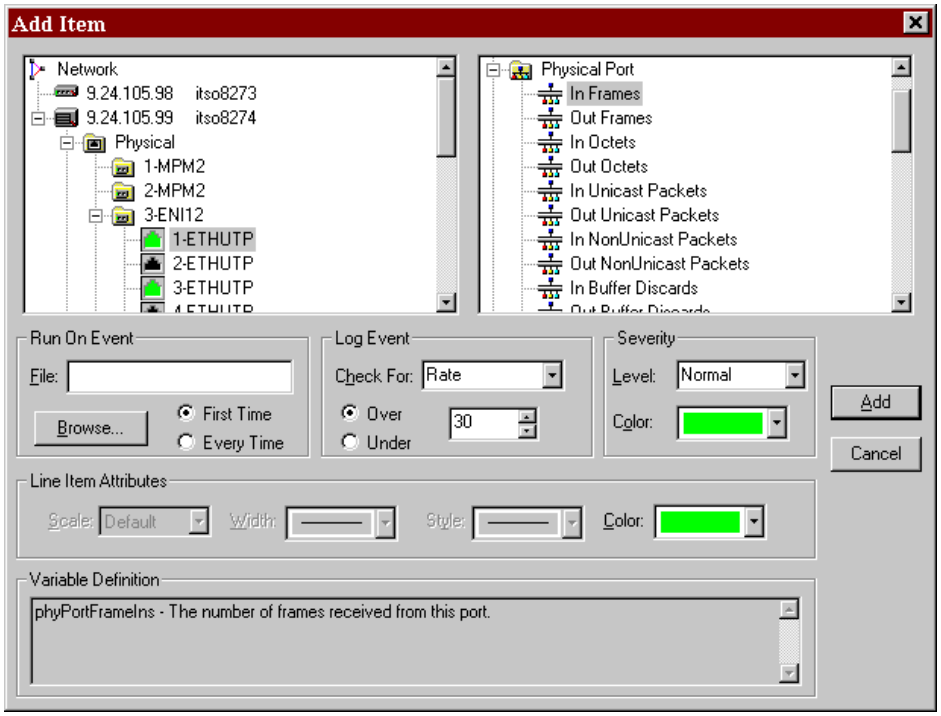


Figure 290. Event Configuration Window

As per the statistical analysis configuration, the user selects the device and then can select the resources within that device to monitor. For each resource the right-hand window will show the MIB variables available for monitoring, exactly the same as for statistics. The user can then select the variable and set some threshold check against the rate, delta value or absolute value. Once this is set, the user can then decide what severity to apply to an event if it is raised, plus whether any further action should run if the event occurs. All the configured events then appear in the event logging window, as shown below.

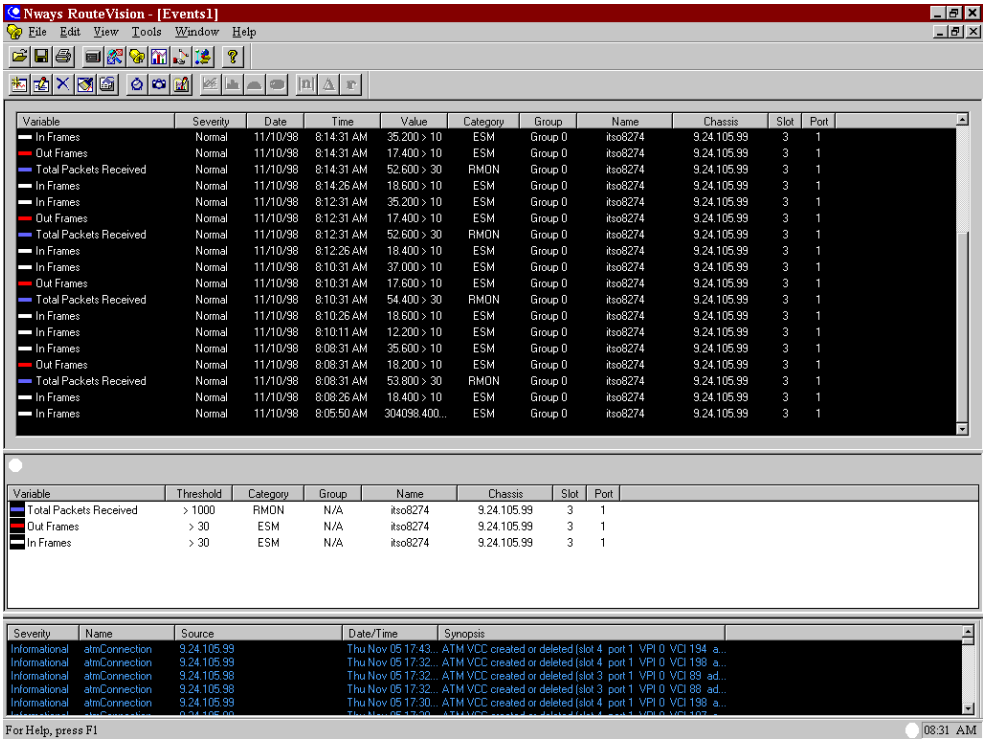


Figure 291. Event Logging Window

In the event logging window, the user can see the configured events per device, plus a running log of the events that have been raised. There is a status light, indicating the polling condition; green would signify that polling is successful for all items to be polled. Selecting the variable with the right-hand mouse button will show the exact status of polling for each individual item, exactly the same as in statistics gathering. The polling timers for statistics and events are completely separate, as are the configuration windows, so it is possible to set the different polling intervals for the same MIB variable but one will be checking for a threshold exception and the other will be checking for the actual value at that point in time.

There seems to be only one threshold that can be set per item, so it is not possible to set a critical event when a threshold is reached and then set a normal event when the monitored value goes below the threshold again. There also appears to be no way to forward these events directly to another management platform such as NetView. The only standard options to run against an event are to send an e-mail message or a network message.

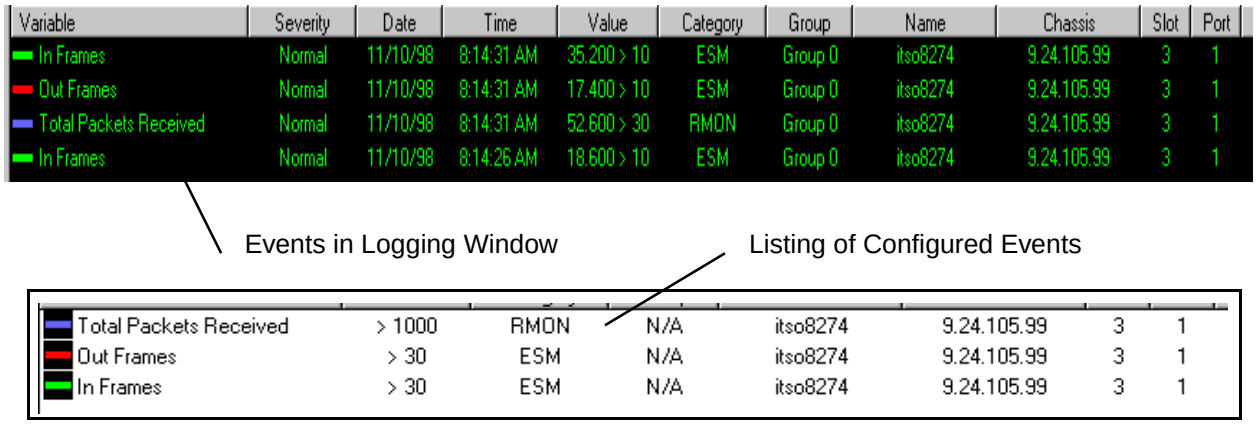


Figure 292. Event Window Detail

The logging and polling values can be altered, in the same way as statistics gathering, by opening the properties window from the **Properties** icon or by the right-hand mouse button on the event window.

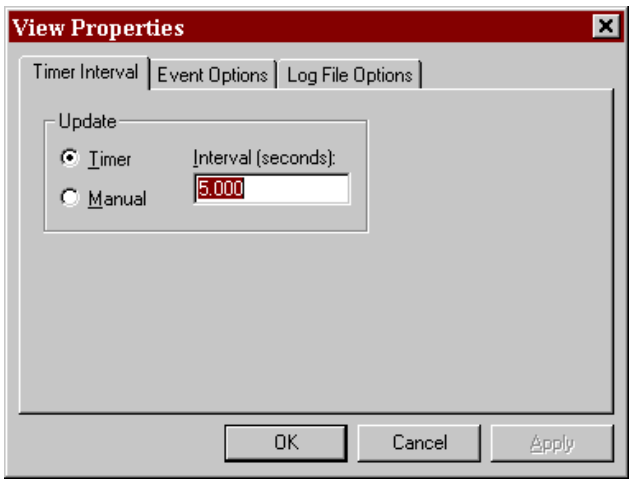


Figure 293. Event Properties Window

As there appears to be no obvious way to forward events to NetView, it was considered more appropriate to use the Nways Manager, LAN ReMon and NetView products to perform threshold checking on the RouteSwitch products in the scenarios discussed in this book. However, in a RouteSwitch-only environment the opposite would be the case.

Chapter 9. Nways Campus Workgroup Manager for NT

This chapter covers the Nways manager application for NT. It shows how to perform planning and installation/customization. The application is then used to manage a small network.

Assuming the network that required management already existed the implementation stages we performed are outlined below:

Network Topology	Obtain and understand the network we need to manage.
Devices	Build a list of the managed devices and the resources we want to manage.
Requirements	Understand and develop the specific management requirements and build a set of tools to manage the environment.
Event/Performance	Build a list of traps that can be generated for our environment and decide what to do with these traps.

First we look at the network topology.

9.1 Network Topology

The network we built for this scenario is shown in Figure 294 on page 305.

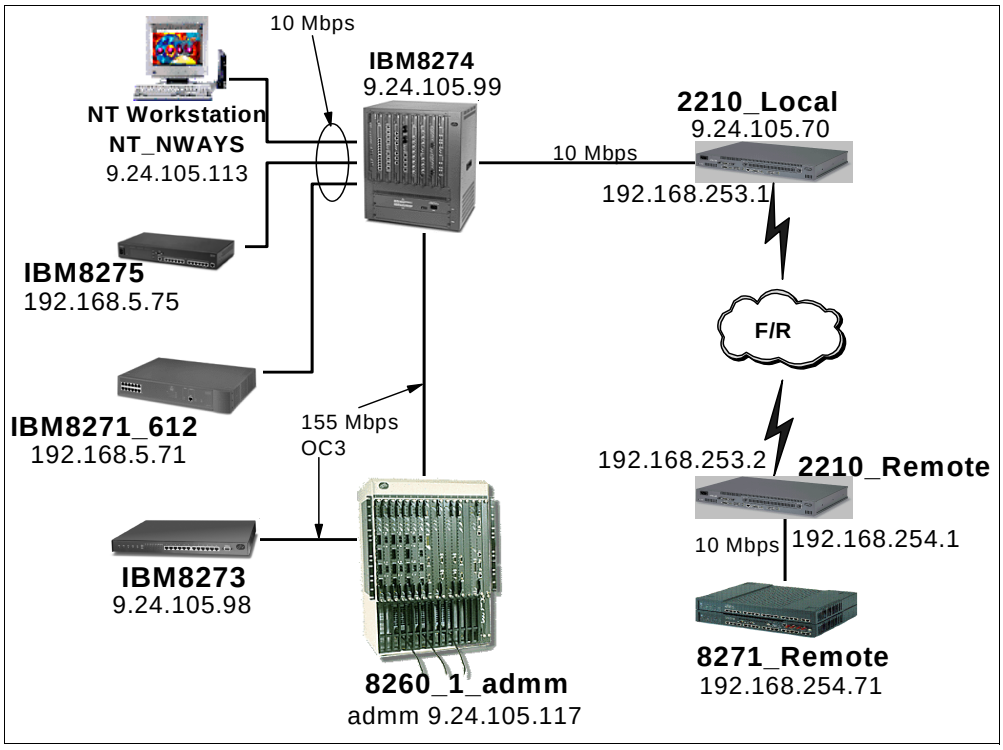


Figure 294. Management Scenario Using Nways Workgroup Manager for Windows NT

Figure 294 on page 305 displays the physical network hardware devices that were used in this case scenario.

We simplified the first network shown in Chapter 3, “Planning for the Nways Management Installation” on page 21. Basically we removed the ATM components.

The network connection method used for the network management station in this scenario was a 10 Mbps Ethernet connection into an IBM 8274 Nways RouteSwitch.

Although this method proved a simple and reliable mode of connecting the network management station we could also have used a fast ethernet or token-ring connection to any device in the network.

9.1.1 Device Components

The following table represents the customized device names and elements that were used during this test.

We connected the NT_NWAYS server to the 8274. The IP address assigned was 9.24.105.113.

Table 19. Device and Element Table for Scenario Two

Hostname	Modules	IP Address	Microcode Level
8260_1_adm m	ADMM CPSW ADMM SWE10F2-F SWE12TP-RJ45 A-CAR (MSS1) A04-FB100MIC A03-MB155 A03-MB155 A12-TP25-RJ	192.168.21.61 9.24.105.117	V3.1.1 V5.21-H V2.00 V2.00 MSS V2.1
IBM 8274	MPM II MPM II Ether/12 HSM2 ATM 2Meg ATM 2Meg	9.24.105.99	V3.2.3 Patch 33
IBM8273		9.24.105.98	V2.1.1
IBM8271		9.24.105.101	V4.0.0 ATM UFC V1.14.0
2210_local	LAN port WAN port	9.24.105.70 192.168.253.1	MRS2.2
2210_remote	LAN port WAN port	192.168.254.1 192.168.253.2	MRS2.2

9.1.2 Requirements

This high-level view provides the customer with information on the functions that the tools will provide.

We have a simplified number of products for the NT installation. For all devices we installed the Workgroup Manager and Workgroup Remote Monitor. For the 8274 we installed RouteVision.

9.2 Installing Nways Workgroup Manager for NT

This chapter covers the steps for installing the Nways Workgroup Manager for NT and associated products, which run on a Windows NT platform.

We cover the installation procedures for the following software products:

- Nways Workgroup Manager NT 1.1.2
- Nways Workgroup Remote Monitor 1.1
  - DB2 Universal Database V5 for using Java Performance Monitor
  - DB2 V5 APAR JR11296 Installation for memory leak
- Nways RouteVision Campus Manager 3.2
- Multiprotocol Routing Services (MRS) Configuration program 2.2
- Configuring Web Server for Web Access

Minimum hardware configuration for Nways Workgroup Manager as per the installation guide is outlined below. For better performance, we recommend having a faster processor, additional RAM and virtual memory for paging. Also, take into account additional memory requirements if you plan to run concurrently the associated network management and configuration programs (that is, RouteVision, Web server, MRS/MSS Configuration programs).

9.2.1 Minimum Hardware Requirements

The minimum recommended requirements are:

- Pentium Processor (200 Mhz Minimum)
- SVGA high-resolution monitor (1024 x 768)
- 128MB of RAM
- Free disk space
- 175MB for applications files
- 150MB for virtual memory paging files
- 100MB for JDBC-compliant database performance data storage if the Java performance monitor is used
- Network interface card supporting TCP/IP protocol
- CD-ROM drive
- Mouse

The installation program will use temporarily additional hard disk space during the course of the installation, after which it is released.

The associated network management and configuration programs have additional RAM and hard-disk space requirements.

9.2.2 Software Requirements

The software requirements are as follows:

- Microsoft Windows NT Version 4.0 with Service Pack 3 and TCP/IP support installed. If your display adapter is set to True-Color color mode, you will also need the post Service Pack 3 get-admin hot-fix from Microsoft.
- IBM Nways RouteVision - If graphical management for IBM 8274 Nways LAN RouteSwitch, IBM 8273 Nways RouteSwitch, or the IBM 8276 Nways Ethernet RoutePort is required. In our lab, we installed the latest version, which is Nways RouteVision Campus Manager 3.2, which is the integration of RouteSwitch Manager, RouteTracker, RouteMonitor, and RouteDirector. It can be used to managed 8273, 8274,8276, and 8277.
- IBM Nways Route Tracker Manager if VLAN configuration is required. Again, as we installed RouteVision Campus Manager 3.2 in our environment, the VLAN configuration feature was built-in.
- IBM Netfinity Manager Version 5.0, if you require Netfinity to be able to be managed from Workgroup Manager map views, client workstations running the Netfinity Services Version 5.0. This function requires that the clients workstations have Netfinity Services 5.0 and a TCP/IP stack with SNMP agent installed. The installation and configuration of Netfinity Services 5.0 is beyond the scope of this book.
- A JDBC-compliant database to be used with Java-based performance management function. For ease of installation, the Enterprise edition of IBM DB2 Universal Database Version 5.0 is provided with Nways Workgroup manager, in a separate CD-ROM. However, you may use any other JDBC-compliant database.
- IBM LAN Adapter Agent for OS/2 and Windows NT workstations with IBM Ethernet and token-ring adapter. This is only required for Java-based adapter management functions for these adapters, from Nways Workgroup Manager.
- Graphical configuration programs for IBM 8210 Multiprotocol Switched Services program (MSS), 2216 MultiAccess concentrator with Multiprotocol Access Services (MAS), and 2210 router with Multiprotocol Routing Services (MRS). Each of these configuration programs are shipped along with respective devices and also can be downloaded from the IBM Networking Web site (www.networking.ibm.com). The programs are required if complete graphical configuration is required from the Nways workgroup manager workstation. The Java device management component provides some level of configuration, but for total GUI-based configuration, the configuration programs must be used, except for the 8210(MSS), which also provides a Web browser interface for configuration. The respective programs can be launched from a Java device management view of 2210, 2216 and 8210 (MSS).
- Web server, if Web access is required to the Workgroup Manager workstation. Examples are IBM Internet Connection Server, Netscape, Microsoft Internet Server, and Lotus Domino.
- Java Development Kit (JDK) Version 1.1.4 (or higher) compliant Web browser for Web access to the Workgroup Manager workstation.

9.3 Pre-Installation Steps

This section outlines the pre-installation and installation steps for Nways Workgroup Manager for Windows NT.

- Make sure that the Windows NT user Id logged in to the management workstation is a member of the administrator group. The install program will fail if the user Id does not have administrator privilege.
- It is highly recommended to close all active applications, in order to avoid any conflicts.

Note

If you have an anti-virus program installed, the installation may fail. Version 2 and earlier versions of IBM AntiVirus for Windows NT are incompatible with the installation program. These versions must be uninstalled prior to installing Nways Workgroup Manager. After installation you may re-install IBM AntiVirus if installation problems are experienced, make sure no anti-virus applications are installed.

9.3.1 Installation Steps

The following steps describe the installation for Nways Workgroup Manager for NT.

1. Insert the Workgroup Manager CD-ROM in your CD-ROM.
   - If you have Autorun set to ON in your Windows NT system, the install program will start automatically.
   - If Autorun is set to OFF, then run setup.exe, which will invoke the install program, where x is the CD-ROM drive letter.
   - Click on **Next** to select the components.
2. Select the required components to be installed.

   We selected:
   - IBM Library Reader for Windows (to view online books)
   - IBM Nways Workgroup Manager for NT (for basic management)
   - IBM Nways Workgroup Remote Montior for NT (for RMON support)

   Note: The Nways Workgroup Remote Monitor is required only for collecting and analyzing RMON data from devices supporting RMON.

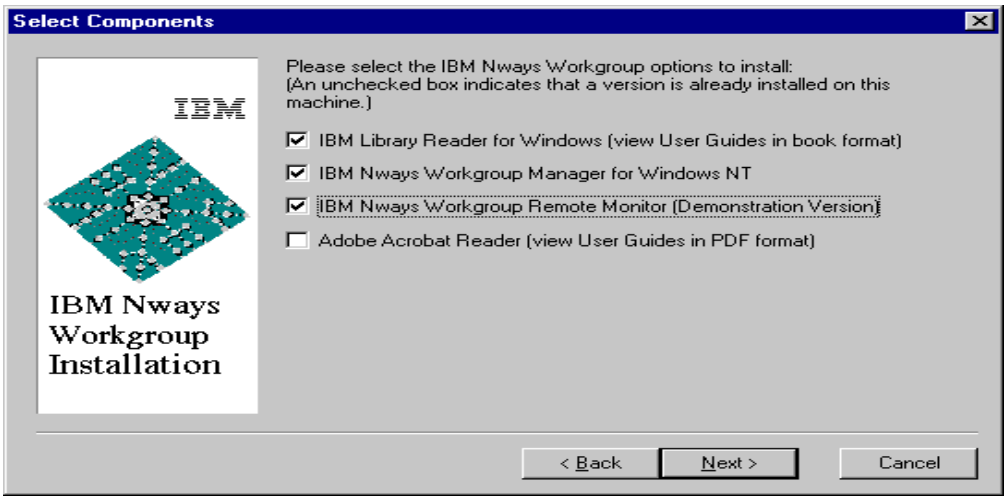


Figure 295. Nways Workgroup Manager for NT - Selecting Components for Install

3. Click on **Next** to start the installation.

   This will start the IBM Library Reader installation. Follow the online instructions to complete the installation.

4. After IBM Library Reader is installed the Nways Workgroup Manager installation program is started automatically.

   - Select the destination directory C:\program files\Nways\.
   - Click on **Next** to continue.

5. Select which device management you want to be executed automatically when Nways Workgroup Manager is started. It only affects the automatic start-up list, as all device management applications are installed in the nways directory. This start-up list can be modified after installation using the Nways Workgroup Manager configuration utility.

   - Click **Next** to continue.

   We selected all the devices that were part of our selection in the lab.

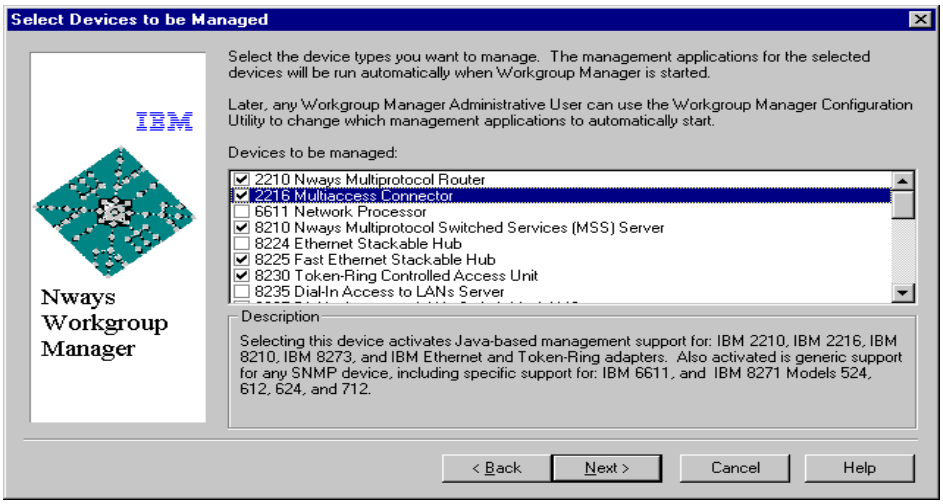


Figure 296. Selecting Devices to Be Managed

6. Select the program folder **IBM Nways Workgroup Manager.**
   - Click on **Next** twice to start the actual copying of files to the Nways directory.
7. After Nways Workgroup Manager files are copied, an informational message is displayed "IBM Nways RouteSwitch Network Manager (5697-B67) is not installed". Ignore this message, as the Nways Workgroup Manager installation program does not seem to recognize the latest version Nways RouteVision Campus Manager 3.2 being installed. We confirmed this by installing the Nways Routevision Campus Manager 3.2 first, and we still got the same message during Nways Workgroup Manager installation. We believe this will be rectified in the upcoming release.
8. To perform the database initialization.

   The options are to create a new database or migrate from a prior version. Use the Create a new database option if no prior version of Nways Manager exists on the machine. Otherwise, use the migration option to migrate the database from an earlier version. As we were starting from a fresh installation, we chose the Create a new database option.
   - Click on **Next** to continue, to start the database creation and unitization process.
9. Using the configuration utility.

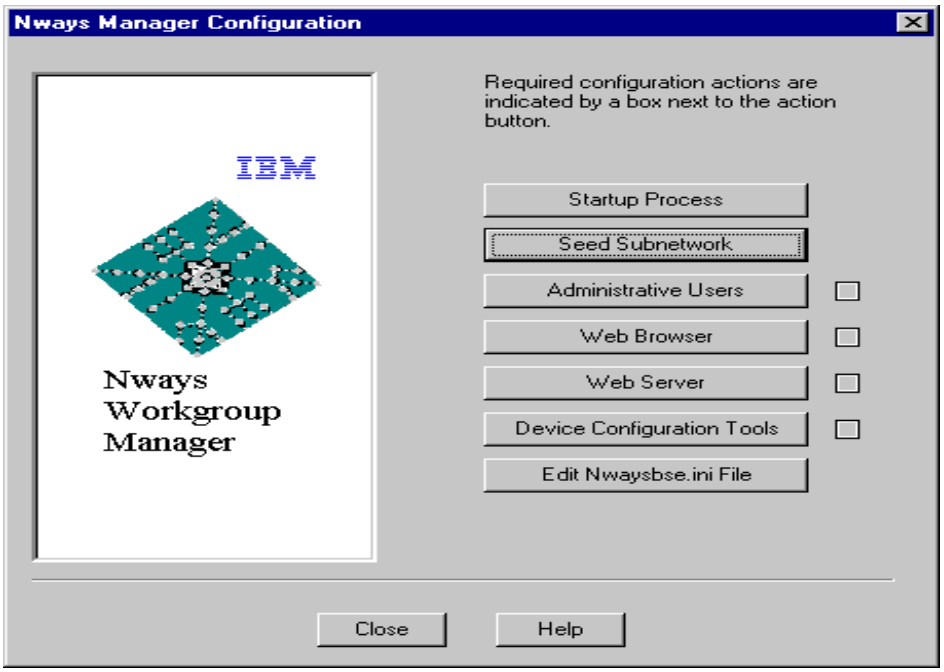


Figure 297. Nways Workgroup Manager for NT Configuration Utility

The Configuration utility allows you to set the configurable parameters for Nways Workgroup Manager. In this section, we address the basic configuration required to get Nways Workgroup Manager up and running. The next section covers more of the Configuration utility. Of course, the Configuration utility can be executed any time after installation, so it is not a must to configure all the parameters, especially related to other associate programs that are installed after IBM Nways Workgroup Manager for Windows

NT installation. We configured only the seed subnetwork and administrative users. Any other configuration that is required is covered in later section.

We set the seed subnetwork to match the IP subnet to which the network management station NT_NWAYS1 was part of. The seed subnetwork is just a starting point for autodiscovery.

We set the following for our seed subnetwork:

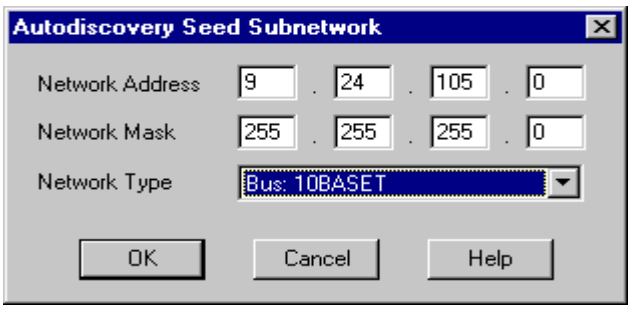


Figure 298. Auto Discovery Seed Subnetwork

In the administrative users panel, all defined NT user Ids by default have operator privilege for Nways Workgroup Manager. We set two users for Administrative privilege:

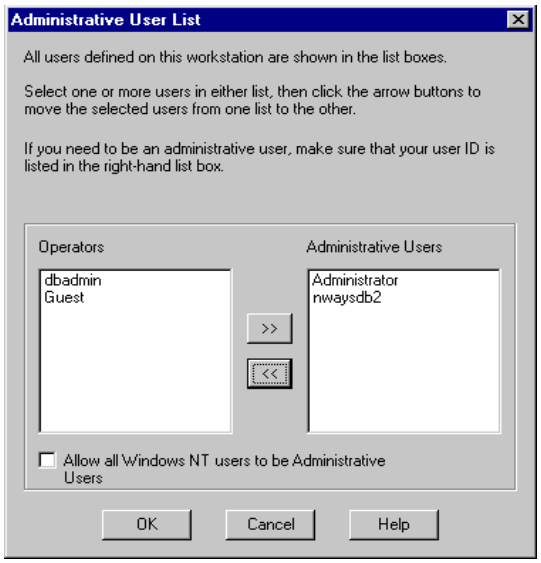


Figure 299. Nways Workgroup Manager for NT - Administrative Users

Notes

- The Nways Administrative users need not be Windows NT administrative users; they could be normal users.
- The list of Nways administrative users is maintained in the NWAYSBASE.INI file under c:\program files\nways\. Write access to normal users to this file should be restricted, to avoid normal users from editing this file and updating the user list.

10. This completes the Nways Workgroup Manager part of the installation. As Nways Workgroup Remote Monitor is part of the same installation process sequence, we cover the steps for it below, including the DB2 V5 installation for NT and the apar fix for the DB2 V5 memory leak.

11. Nways Workgroup Remote Monitor Installation.

    As we selected Remote Monitor in Step 2 for installation, the product installation will automatically start after Nways Workgroup Manager installation is completed.

    At the welcome screen click on **Next.**

    The message saying "Nways Workgroup Manager has been installed on this system. Would you like to install the Nways Workgroup Manager Interface?" appears. Click on the **Yes** button to install the interface to Nways Workgroup Manager.

    Accept c:\Program files\Remon as the default directory path for Nways Workgroup Remote Monitor files. You may change the path if required.

    Click on the **Finish** button to complete the setup of Nways Workgroup Remote Monitor for Windows NT.

9.3.2 IBM DB2 Universal Database for Windows NT V5 Installation

DB2 Enterprise edition, which provides the JDBC-compliant database capability is required for the Nways Workgroup Manager Java-based performance management component to store performance data. The DB2 V5 CD-ROM is provided with Nways Workgroup Manager in a separate CD-ROM.

1. Insert the DB2 V5 CD into the CD-ROM drive.
   - If you have Autorun set to ON in your Windows NT system, the install program will start automatically.
   - If Autorun is set to OFF, then run x:\setup.exe, which will invoke the install program, where x is the CD-ROM drive letter.
2. Select the DB2 Universal Database Enterprise Edition to install.
3. Select a typical install.
4. Select C:\SQLLIB as the default directory.
5. At the username and password prompt, enter a user id and password, which should be a Windows NT Administrative user. Also user names should be limited to eight characters, which is a limitation of DB2, thus the default user Id of Administrator will not work. We created a new administrative user nwaysdb2 in our environment.

   Ignore the message Setup is unable to validate the password. Setup will continue, and follow through the online instructions to complete the installation of DB2.

6. Select **I will restart my computer later**, as we'll install the DB2 apar fix for APAR JR11296.
7. Installing DB2 V5 APAR fix JR11296.

   The APAR fix JR11296 is required to correct a memory leak in DB2 V5. We downloaded the latest cumulative fixpak WR09045 for DB2 V5 which contained the fix for APAR JR11296 from the ftp Web site:

```
ftp.software.ibm.com/ps/products/db2/fixes/english-us/db2ntv5/us9045/us904.5.zip.
```

The WR09045 is a US-english version. Other language versions of the fixpak are also available on the same site.

- Create a temporary directory to unzip the fixpak, for example c:\temp. An unzip program (that is, pkunzip or Winzip) is required to unzip.

  If DB2 was previously installed and running, stop all DB2 processes by using the following commands:

  ```
  db2stop
  db2admin stop
  ```

- Run c:\temp\setup.exe.

  Follow the online instructions to completed the fixpak installation, and restart the computer to make the changes effective.

8. IBM DB2 V5 post installation steps

   Unzip the JDBC drivers from c:\sqllib\java\db2java.zip into the nways directory: c:\program files\nways\java\websvr\code.

   Note: We found that some older versions of pkunzip did not work correctly when dealing with the directory structure and long file names. We used the Winzip program.

   If DB2 is not automatically started, then issue a db2start command to start the DB2 server.

   To create the database that will be used JPM component:

   - Change to the \program files\nways\bin directory.
   - Run the command:

     ```
     db2cmd CreateDatabase.bat -create
     ```

   A database called IBMNMPBD will be created under the same disk that DB2 was installed.

9.4 Installing Additional Management Applications

In this section, we explain the installation procedures for additional network management and configuration applications. These stand-alone programs are stand-alone in nature, in that they can be run without installing Nways Workgroup Manager. Once integrated, they can be launched within Nways Workgroup Managermaps and views.

The products we cover in this section are:

- Nways RouteVision Campus Manager 3.2
- Multiprotocol Routing Services (MRS) Configuration Program 2.2
- Web Server for Web Access

9.4.1 Nways RouteVision

The Nways RouteVision Campus Manager installation and configuration are already covered under Chapter 8, “RouteVision Suite” on page 269.

9.4.2 2210 Multiprotocol Routing Services Configuration program

The IBM 2210 MRS Configuration program allows graphical configuration from a Windows, OS/2 or AIX workstation.

The latest version of MRS code for 2210 routers is 3.1, but the latest level supported by Nways Workgroup Managerfor NT 1.1.1 is MRS 2.2 (CC2), as stated in the Technical Tips document for Nways Workgroup Manager version 1.1.1 on the IBM Networking Web site. Thus, we used the MRS 2.2 Configuration with PTF NP00883 configuration as it had to match with the MRS code installed on the router, otherwise unpredictable results could occur.

All the programs and code for 2210 can be obtained from the Internet at:

```
http://www.networking.ibm.com/support/code.nsf/2210code?OpenView
```

Installation steps are very straight forward:

- If you have diskettes, insert diskette # 1, and run the program called install.exe, which will follow you through the installation.
- If you have a CD-ROM, then it usually is in a directory called config. Run the program install.exe from that directory.

9.4.3 Web Server Installation

Almost any Web server will work with the Nways Workgroup Manager (NWGM). Note that your Web server does not need Java support. The Web server accesses the NWGM Java code only as data.

To enable Web-based network management, you must perform some configuration steps for your Web server. You should perform the following general steps. The details will depend on your Web server software.

1. Locate the NWGM Web pages subdirectory. On Windows NT, the NWGM Web page subdirectory is named <nways>\java\websvr, where <nways> is the directory to which you installed the NWGM product. An example in our scenario is C:\Program Files\Nways\java\websvr.
2. Decide what the logical directory name will be for your NWGM pages. With most Web servers, you are free to choose any logical directory name you wish. For example, you could choose /NetworkManagement, /Nways, /NetMgmt/Nways, etc.
3. Add your logical directory name to the Web server as an alias for the NWGM Web server subdirectory. Using the administration program for your Web server, you need to specify the actual NWGM Web pages subdirectory and the logical directory name you have chosen for it to the Web server.
4. Set security parameters to control access to the NWGM pages. Publishing the NWGM pages on your Web server without controlling access to them would allow anyone with a Web browser to manage your network. At a minimum, you should restrict access to your NWGM pages. The method for doing this depends on your Web server. You might also want to consider using SSL and other security features of your Web server to enhance security.

9.4.3.1 Netscape Enterprise Server 2.01 and 3.01 for Windows NT Example

The following lists the steps to install the Netscape Web Server:

1. Start the administration program Administer Netscape Servers.

2. Select the appropriate Netscape Enterprise Server from the list of installed servers.
3. Select the **View Server Settings** menu item.
4. Under the Content Settings section, select the **Additional Document Directory**.
5. Enter the logical directory name you wish to use in the URL prefix entry box. For example, you might enter Nways.
6. Enter the NWGM Web server directory name in the Map To Directory field. For example, you might enter c:\Program Files\Nways\java\websvr.
7. Click the **OK** button.
8. On the Save and Apply Changes page, you'll be asked to save and apply the changes.

9.4.3.2 Microsoft Peer Web Server Example

The Microsoft Peer Web Services is shipped with Windows NT, and you can use its Web server with the NWGM. After you install and start Peer Web Services, you can add the NWGM Web server directory by performing the following steps:

1. Start the Microsoft Internet Service Manager.
2. Select the **WWW** service.
3. Select the **Properties > Service Properties**... menu items from the menu bar.
4. Select **Directories property sheet**.
5. Click the **Add** button to bring up the Directory Properties dialog.
6. Enter the NWGM Web server directory name in the Directory text field. For example, you might enter c:\Program Files\Nways\java\websvr.
7. Select the **Virtual Directory** radio button.
8. Enter the logical directory name in the Alias text field. For example you might enter /Nways.
9. Click the **OK** button to finish.

9.4.3.3 IBM Internet Connection Secure Server V2R4 Example

The following steps describe the installations steps for the IBM Internet Connection Secure Sever.

1. Start the Configuration and Administration Forms page in your Web browser.
2. Select the **Request Processing** item to get the Request Processing page.
3. Select the **Request Routing** item to get the Request Routing page.
4. Select the **Insert before** radio button.
5. Enter **Map** in the Action text field.
6. Enter the logical directory name and a wildcard in the URL request template text field. For example, you might enter /Nways/* .
7. Enter the NWGM Web server directory name in the Replacement file path text field: `c:\Program Files\Nways\java\websvr\*` .

8. Click the **Apply** button.

9.4.4 Configuration of DIA on Win/NT and Win/95

The next steps describe the configuration for the distributed intelligence agent.

1. Install JRE 1.1.4 or later on the DIA target system.

> **Note**
>
> You must install both Java Runtime Environment (JRE) and Java Just-in-Time (JIT) bytecode compiler in order to run DIA application (LoadDIA.class file) on a Windows-based client system. The JRE 1.1.6 and JIT update from Symantec Version x3.00.053 can be obtained from the following web site:
>
> `http://java.sun.com/products/jdk/1.1/jre/download116-jre-windows.html`

2. After JRE 1.1.6 has been installed, the default directory \Program Files\Javasoft\jre\1.1\bin will be created. Use ftp to download the following files from the management system to the target system's previous default directory.

   ```
   /usr/CML/JMA/java/websvr/code/LoadDIA.class
   /usr/CML/JMA/dia/runDIA.bat
   ```

3. Edit the paths specified in the runDIA.bat file on the target system. If a path includes spaces, the path must be enclosed in double-quotation marks, or the path must be specified using the short MS-DOS version of the path name. For Win/NT, all backslashes (\) must be escaped; thus, two backslashes (\\) are typed. The following screen shows the example of runDIA.bat on Win/NT:

```
SET DIA_JAVA_PATH="c:Program Files\\JavaSoft\\JRE\\1.1\\bin\\jre.exe"
SET DIA_JAVA_LIBPATH="c:Program Files\\JavaSoft\\JRE\\1.1\\lib"
SET DIA_DIA_PATH="c:Program Files\\JavaSoft\\JRE\\1.1\\bin"
SET DIA_URL="http://rs600033t.itso.ral.ibm.com/nways"
SET DIA_NWAYS_SERVER="rs600033t.itso.ral.ibm.com"

rem ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
rem The remainder of this file should not need to be edited.
rem ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.
.
.
```

The runDIA.bat for Win/95 will be similar to the following screen:

```
SET DIA_JAVA_PATH=c:Progra~1\JavaSoft\JRE\1.1\bin\jre.exe
SET DIA_JAVA_LIBPATH=c:Progra~1\JavaSoft\JRE\1.1\lib
SET DIA_DIA_PATH=c:Progra~1\JavaSoft\JRE\1.1\bin
SET DIA_URL="http://rs600033t.itso.ral.ibm.com/nways"
SET DIA_NWAYS_SERVER="rs600033t.itso.ral.ibm.com"

rem ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
rem The remainder of this file should not need to be edited.
rem ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.
.
.
```

4. Execute the batch file runDIA.bat.

   You should see the following screen. The warning message about SNMP users.def and systems.def files will occur if SNMP service is not configured on this workstation; ignore the message.

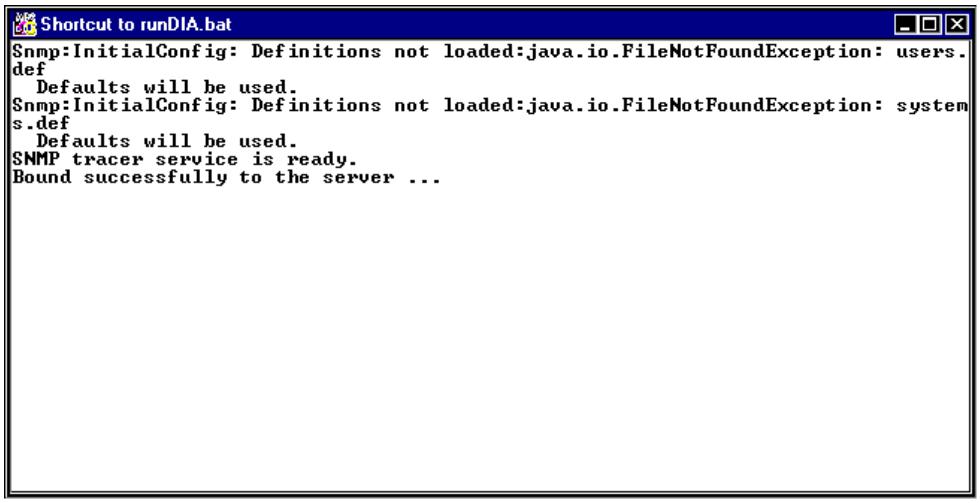


Figure 300. DIA Client on Windows-Based System

After you install and start the DIA client on target system, use the dpadmin command to customize performance management on the network management server (see 7.3.2, “DIA Configuration” on page 217). The DIA topology that configured remote DIAs will look like Figure 301.

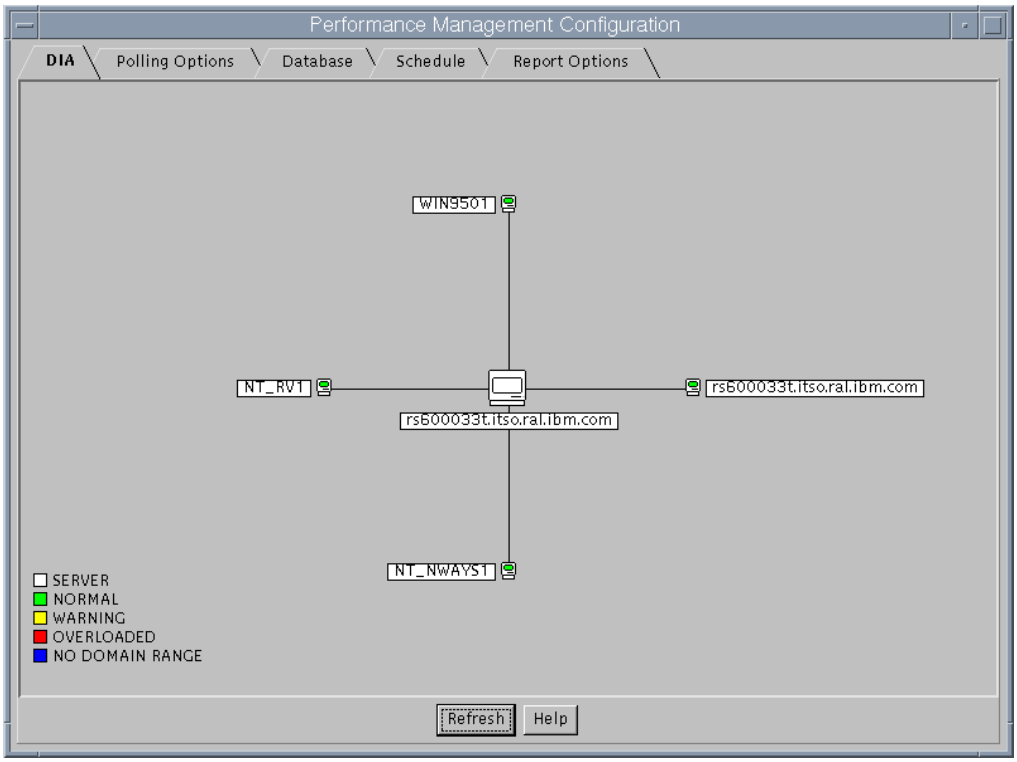


Figure 301. DIA Topology with Three DIA Clients Running

9.5 Using Nways Workgroup Manager for NT

This section covers the configuration required for Nways on the NT platform for scenario 2. After the initial installation we discovered the network.

9.5.1 Discovering the Network

After the setup and installation of Nways Workgroup Manager for Windows NT the next step is to discover the network connected devices. This operation is necessary in order to be able to do the following:

- Configure
- Customize
- Enable

The tools will allow you to perform management functions on the specific network connected hardware. The initial System Administrator screen is shown in Figure 302.

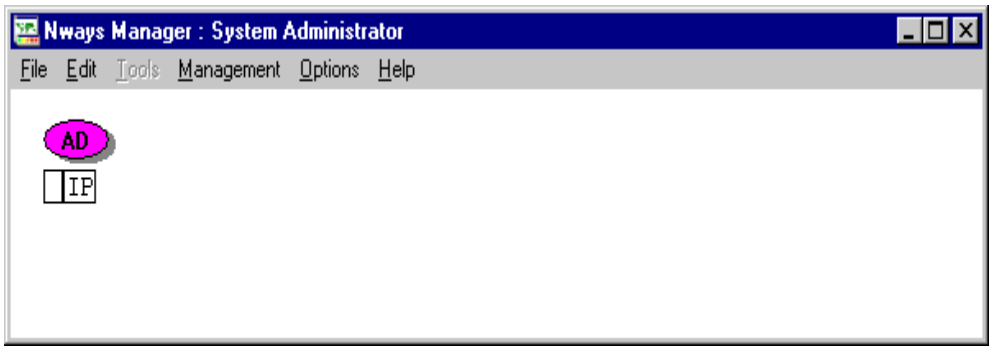


Figure 302. Nways System Administrator Panel

To initiate an automatic discovery of the network that your network management station is connected to, double-click the left mouse button on the **AD IP** icon displayed in Figure 302.

The panel in Figure 303 will be displayed. By clicking once on the **Yes** option you will initiate the automatic network discovery process.

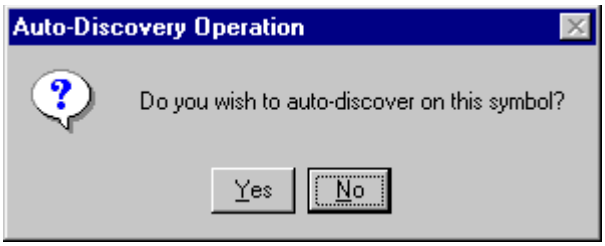


Figure 303. Auto-Discovery of an IP Network

The length of time that it takes Nways Workgroup Manager to discover all the network-related devices connected to the chosen IP network is totally dependent on the numeric size of the installed hardware base of the network.

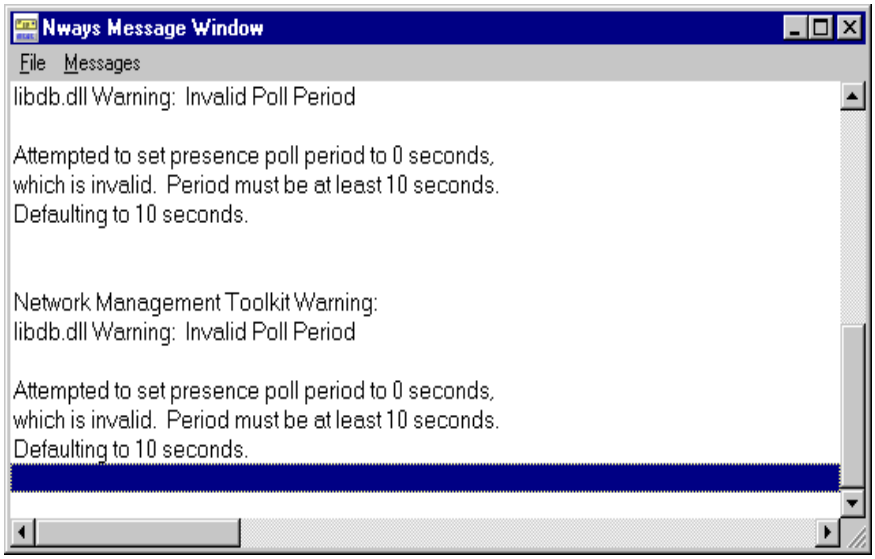


Figure 304. Nways Message Window

If during the discovery process any problems have been encountered by Nways Workgroup Manager, a panel message window similar to that shown in Figure 304 on page 320 will appear. All problems, errors and non-complaints will be listed for information purposes within this panel.

Once completed with the auto-discovery of the IP network Figure 305 appears. With the completion of the auto-discovery process the following three symbols are created:

- Subnetworks
- Sites
- Subsystem

These symbols allow the user to further do the following functions:

- Manage
- Configure
- Fine tune
- Discover other associated networks and hardware devices linked to the selected IP network in this example

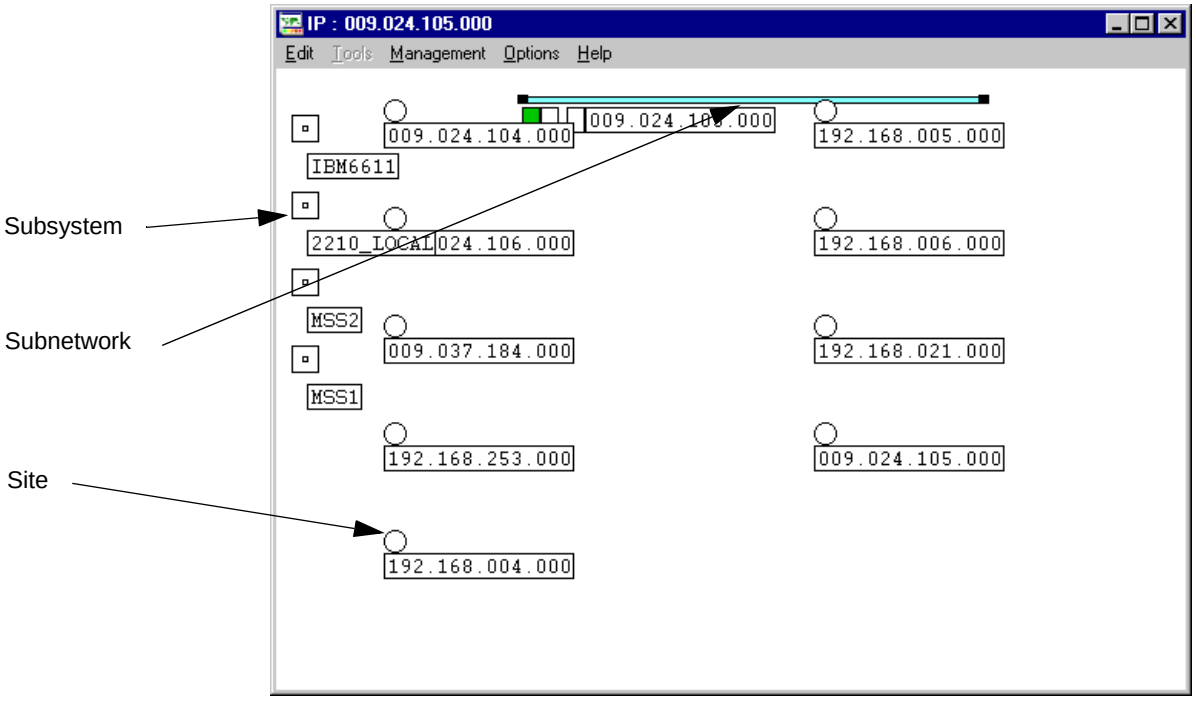


Figure 305. Site View for 9.25.105.0 with Auto-Discovery Complete

Figure 306 on page 322 shows the IP network view after discovery completed. As the network in scenario 2 for managing by Nways Workgroup Manager is part of network in scenario 1, we can see the following networks in the IP view:

- 9.24.104.0
- 9.24.105.0
- 9.24.106.0
- 9.37.184.0
- 192.168.4.0
- 192.168.5.0
- 192.168.6.0
- 192.168.21.0
- 192.168.253.0
- 192.168.254.0

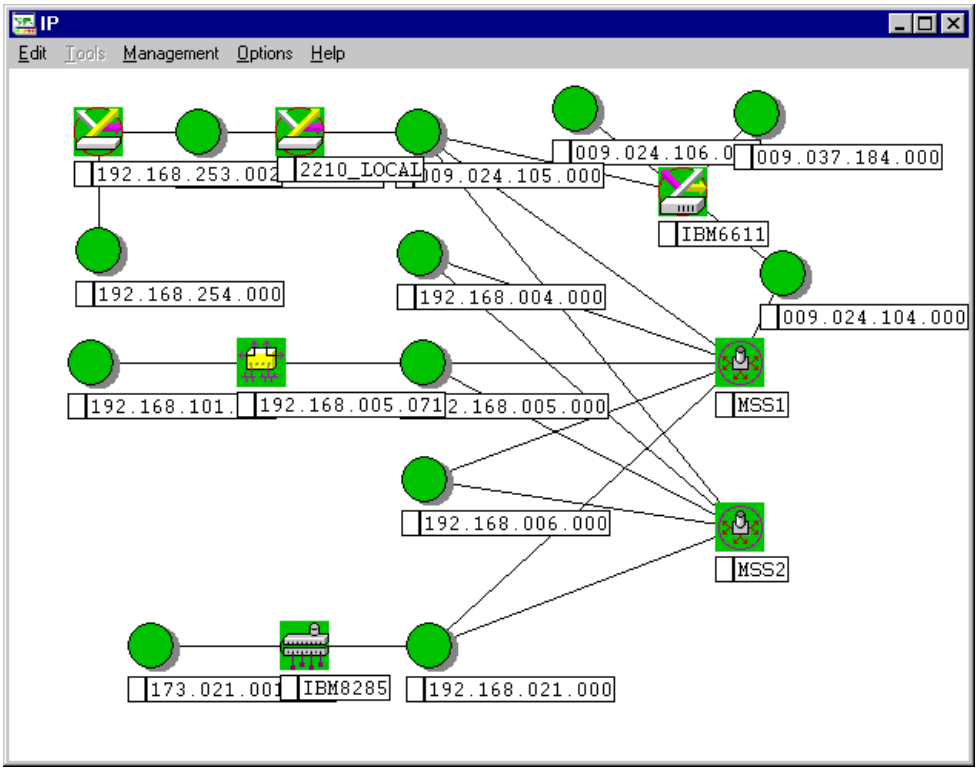


Figure 306. IP Network View after Auto Discovery Completed

These subnetworks displayed because they were found in the MSS1 interface during auto-discovery. MSS1 and MSS2 were configured to back up each other so we can see the connections from subnetwork 9.24.105.0, 192.168.4.0, 192.168.5.0, 192.168.6.0, and 192.168.21.0 to both of them. Here we concentrate on only some of the subnetworks and devices.

The subnetworks to be managed are:

- 9.24.105.0
- 192.168.5.0
- 192.168.253.0
- 192.168.254.0

The network devices to be managed are:

- IBM2210: 9.24.105.70, 192.168.254.1
- IBM8260: 9.24.105.117
- IBM8271: 192.168.5.71, 192.168.254.71
- IBM8273: 9.24.105.98
- IBM8274: 9.24.105.99
- IBM8275: 192.168.5.75

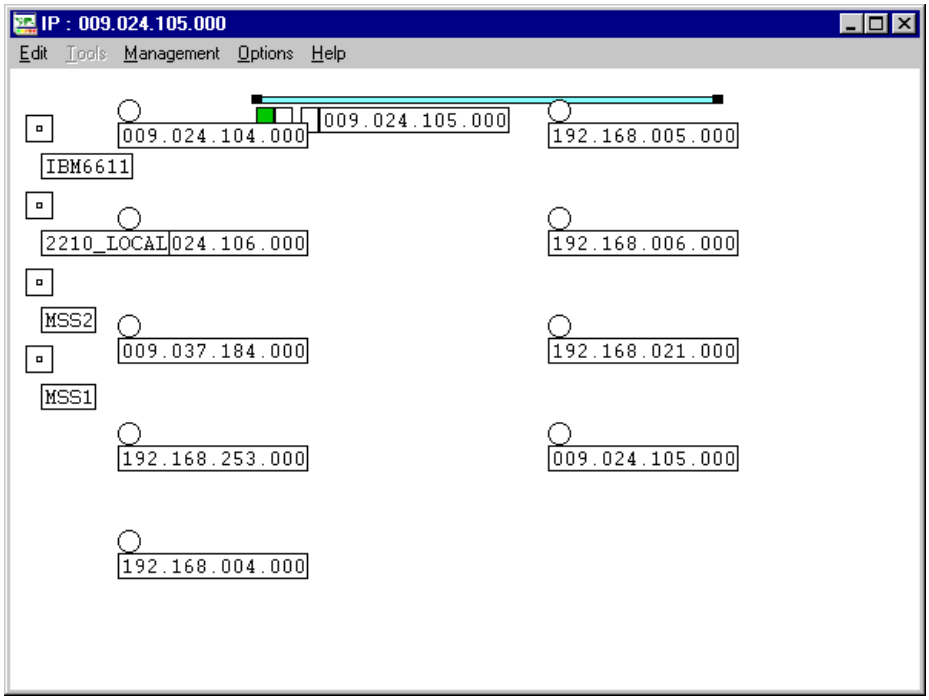


Figure 307. Associated Networks that Have Been Discovered

When you double-click on the site symbol 009.024.105.000 in Figure 306, the IP:009.024.105.00 window will be displayed as shown in Figure 307. There is a thick bar named 009.024.105.000 which represents the subnetwork on the top of this window. Double-click on this subnetwork symbol, and Figure 308 which contains the topology for 9.24.105.0 will appear.

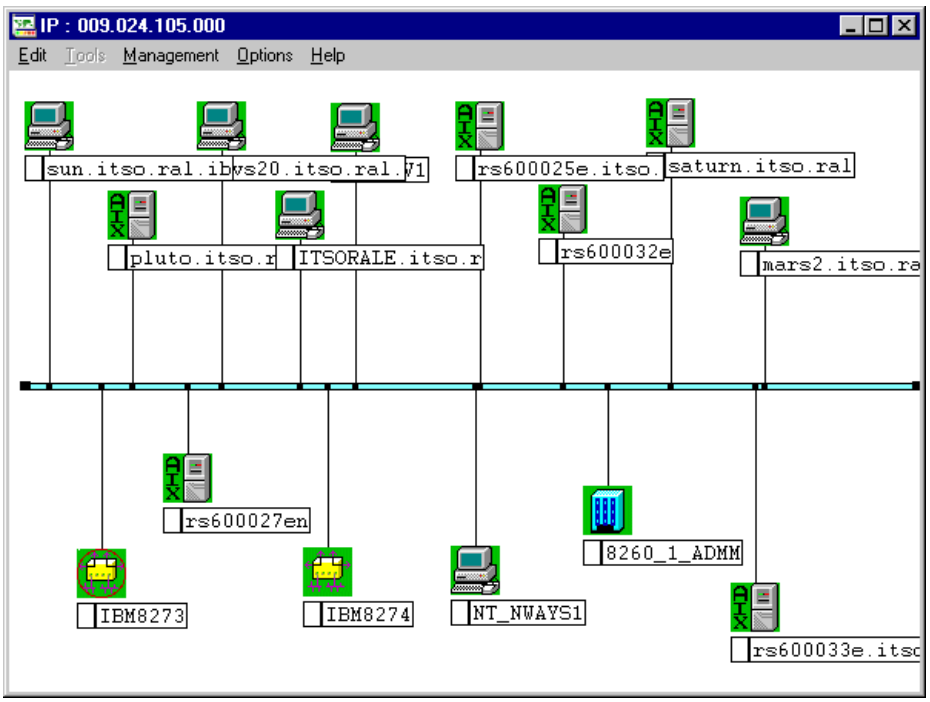


Figure 308. Network Devices Discovered in 9.24.105.0 Subnetwork

9.5.2 Discovering Additional Associated Networks

Frequently, it is necessary to discover alternative networks other than the network to which your network management station is connected. These networks are often linked to the network management station's IP network via one of the following connectivity methods:

- A router
- A switch
- A bridge
- A multiprotocol switched server (MSS)

The auto-discovery process is exactly the same as discussed in 9.5.1, "Discovering the Network" on page 319. The only difference is that the application is launched from the panel displayed in Figure 307.

By double-clicking the left mouse button on the **192.168.005.000** network icon in Figure 306, the window in Figure 309 is displayed.

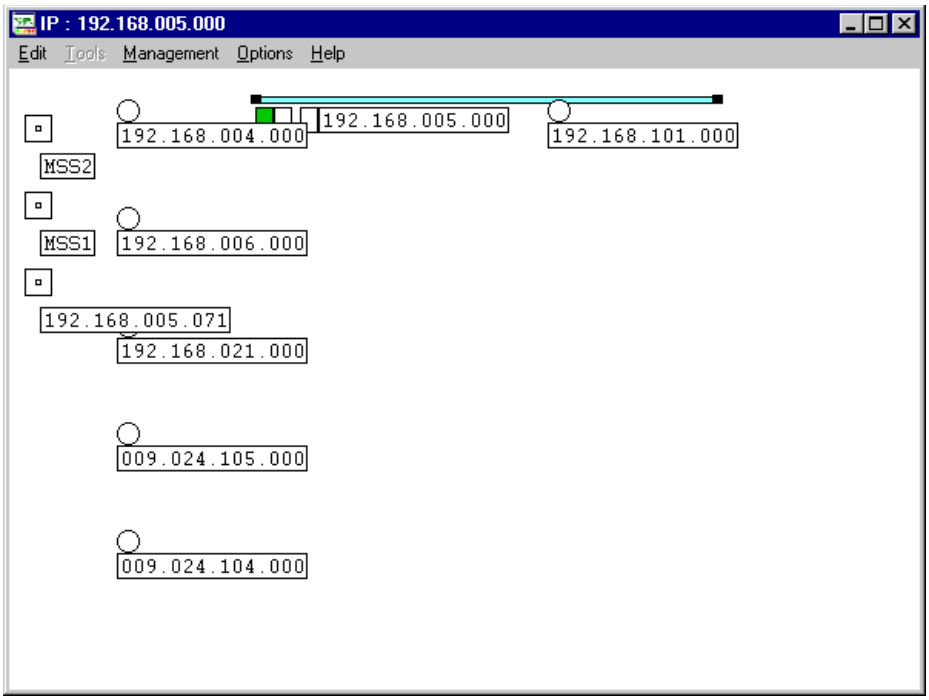


Figure 309. Ethernet 192.168.5.0 Subnetwork

Double-click on the displayed Ethernet subnetwork symbol and a panel similar to that displayed in Figure 311 will be displayed and the auto discovery dialog will prompt for an answer.

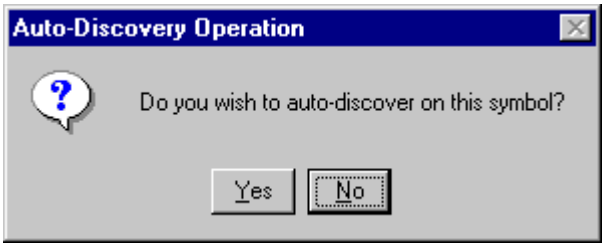


Figure 310. Selecting the Discovery Operation

Left mouse click on the **Yes** and the auto-discovery process will start. In this example, as can be seen in Figure 311, three subsystems were found:

- IBM8275 (192.168.5.75)
- 8271_LOCAL (192.168.5.71)
- WIN9501 (192.168.5.125)

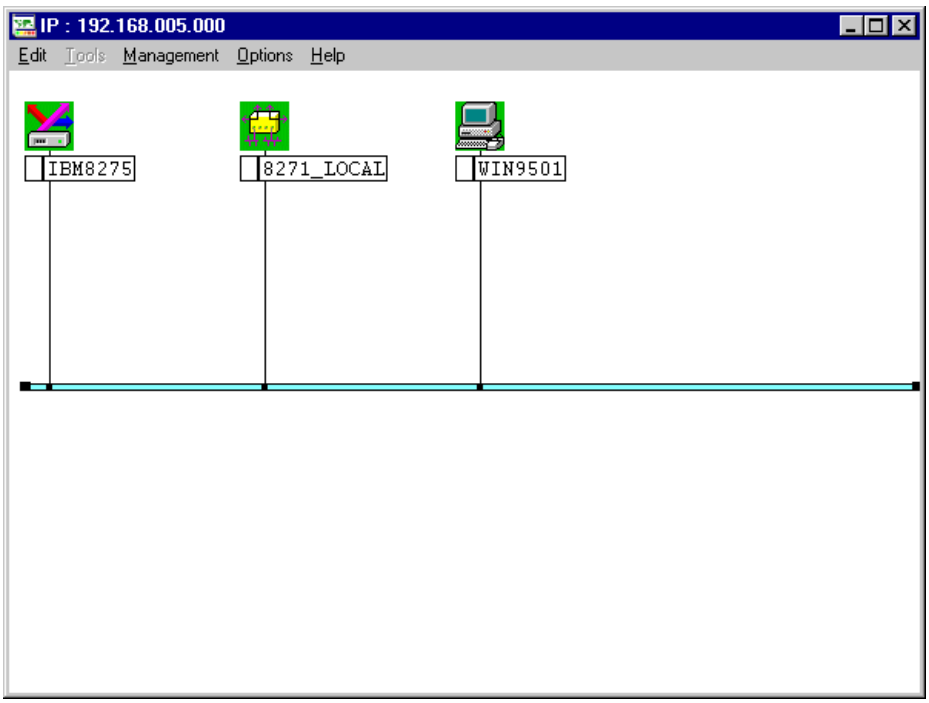


Figure 311. A Fully Discovered Network 192.168.5.0

After every subnetwork was discovered and every subsystem we want to manage was found and represented by various symbols on subsystem windows, these symbols can be rearranged manually. The following list contains the actions that you can do in order to rearrange them:

- Copying Symbols

  To copy a network view element, press and hold the **Ctrl** key, and then click the symbol with mouse button 1. Drag the cursor to the required location and release the mouse button. A duplicate of the symbol is placed in the new location; the original symbol remains in its original location.

- Moving Symbols

To move a symbol or an associated name label, click the symbol or label with mouse button 1, and then drag the symbol or label to the required location. If you click the symbol, the symbol and the label move; if you click the label, only the label moves.

- Modifying Symbols

  To modify the information stored in the database for a selected view symbol, select the symbol you want to modify. Then, select **Edit..Modify..Attributes...** from the menu bar. A dialog box is displayed listing the modification options. Select the modification you want to make and click **Execute**.

- Resizing Symbols

  To resize domain, site, or subnetwork symbols, select the symbol and press the Shift key. Hold down mouse button 2 and drag the cursor to resize the symbol.

- Renaming Symbols

  You can rename any network view element except a mini-symbol. To rename a symbol, select the symbol, and then select **Edit..Modify..Name...** from the menu bar in your network view management window. The Rename dialog box is displayed, showing the old name and prompting you to type a new name. Type a name in the Name field and click **OK**.

- Deleting Symbols

  To delete a symbol or icon, select the symbol or icon you want to remove, and then select **Edit..Clear** or **Edit..Delete** from your window's menu bar.

  - Select the Clear option to remove a single element from your current window; this does not affect the element in any other window in which it is displayed.
  - Select the Delete option to remove all copies of a symbol from your network.

  In the case of subsystems, a dialog box is displayed prompting you to either delete the subsystem from the view only or delete the subsystem and the database records. Select either No or Yes, respectively.

9.6 Application Configuration

Once a network has been discovered by the network management station it becomes necessary to fine tune the discovered network to be able to provide the management station with the alarms, events, and statistics which are all beneficial to the network manager so that a strict control of faults and fault diagnostics can be sustained in order to keep the managed network running at its optimum performance.

First of all, we set the polling parameters for each subsystem (device). Nways Workgroup Manager uses three types of polling:

- Alarm polling is used to determine whether a network device is operating. If an alarm poll is not responded to, you can configure Nways Workgroup Manager to generate a fault.
- Statistics polling is used to poll for real-time and historical statistics.

- Threshold polling is used to poll specific attributes and generate a fault if the configured threshold is exceeded.

Note: Polling is performed only while the Nways Workgroup Manager application is running. If you exit the application, historical statistics and threshold polling will cease until you restart the application.

To see all the subsystems that you are polling and quickly turn polling on or off or modify the polling periods, select **Management..Performance..Polling Summary...** from the menu bar of any View window (Figure 312). The Polling Summary dialog box is displayed as shown in Figure 313.

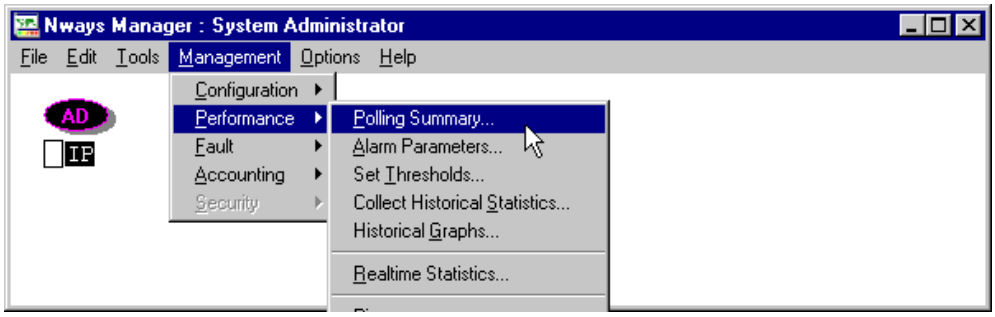


Figure 312. Opening Polling Summary from Menu Bar

The polling summary is shown in Figure 313 on page 327.

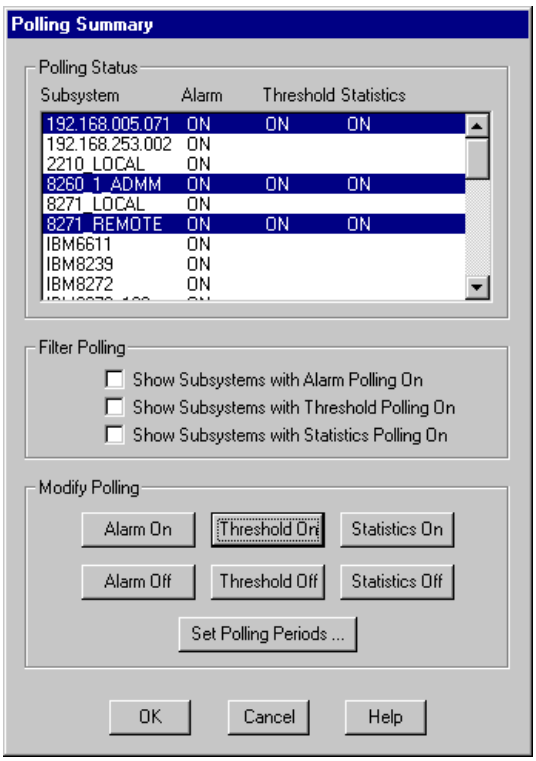


Figure 313. Polling Summary Dialog

You can see whether each subsystem listed is currently being polled for alarms, thresholds, or statistics. Dashes indicate there are no pollable attributes. To

display subsystems for which a particular polling type is enabled, select the appropriate Filter Polling check box and deselect the other Filter Polling check boxes.

The Modify Polling push buttons turn each type of polling on or off for a selected subsystem without using the specific polling dialog box. To modify an existing alarm, a threshold, and statistics polling, use the Threshold Polling and Statistics Polling options. The default alarm polling period and the default severity level are specified in the nwaysbse.ini file. The polling parameters can also be changed in the Alarm, Threshold, and Statistics parameter dialog boxes. To turn polling on or off, select one or more entries from the Polling Status list, click the appropriate Modify Polling push buttons, and click **OK**. For example, we turned on the Threshold and Statistics for 8271_612, 8260_ADMM, and 8271_Local.

Next we will set the polling periods for these devices by clicking on **Set Polling Period.** Figure 314 appears. From this dialog, you can enter a polling period value for alarm, threshold, and statistical polling. The minimum value permitted for a polling period is calculated. The Performance Handler first identifies the smallest polling period already specified for the selected subsystems and then performs the following calculation:

```
Minimum Polling Period = (2 * Transport Time + 1) * (Retry Count + 1)
```

The Transport Time and Retry Count values were entered when you first created your subsystem. These value can be changed from the **File...Modify...Attribute** menus.

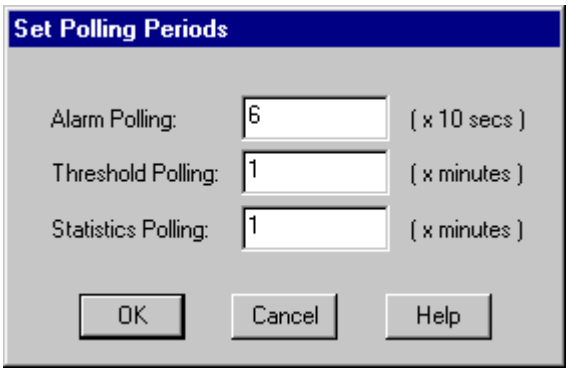


Figure 314. Polling Periods Dialog

The Alarm Polling and Threshold and Statistics Polling are also set up for 1 minute. Click **OK** when finished.

9.6.1 Additional Setup

Additional setup that may necessary is setting up the community name to access the network devices. The community name using to access devices was defined in the subsystem attribute. It can be changed by the following steps:

- Select the subsystem to be changed.
- Select **File...Modify...Attribute...** from the menu bar. The device attribute dialog will be displayed.
- Change the community name for that device and click **OK** to finish.

The Inventory panel can be accessed by selecting a device symbol then selecting **Accounting...Inventory...** from the menu bar (see Figure 315). The Inventory dialog as shown in Figure 316 will be displayed. You can input the information for the device such as inventory number, installation date, serial number, etc. This information needs to be input manually.

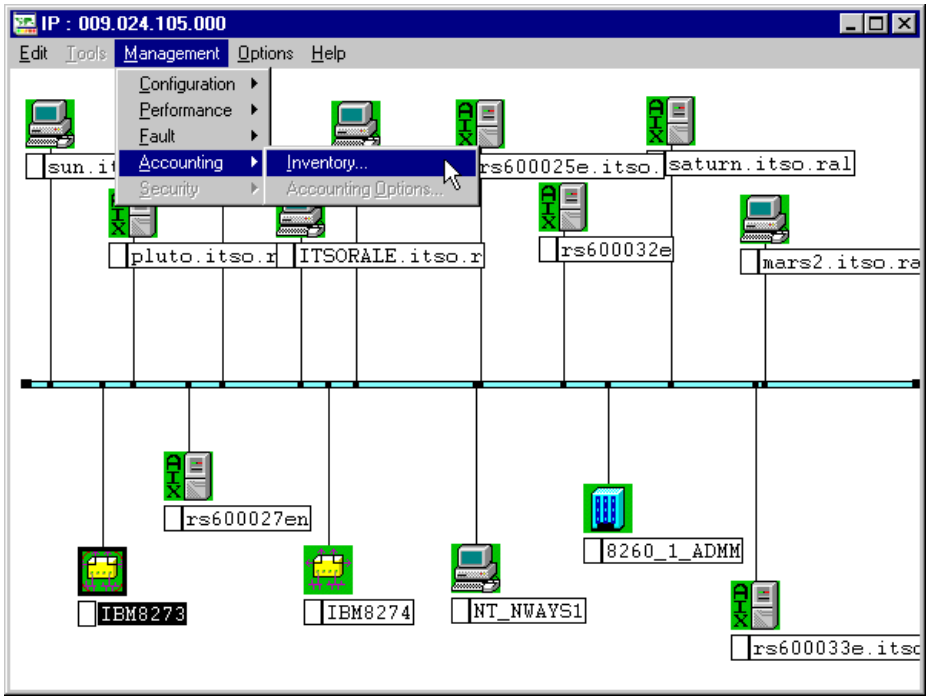


Figure 315. Starting Inventory Control of a Network Device

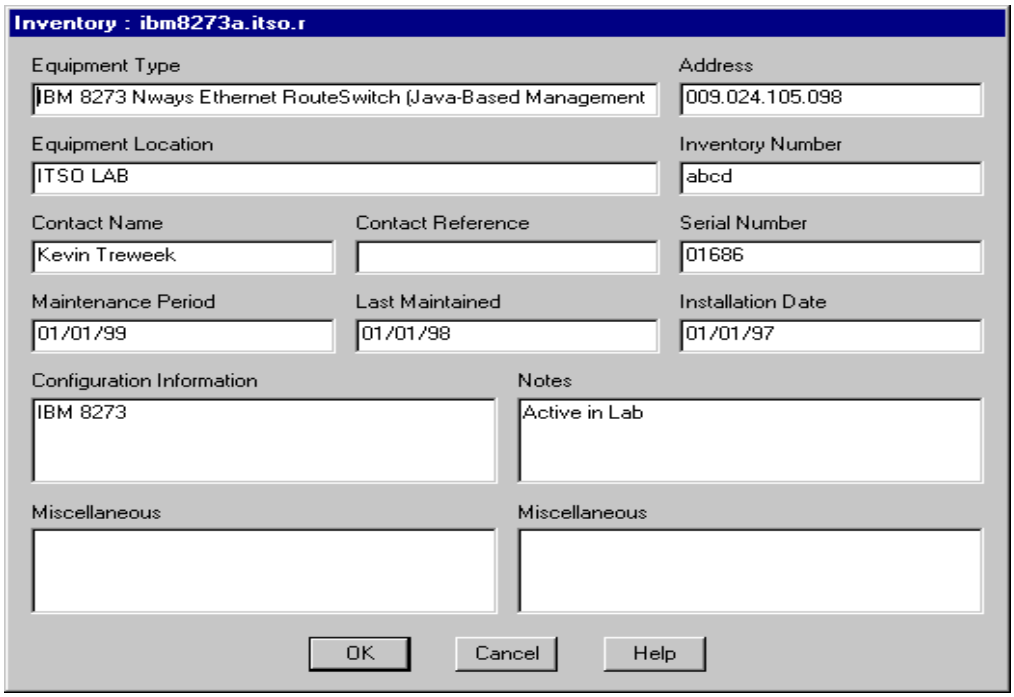


Figure 316. Inventory Information for IBM8273

9.7 Configuration Management

Once you complete the installation and configuration for Nways Workgroup Manager, you can now manage the network using Nways. To configure the devices, you have two methods depending on device specifics and individual preference.

- Use Configuration options from the menu bar.
- Use specific device configuration management such as MSS/MRS/MAS configuration tools, Java Management Application, and Nways RouteVision.

9.7.1 Using Configuration Options

The Configuration options for each device are different. They allow you to configure the device by listing the configuration items for executing. To start Configuration options for a device, do the following:

- Select the device you want to work with using a single click of the mouse.
- Select **Management->Configuration->Configuration Options** from the menu bar (see Figure 317).

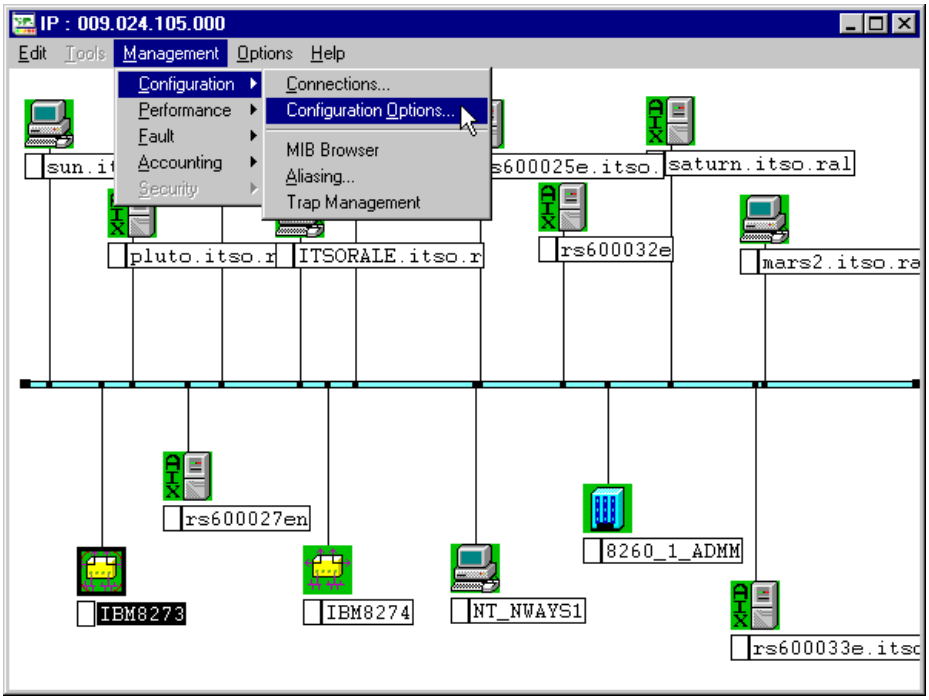


Figure 317. Starting Configuration Options from Menu Bar

The configuration options window will appear.

Figure 318 is the configuration options for IBM8273. As listed in the window, there are two methods to configure the 8273:

- Launch RouteSwitch Manager (or RouteVision)
- Telnet to device

You can select a method of configuration by simply selecting the list and clicking **Execute** to start it.

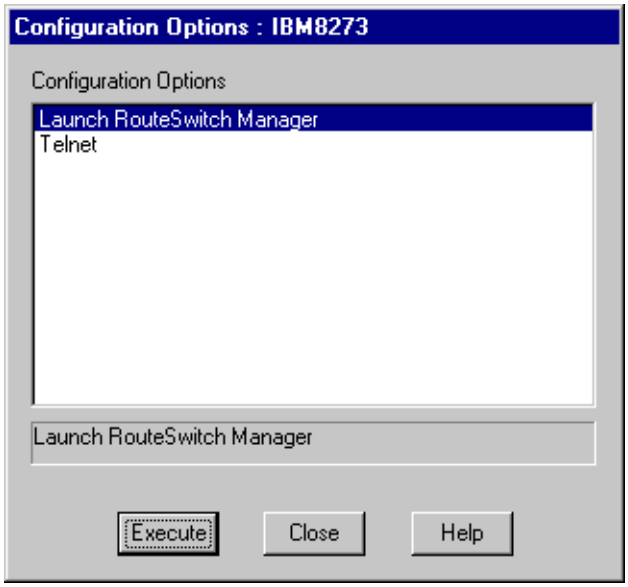


Figure 318. Configuration Options for IBM8273

For an 8260, there are more configuration options, as displayed in Figure 319.

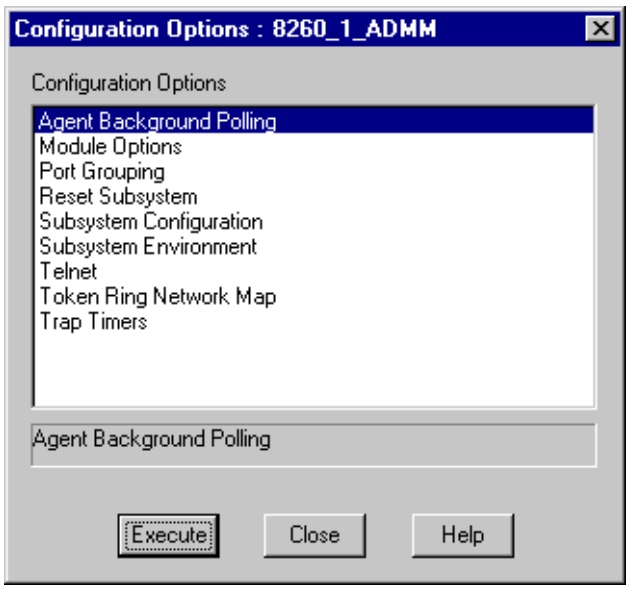


Figure 319. Configuration Options for 8260

You can configure the following for the 8260:

- Agent Background Polling
- Module Options
- Port Grouping
- Reset Subsystem
- Subsystem Configuration
- Subsystem Environment
- Telnet
- Token Ring Network Map
- Trap Timers

By selecting the Module Option and clicking **Execute**, the Module Options window shown in Figure 320 will displayed.

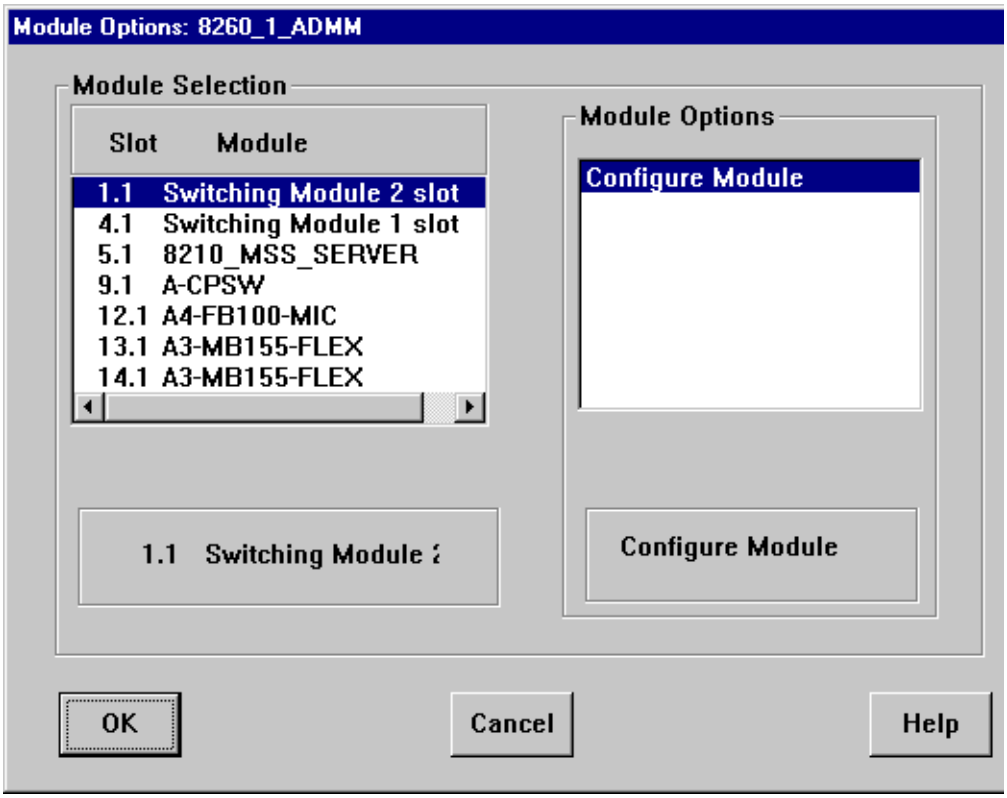


Figure 320. Module Options Dialog for 8260

From this Module Options windows you can configure or modify parameters for each 8260 module listed in the Module selection windows.

The Configuration Options will work in this way for every network devices.

9.7.2 Using JMA and Configuration Tools

The Nways Workgroup Manager Java-based management application (JMA) is similar to a JMA in Nways Manager for AIX. By using the JMA, you can manage general elements of any SNMP device without having to install an actual device manager.

For details of using and configuring JMA, refer to *Nways Workgroup Manager for Windows NT User's Guide*, SA27-4194-02 or you can follow the JMA and JPM guide in Chapter 7, "Nways Java/Web Management Applications" on page 211. Figure 321 is the example view of JMA for MSS.

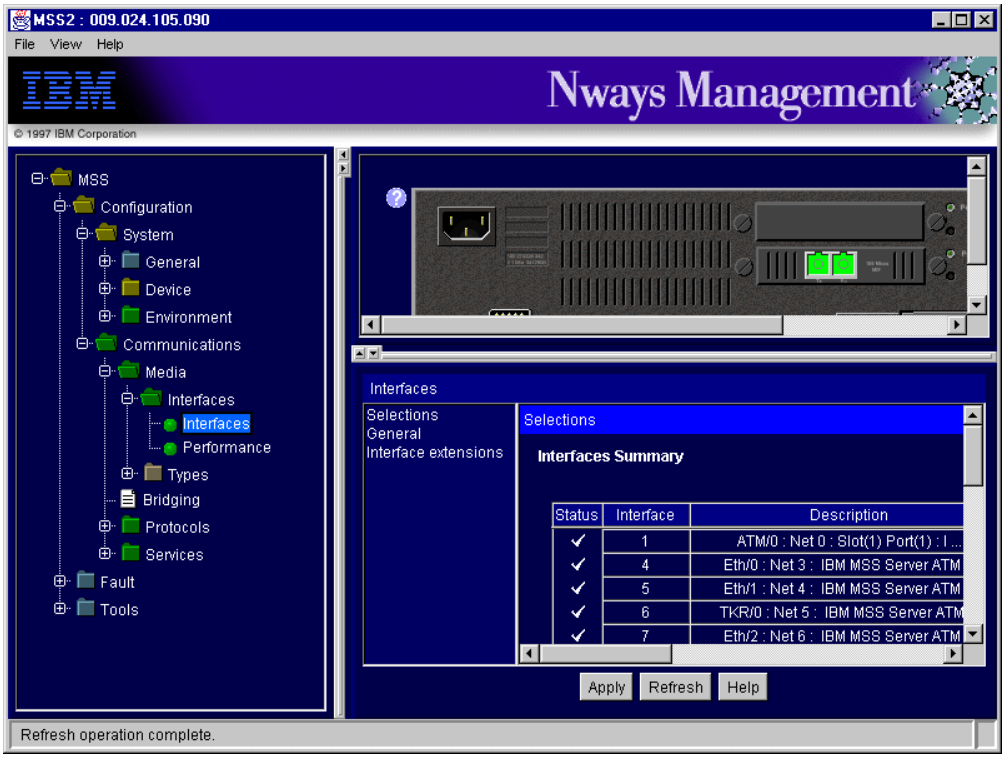


Figure 321. 8210 JMA View

The following configuration tools are supported under Nways and can be launched from the JMA view when running the GUI locally on the network management station (they are not supported through web-browser access from the JMA):

- The MSS Configuration Program for MSS
- The MRS Configuration Program for 2210
- The MAS Configuration Program for 2216

To start configuration tools from JMA, you must configure the directory and executable command for these tools (see 9.4.2, “2210 Multiprotocol Routing Services Configuration program” on page 315). Once the JMA window for a device opens, you will see the Configuration Tool page under the Tools folder in the Navigation tree. So you can launch the MSS configuration tool by:

- Double-clicking on the MSS subsystem symbol to open JMA.
- Selecting **Configuration Tool** under the Tools folder.
- Clicking on **Apply** (see Figure 322 on page 334).

This will launch the MSS Configuration tool and you can work on it.

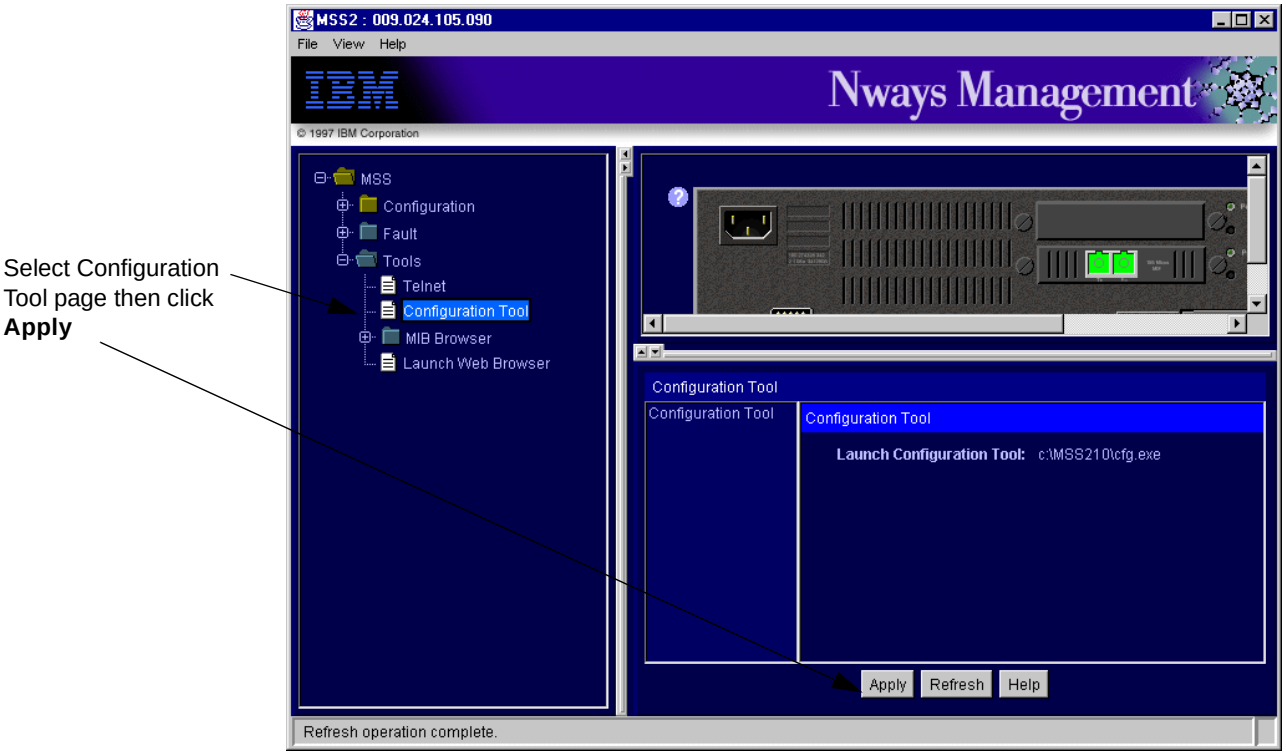


Figure 322. Starting MSS Configuration Program from 8210 JMA

9.7.3 8260 Management

The 8260 accessed can be configured by double-clicking on the device. Hub is shown in Figure 323 on page 335.

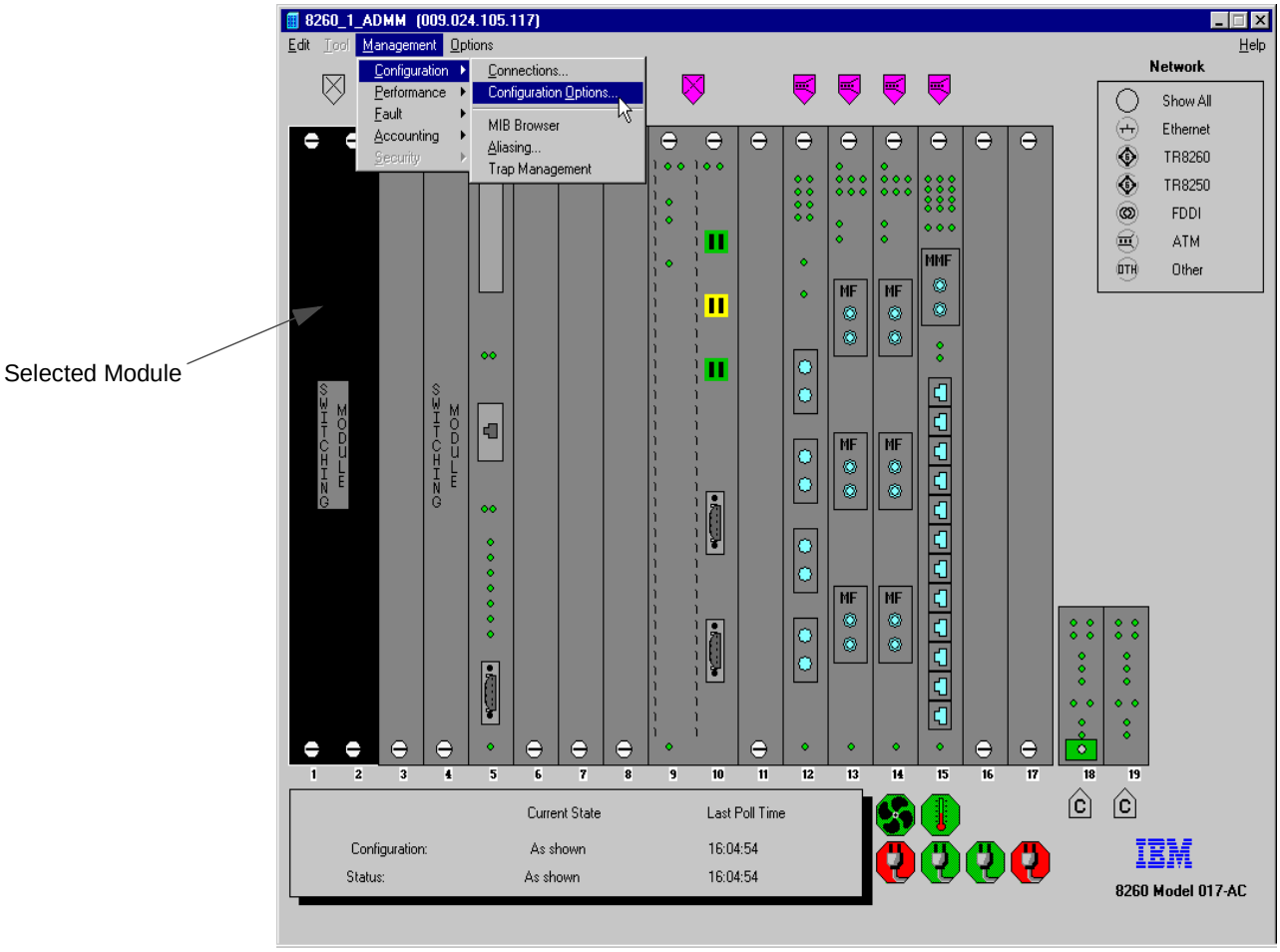


Figure 323. Starting JMA for 8260 Switch Module from 8260 Device-Specific View

Select **Management** followed by **Configuration Options** (Figure 324 on page 336).

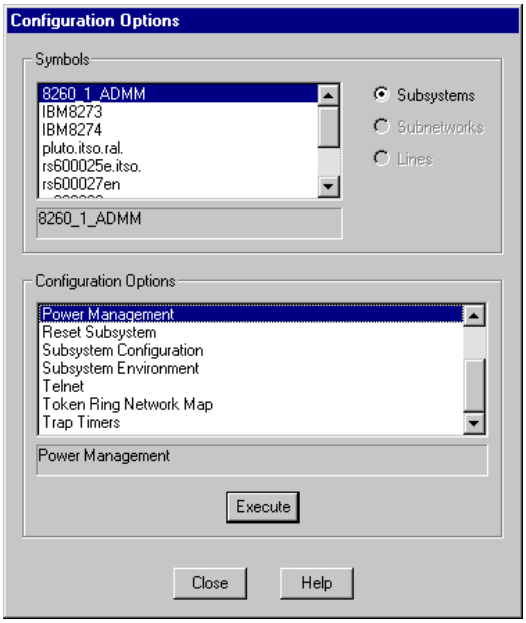


Figure 324. Configuration Options

If we double-click on the switch module, the JMA shown in Figure 325 on page 336 will appear.

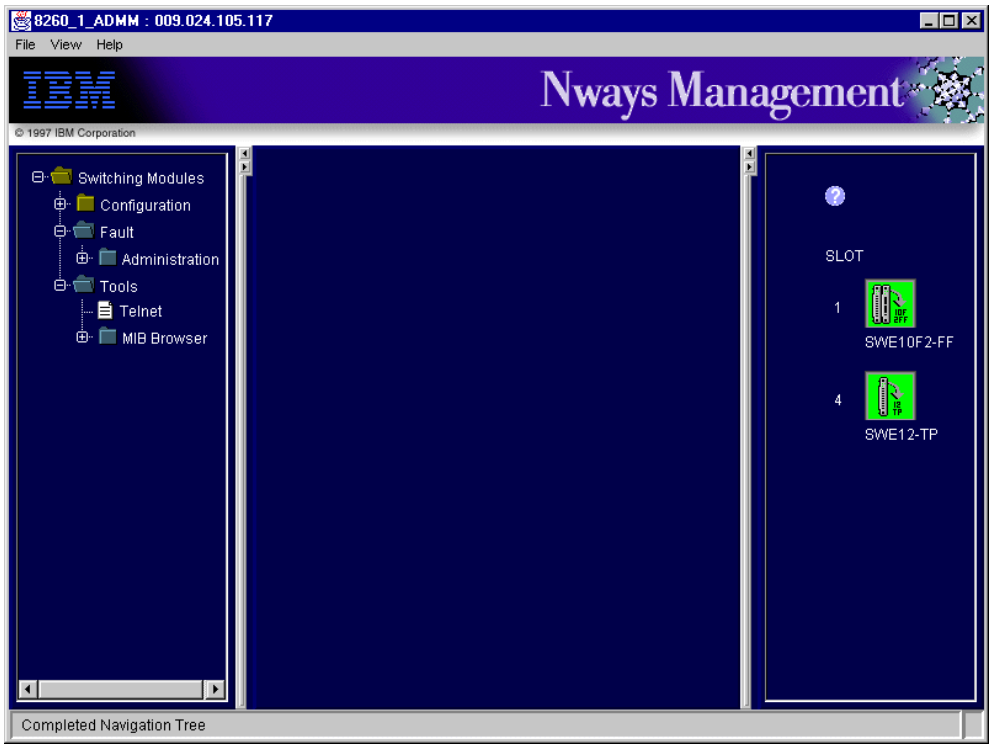


Figure 325. Configuration Options for 8260 Switch Module (JMA View)

This shows the switch modules. If we double-click on this we can see the configuration shown in Figure 326 on page 337.

Figure 326. JMA for Selected Switch Module

This shows the JMA for switch module on 8260.

Some ATM configurations can be viewed from the configuration options. These are shown in Figure 327 on page 337.

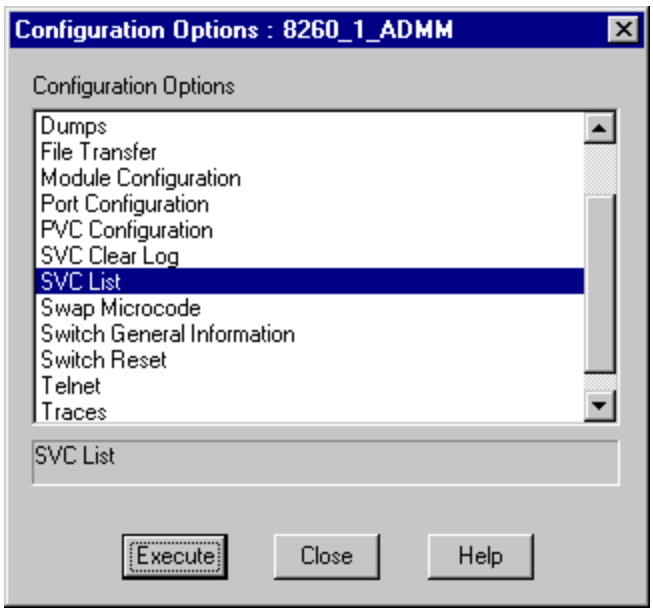


Figure 327. ATM Options

9.8 Fault Management

Next you may configure trap management if you want to use the Trap windows to display traps received from network devices. To open trap windows, select **Management...Configuration...Trap Management...** from the menu bar (see Figure 328). The Trap window is shown in Figure 329.

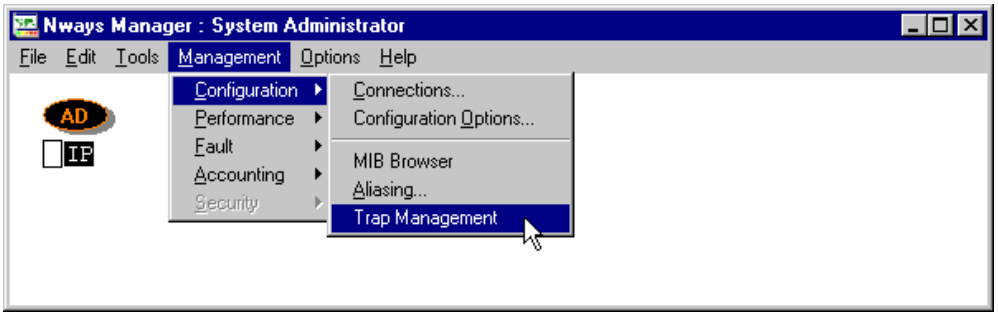


Figure 328. Starting Trap Management from the Menu Bar

The Trap Window displays the traps received from devices but we must load the ASN.1 Trap File to this window to enable Trap interpretation. To load the ASN.1 Trap File, select **Tools...Load ASN.1 Trap File...** from the menu bar on the Trap Window (see Figure 329).

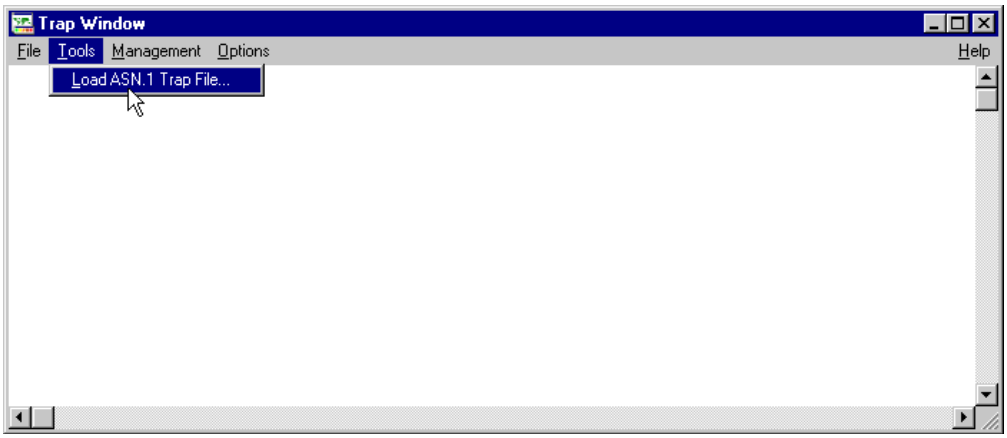


Figure 329. Tools for Load ASN.1 Trap File

The ASN.1(MIB) trap file will be listed in the window as shown in Figure 330. Select the file to load into Trap Window and click **Open** to start loading. If you have other MIB files associated to specific devices, you can copy those files to this system then load them to Trap Window. In our scenario, we loaded the following ASN.1 files:

- ibm8271.mib
- ibm8271e.mib
- ibm8250.mib
- ibmcpsw.mib
- ibm8225.mib

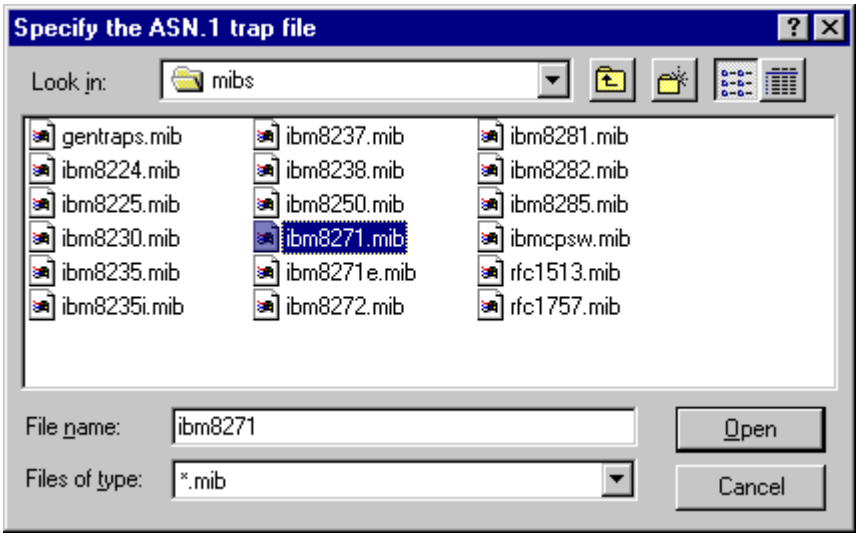


Figure 330. ASN.1 Files Selection Dialog

After loading ASN.1 trap files to Trap Windows select **File...Save...** from the menu bar to save the configuration of this Trap Window. So next time you start Nways Workgroup Manager, you can open the saved trap configuration file to Trap Window.

In terms of fault management, when a device or line fault occurs, you will need to identify, filter, and record the fault, and initiate the appropriate corrective action. A fault condition that occurred in Nways Workgroup Manager is one of the following:

- A polling time-out
- A breach of an attribute threshold that you defined
- Unsolicited information supplied by a subsystem in the form of a trap message

When a fault is recognized anywhere on your network, the following steps occur:

- The appropriate subsystem symbol flashes in the network view. This propagates up the symbol hierarchy.
- An entry for the fault is created in the Current Faults dialog box and the fault is indicated as being active.
- The fault count in the Status window is incremented, and the appropriate symbol in the window flashes.

A faulty subsystem in your network causes the subsystem icon and containing symbol further up in the network hierarchy to flash. In the case of a faulty line or subnetwork, the line or subnetwork itself flashes. A symbol alternates (the symbol color changes) between its current status color and the highest fault level color reported by any faulty subsystem with which it is associated.

The five fault colors are described as follows:

- Level 1 Lemon Yellow Least Critical
- Level 2 Yellow Orange
- Level 3 Orange
- Level 4 Red Orange

- Level 5 Red Most Critical

In addition to the network view symbols flashing, the Fault Level Indicators in the Status window, which is initially present at the bottom right corner of the view window, flash at the appropriate fault level. Symbols continue to flash until you take appropriate action to stop them through the Current Faults dialog box, unless the fault is a system-cleared fault, which is either:

- Faults due to a threshold being exceeded
- Faults due to alarm polling

Too many acknowledged and system-cleared fault records can make your system run slowly, and too many historical faults will use up your disk space. You can specify the amount of data to store in the fault event files through the Fault Setup dialog box.

Select **System..Fault Setup...** from the Status window menu bar. The Fault Setup dialog box is displayed as shown in Figure 331.

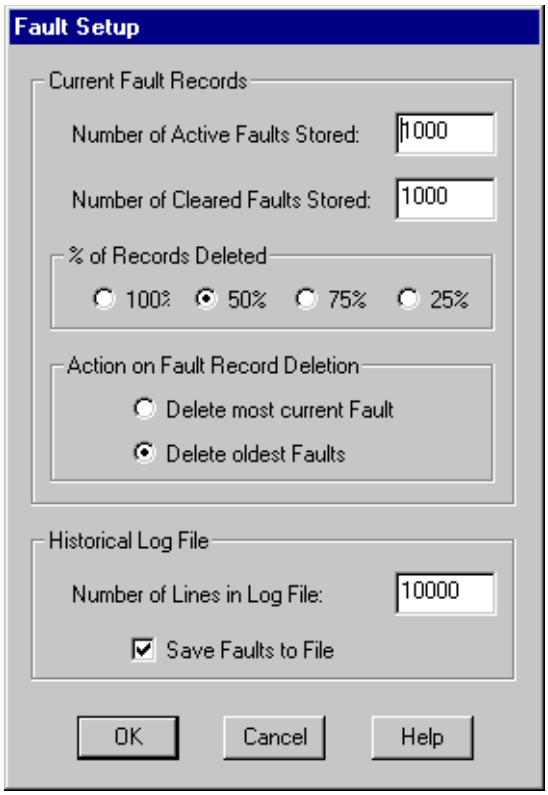


Figure 331. Fault Setup Dialog

The Number of Active Faults Stored field allows you to specify the number of fault records for active faults that are saved in the network view.

The Number of Cleared Faults Stored field allows you to specify the number of system-cleared fault records that are saved in the network view.

Once you have set the limit on the number of records, you specify how much data is deleted when one of these limits is reached. The Action on Fault Record Deletion radio buttons allow you to have the most current faults, or the oldest

faults deleted. The percentage of records deleted is specified in the % of Records Deleted field.

The Number of Lines in Log File field allows you to specify the number of historical fault records that are saved in each of the fault event files. The default value is 10000. To save these records, enable the **Save Faults to File** check box.

9.8.1 Setting/Filtering Fault Options

Since one source of faults come from unsolicited information supplied by a subsystem in the form of a trap message, you can configure these traps to be associated with certain fault conditions or filter them from initiating fault condition.

To start Fault Options, select **Management...Fault...Fault Options...** from the Status Windows menu bar. Figure 332 will displayed.

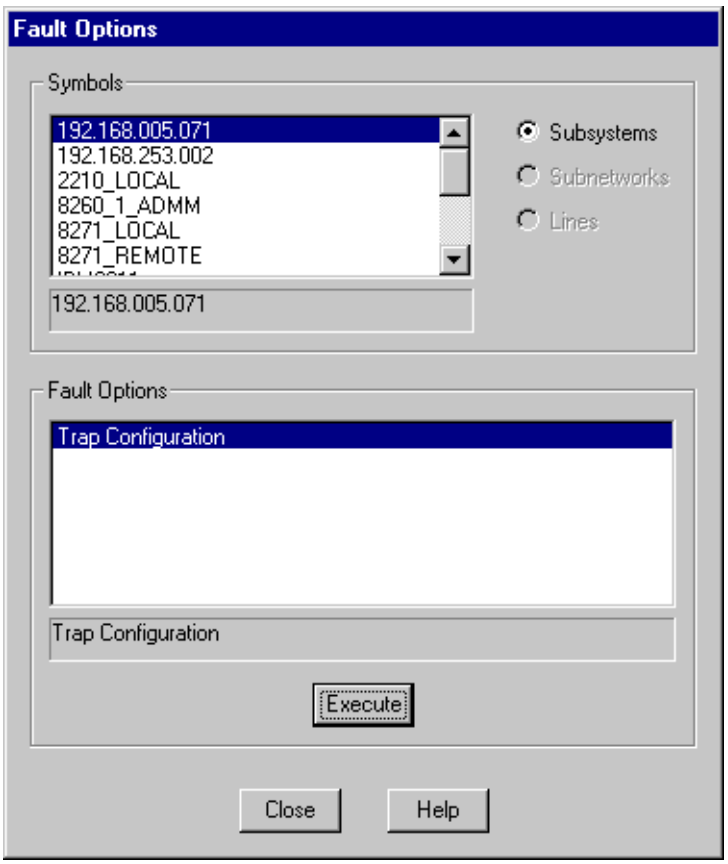


Figure 332. Fault Options Dialog

Note: If you select a device icon then select **Management...Fault...Fault Options** from the menu bar, you will see only Fault Options for that device.

From the Fault Options dialog, select a device from the Symbols panel and **Trap Configuration** in the Fault Options panel then click **Execute.** The Trap Configuration of that device will come up as shown in Figure 333.

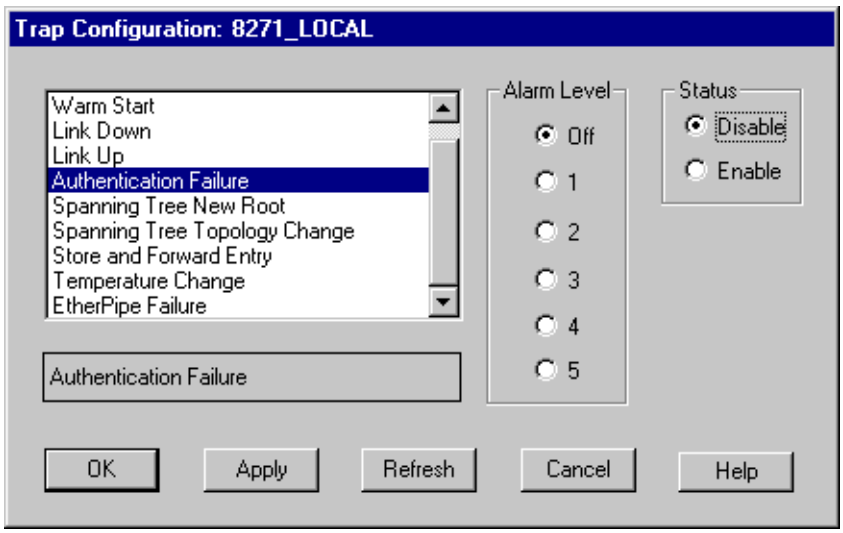


Figure 333. Trap Configuration Dialog

From this Trap Configuration dialog, you can set the Alarm Level for each trap or turn it off (prevent fault condition to occur). For example, select the **Authentication Failure** trap and set Alarm Level to Off then click **Apply.** This will turn off fault condition for the authentication failure trap for this device (8271_LOCAL).

The right-most status panel on this dialog shows the current setting parameter in the device configuration. You can set/change this parameter to the device if you have the Write Access community name.

For the 2210, from the interface we can set the traps.

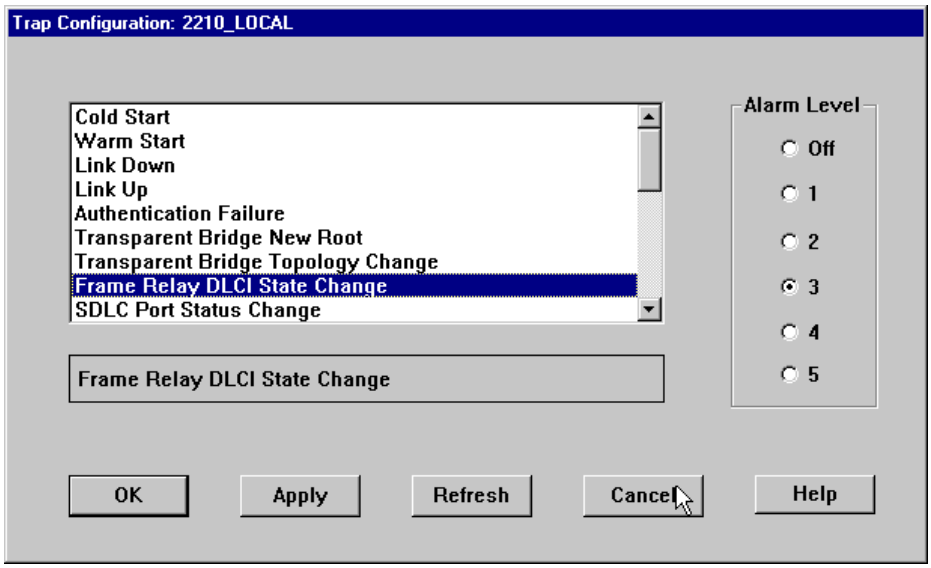


Figure 334. Trap Configuration for 2210

Select **OK**.

9.8.2 Adding Traps to Fault Conditions from Trap Window

To add traps to the fault conditions select **Fault Conditions** from the Trap Window menu bar as shown below.

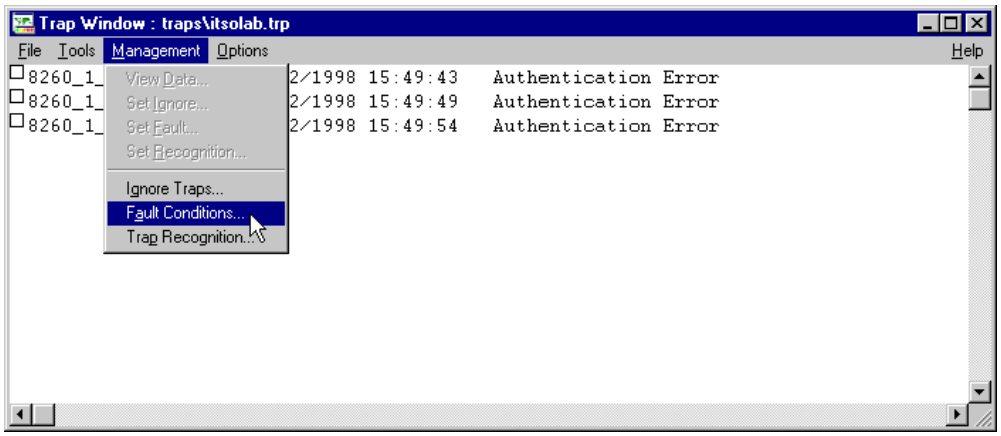


Figure 335. Starting Fault Condition Dialog

Select the trap, device and the fault level required for this trap.

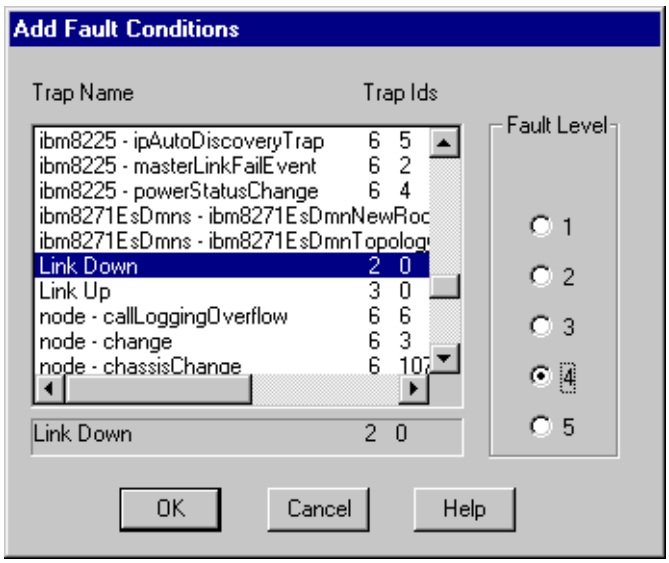


Figure 336. Adding/Changing Fault Conditions

Once selected click on **OK**. The trap now appears in the Fault Conditions window.

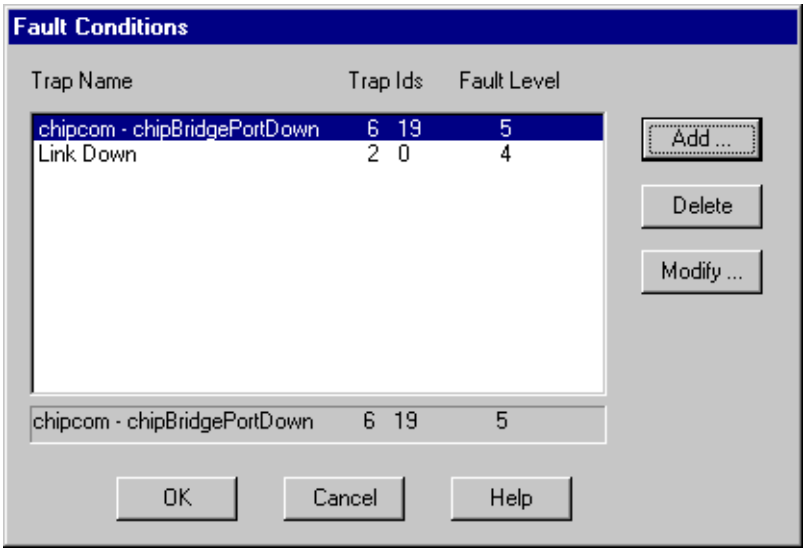


Figure 337. Fault Conditions Dialog

When the Link Down trap is received with an alarm level of 5 the box next to the event will be red.

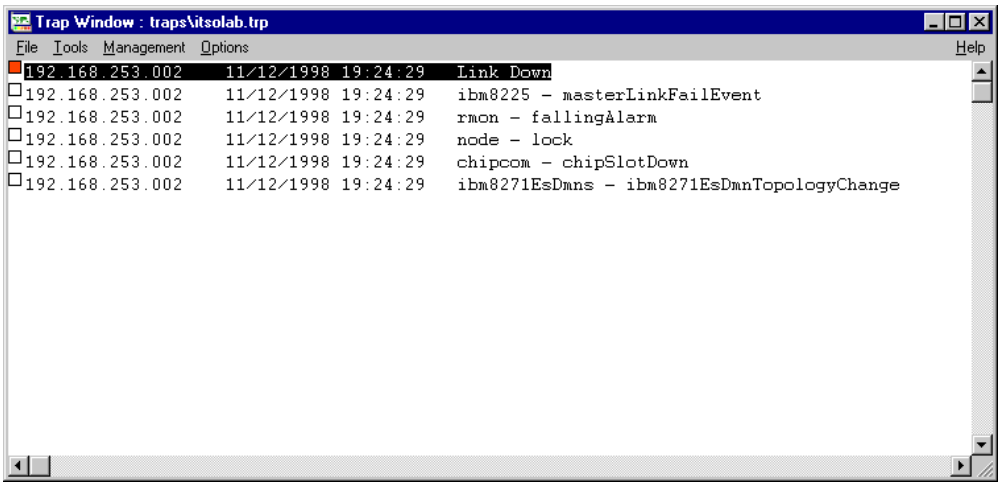


Figure 338. Link Down Trap Received in Trap Window

9.8.3 Using the Current Fault Window

The status window is controlled by the five event categories. By double-clicking on one of the boxes you will see the current events of that category.

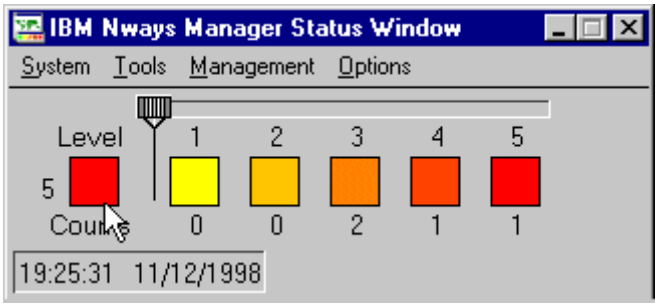


Figure 339. IBM Nways Manager Status Manager

By clicking on one of the severity boxes the current faults for that severity will be displayed (see Figure 340 on page 345).

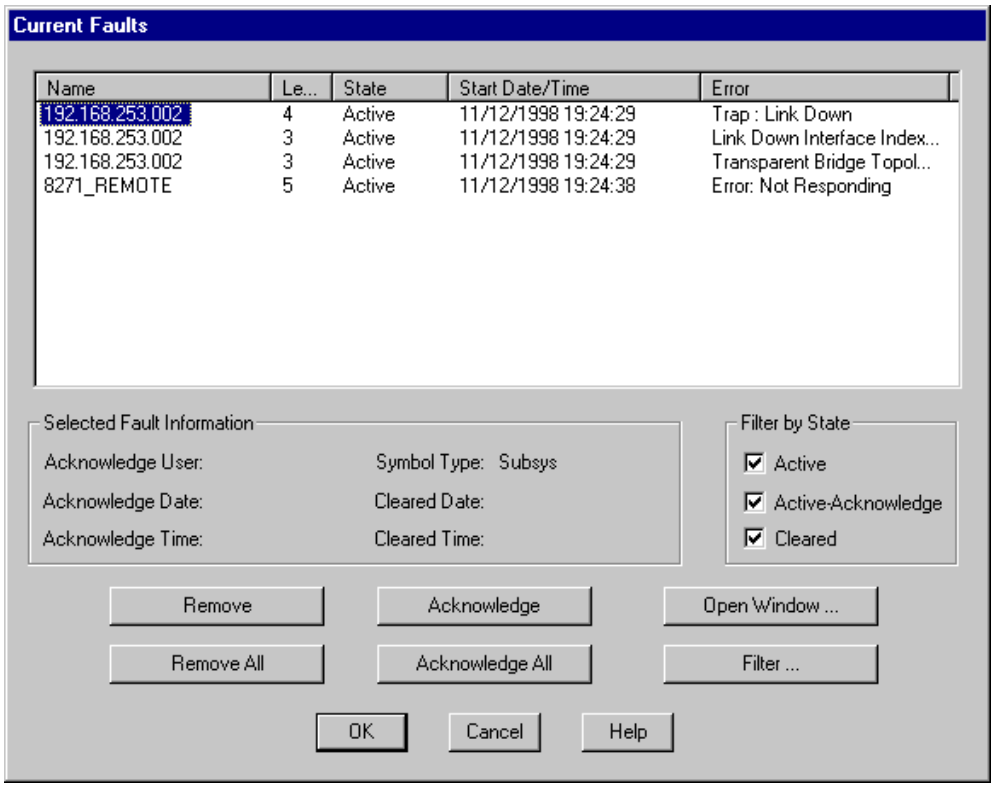


Figure 340. Current Faults Window

From here we can perform some filtering. Select **Filter**.

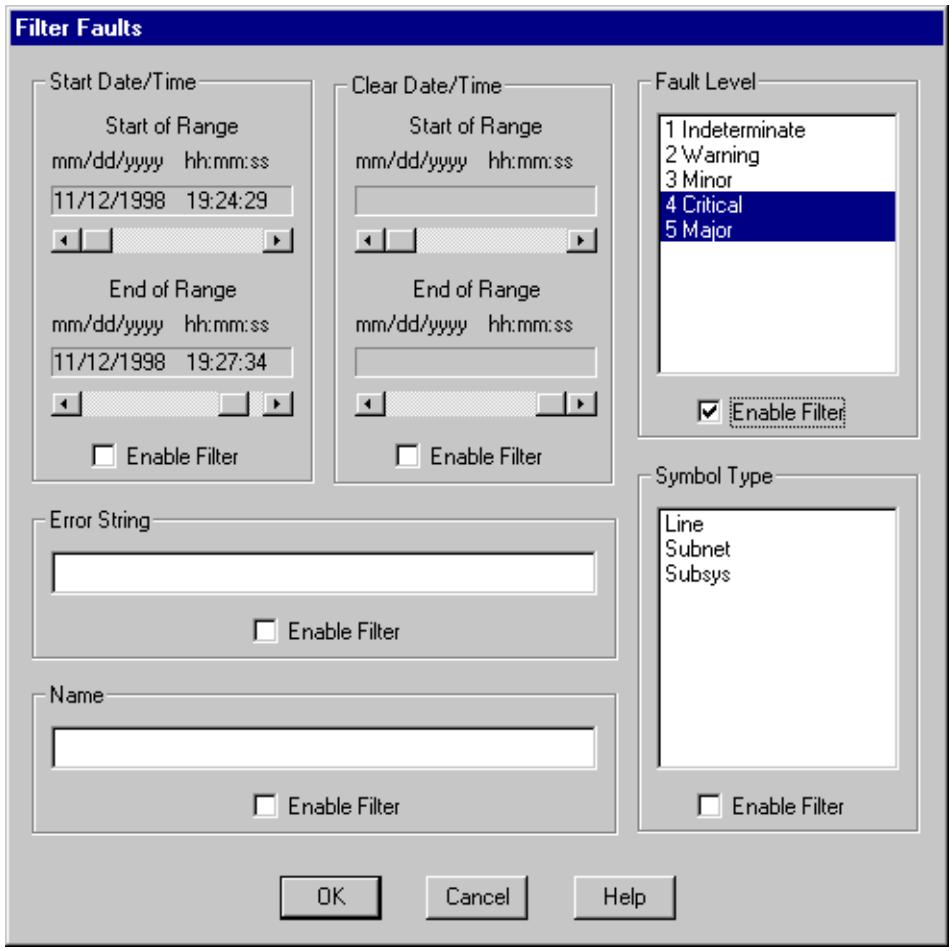


Figure 341. Faults Display Filtering

Here we set up a filter for levels 4 and 5 only.

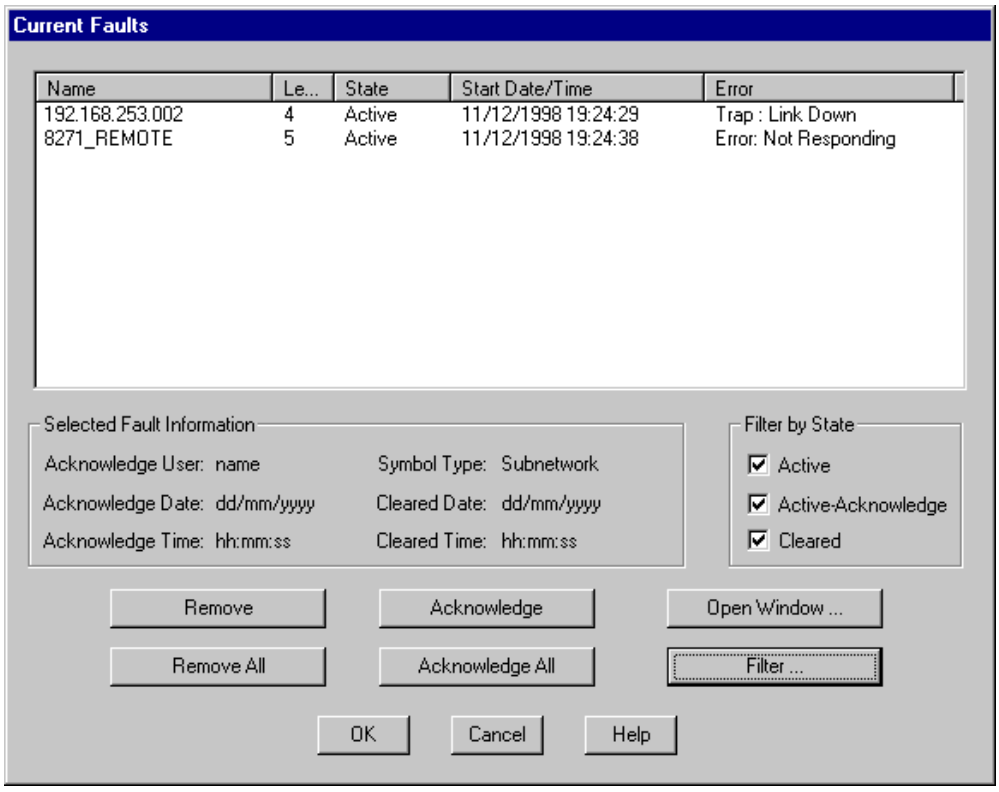


Figure 342. Current Faults Window with Only Fault Levels 4 and 5

We wanted to add the 8274 trap definition to the Nways for NT. This involved using the ASN format MIB file called xylan-9slot-trap.mib, which contains the trap definitions.

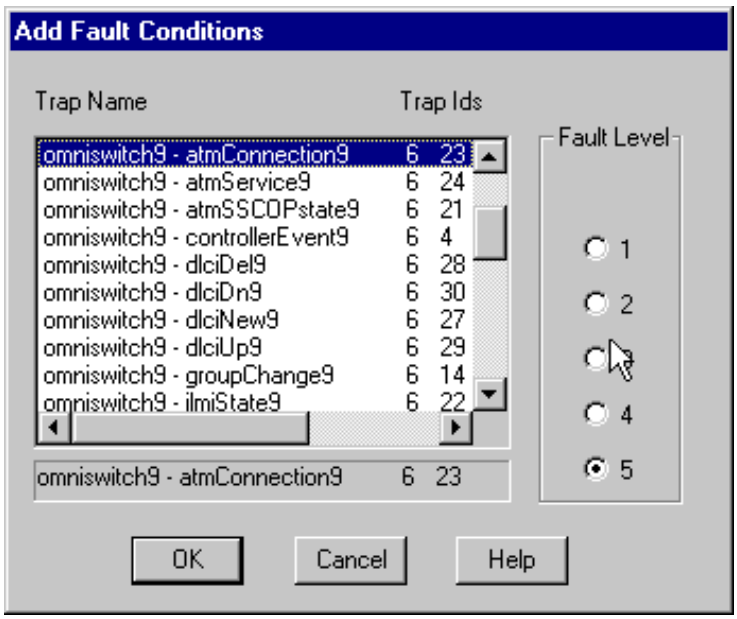


Figure 343. 8274 Trap Definitions

These traps are handled the same way as the previous example by defining a level 5.

9.9 Performance Management

This section takes a brief look at performance monitoring from the Workgroup Manager. JPM is the main performance tool with the complimentary Remote Monitor tool for monitoring RMON standards compliant agents for LAN performance.

To start performance select **Performance** followed by **Alarm Parameters** (see Figure 344 on page 348).

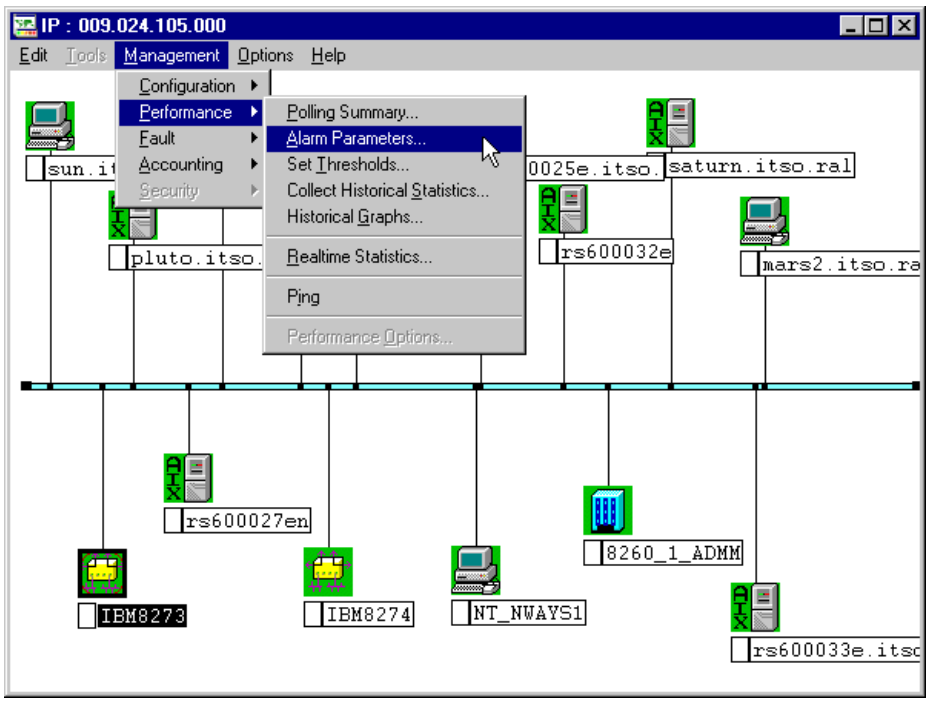


Figure 344. Performance Option on Menu Bar

Some performance can be performed through the MIB browser. If we browse the MIB for the 2210 (see Figure 345 on page 349).

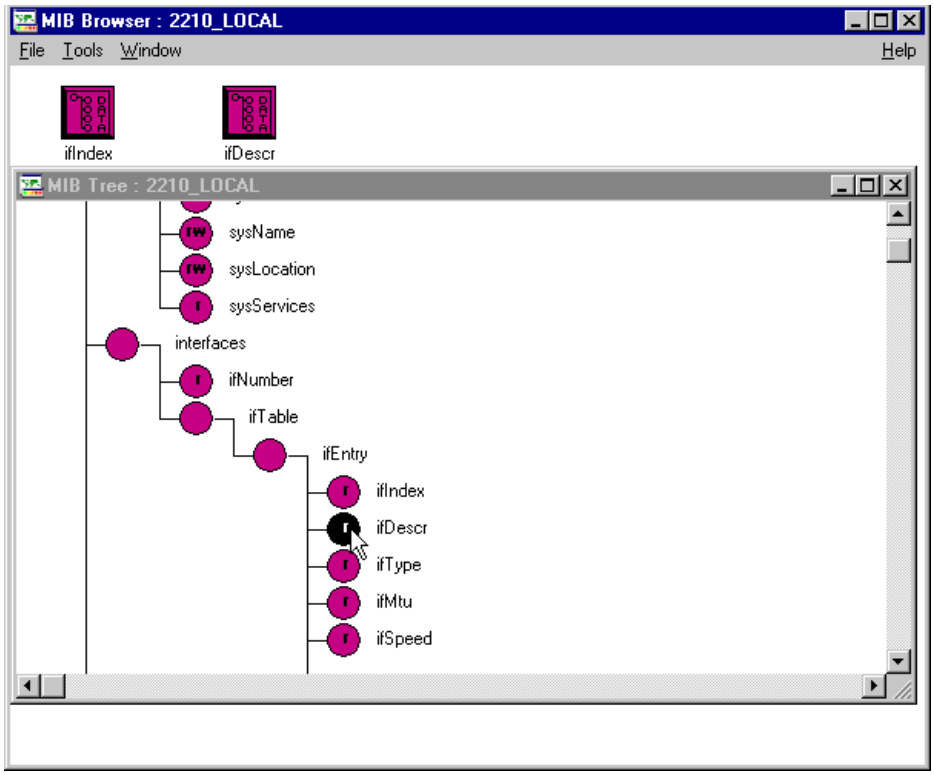


Figure 345. MIB Browser Window for 2210_LOCAL

Select **Graph** as shown in Figure 346 on page 349.

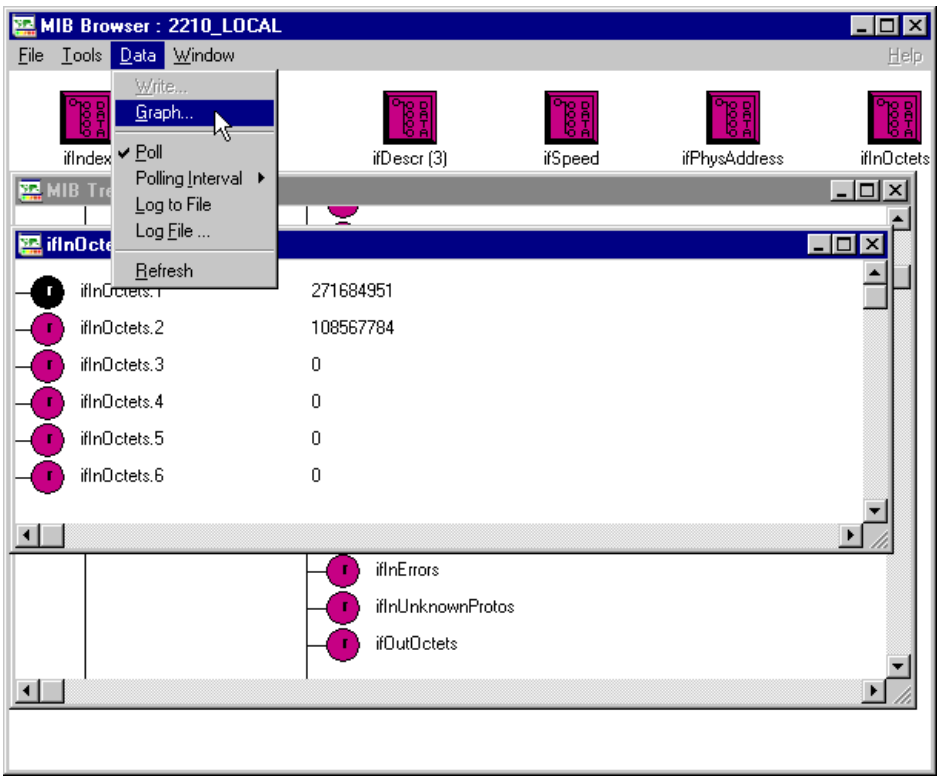


Figure 346. Starting Graph for a MIB Variable

We starting graphing for interface input packets(Figure 347 on page 350).

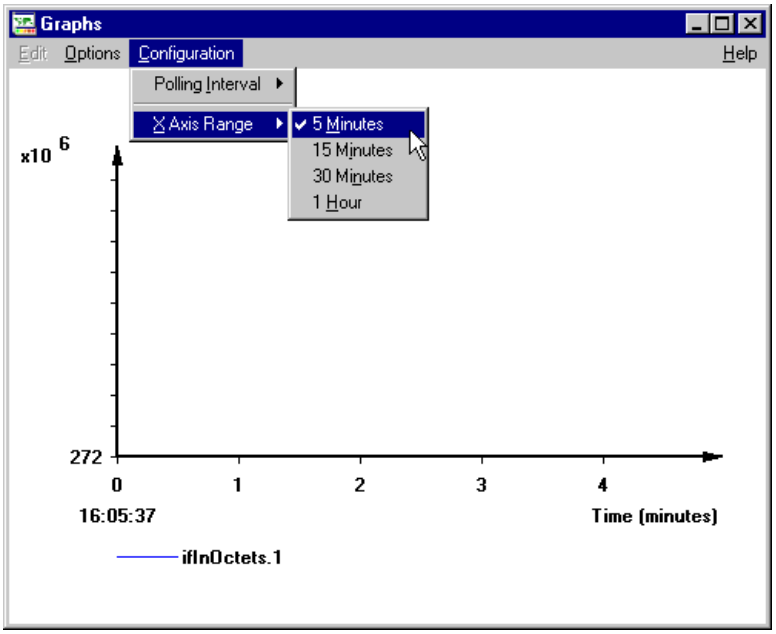


Figure 347. Setting Graph Range

Select **X Axis Range** to define the range and polling interval.

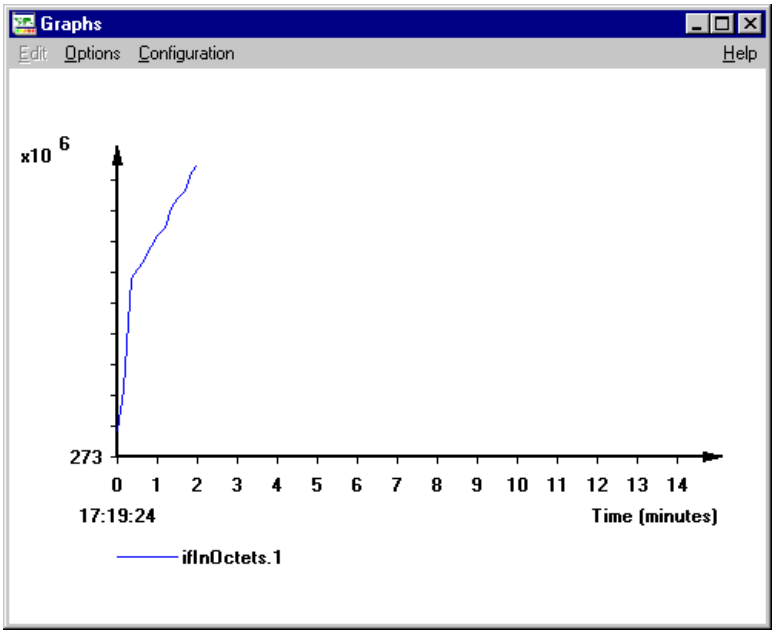


Figure 348. Graphs Plotted for ifInOctets.1 (Interface Input Packet)

This data is a real-time graph and it's accumulated and not rated (per second).

9.9.1 Using Java Performance Management (JPM)

As mentioned earlier the performance is done through the JPM. Refer to "Examples Using the Java Management Applications" on page 237 for additional examples.

Figure 349 on page 351 shows the options for the JPM.

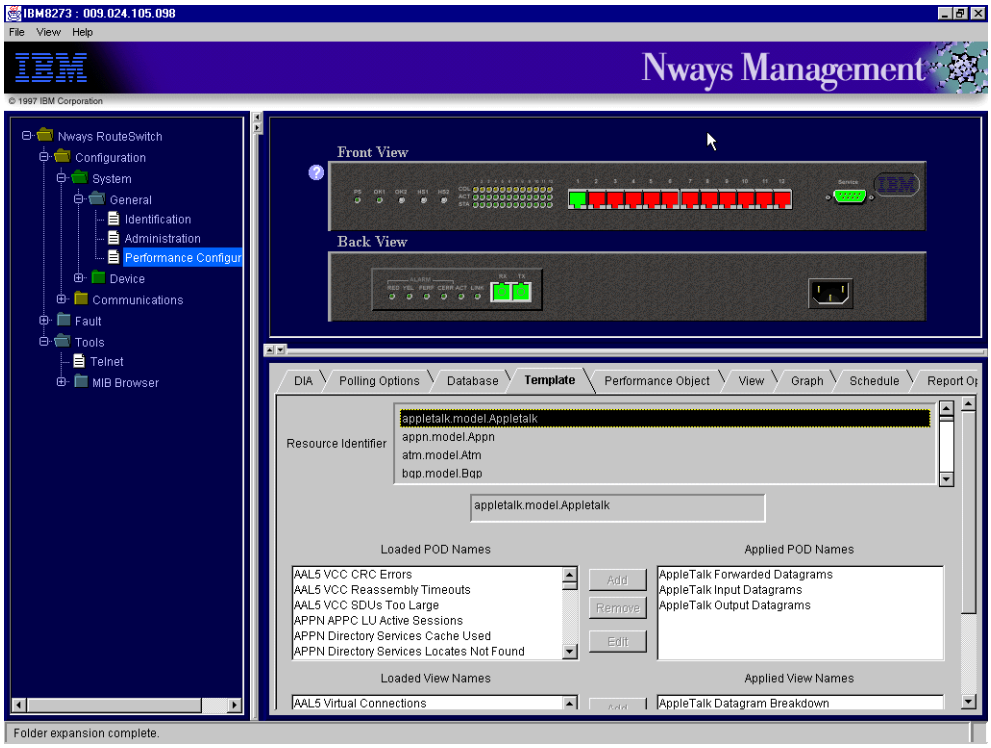


Figure 349. Configuring Performance from JMA

Chapter 10. Nways Manager Application Information

This chapter contains information based on the problems and issues we faced during the project. Also we discuss the application daemons and what each of these daemons do. The following sections are discussed:

- Database Cleanup Procedures
- Problems During Installation
- General Tuning Tips
- Daemons and Executables

Below are some good reference Web sites:

- www.raleigh.ibm.com/support
- www.networking.ibm.com/support/techtips.nsf/maix12tips
- www.networking.ibm.com/support/techtips.nsf/maix12tips?openview

10.1 Database Cleanup Procedures

Many of the Nways databases refer to the NetView databases, we had to clear down the databases a number of times. The following procedures guide you to clean up the databases using smit nv6000:

- NetView Topology and Object Databases
  - Select **Maintain->Clear Databases->Clear Topology**
- NetView Map databases
  - Select **Control -> Restart automatic map generation.**

The Nways manager smit options are accessed via smit cml.

- LNM databases
  - Select **Maintain -> LAN maintenance -> Clear IBM LAN databases.**
- Hubs topology
  - Select **Maintain -> Hub Manager capability maintenance -> Clear the IBM Hubs Topology.**
- ATM topology
  - Select **Maintain -> Campus Manager - ATM maintenance -> Clear the Campus Manager - ATM Topology.**

The smit options for the MAT are accesses using the command smit mgtapptran:

- Stop the daemons by selecting **Control -> Stop daemons.**
- Clear the database by selecting **Maintain -> Clear databases.**

10.2 Problems during Installation

Some issues when installing the applications.

1. Java Run-Time Environment

   The new Java installation program provided for V1.2 will fail if the required level of the Java Run-Time Environment is not installed. To determine if the prerequisites are met use the following commands:

```
java -fullversion
```

This command should return JDK 1.1.2 ... 19970920 or higher. Follow this with the command:

```
lslpp -l Java
```

The reply from the lslpp command should give the following information:

```
Java.rte.bin v1.1.2.0
Java.rte.classes V1.1.2.0
Java.rte.lib V1.1.2.0
```

2. Java install never completes

   Another symptom of having the wrong level of the Java Run-Time environment installed is having the Java install never complete. A symptom of this condition is the Java process pegging the machine consistently at over 90%. We found that JREs containing java.rte.bin files at earlier than V1.1.2 caused this problem.

3. Install error missing bos.install file

   The Nways install process checks for the required AIX bos.install files for both supported AIX versions (V4.1.5 and V4.2.1). If you are running on AIX V4.1.5 you will get erroneous messages saying you are missing prerequisites:

   ```
   bos.install.4.2.1.0.bff
   bos.install.4.2.1.3.bff
   ```

   These messages can be ignored.

4. Install failure due to small /tmp

   A database reorganization is run after every PSM is installed. A temporary file is created by this. Once the MAT is started, these files are removed. Until then the temporary files exist in /tmp. If /tmp is too small, the install will fail.

5. ATM customization changed

   All Nways databases are migrated during V1.2 installation except for:

   - AHMostopo.db
   - ATM and Hub polling parameters.

6. Success of installation

   The installation process puts entries in the following locations:

   ```
   /usr/CML/install_log/smit.log
   /usr/CML/install_log/xxx.log
   ```

   where xxx is the fileset being installed (such as ahm6000.base.log).

7. Core dump by cmld

   The Nways Manager for AIX V1.2 had a bug in the cmld that caused a core dump at initial startup after installation. This occurs when the installation included all of the components (not a selective install). A fix is now available for this problem.

8. Installation of NCM ATM

   The Nways Campus Manager V3.3 (contained in the Nways Manager for AIX V1.2 package) no longer contains the processes for managing ATM devices (no PSMs or MAT). These functions were moved to the NCM LAN V3.3 component. This causes problems if the ATM application is installed over the

Nways Manager for AIX V1.1 code *without* installing the new NCM LAN package (from Nways Manager V1.2).

If the NCM ATM V3.3 is installed without replacing MAT and the ATM device PSMs, the ovwdb will be corrupted. This will require removing *all* of the databases (including IP) before NCM can be installed successfully (NCM LAN or NCM ATM).

9. ReMon summary view not staying up

   The installation instructions for Nways Remote Monitor require that you have to set the **RMONHOME** environment variable to point to the directory where it has been installed. Failure to do this will have the symptom of the ReMon Summary Viewpoint screen disappearing from view once displayed.

10.2.1 Operational Problems

Some operational problems we encountered are as follows:

1. Core dump by oscmgr

   A core dump by the oscmgr daemon is caused when the cache size has been set too low.

2. Netscape core dump

   The JMA help information is stored as HTML Web pages. When you ask for help from a JMA window, a web browser is launched to display the appropriate HTML help pages. If you configured Netscape V3.01 as your preferred Web browser, you may experience a core dump. Netscape does not support internationalization, so if you have set the LANG environment variable to a value other than C it will have a core dump. This is set using the command:

   ```
   export LANG=C
   ```

3. ovaddobj Failures

   During the installation process of Nways, and during some cleanup procedures, the command ovaddobj is executed. If there is a problem with NetView configuration or DNS name resolution, this command can fail, causing various symptoms including failures in IP discovery.

   Note: If problems exist with NetView configuration the `/usr/OS/service/reset_ci` command is recommended to resolve/cleanup configuration problems:

   However, assuming NetView is properly configured, one of the causes of ovaddob failures is the use of the netsvc.conf set to direct NetView to a host name file rather than DNS as primary name resolution. If the host names file contains the short name format, for example node005 rather than the full name used by DNS (that is, node005.raleigh.ibm.com), name resolution during IP discovery can fail.

   One way to avoid conflicts, if you need to use a local host names file, is to define the resolution configuration within netsvc.conf to the following:

   ```
   hosts = local, bind
   ```

   This will cause the local host name to be used first, and if resolution fails, the DNS will be used.

4. Java applet unable to connect to server

One installation error that can be easily circumvented is when the Nways Java Integrator registration fails during the install. This will show up as an error in nwaysmanager.jma.log. The operational symptom is that when you start up a Java Device Management application an error window pops up saying that the application was unable to connect to the server.

To fix this problem issue the following commands:

```
ovaddobj NwaysJMA.lrf
ovstart JMAintegrator
```

5. Launch of Config Tool Fails

   Problems with your PATH variable can cause a failure to launch the device configuration tools for the 2210, 2216 and MSS from the JMA. The solution is to edit your /etc/environment file and add a dot to your PATH statement.

6. System hangs

   There are situations where Nways applications seem to be using AIX resources (memory buffers) in such a way that the effect is memory leaks that eventually (over a period of days) can cause the operating system to come to complete halt (hang). We have identified an AIX PTF that is being packaged that has fixes in this area. Testing is not far enough along to specify how to identify the PTF but you should call AIX support and ask for the very latest PTF for their appropriate AIX level of the following components:

   - bos.net.tcp.client
   - bos.net.tcp.server
   - bos.net.nfs.client
   - bos.net.nfs.server

7. Operational error logs

   ObjectStore will log exceptions by application in one of the following:

   ```
   /etc/environment/OS_ROOTDIR
   /usr/CML/conf/OSserver.conf/OS_AS_START
   /usr/CML/conf/OSserver.conf/OS_CACHE_DIR
   /usr/CML/conf/OSserver.conf/OS_COMSEG_DIR
   /usr/CML/conf/OSserver.conf/OS_CACHE_SIZE
   ```

   Other log files key to problem resolution are:

   ```
   nv6000.log
   /usr/OV/log/nettl.LOG00
   /usr/CML/install_log
   /usr/CML/deinstall_log
   /tmp/oss_out
   /tmp/rabmEventServer.log
   ```

8. File system filling up

   One problem reported is /usr file system space filling up due to a large number of mgtapptran log files. The MAT should be removing all of these log files when started with NetView for AIX, but this is not always happening. The solution was to manually remove the files as following:

   - Exit the NetView end-user interface.
   - Stop MAT by running smit and selecting **Communications Applications -> Application Transporter -> Control -> Stop Daemons.**
   - From the command line, enter `rm /usr/lpp/mgtapptran/db/logfiles/*.log`.

- Re-start the NetView GUI which will restart the MAT.

9. MAT startup failure

   When NetView is started, you may see the following messages:

```
Application Transporter Request Broker V.3 R.0 Port No xxxx
Application Transporter System Startup: ..
Starting application: RnvgateAlert Manager: Unknown failure
ovhelp: Cannot initilize OVw API: Cannot connect to database
Starting application: Rnvch
Starting application: Rwatchovhelp: Cannot initialize OVw API: Cannot connect
to database
Warning: XrRemoveInput: Input handler not found
Application Transporter System shutdown: ..
Shutting down application: RnvgateWarning: XtRemoveInput: Input handler not
found ...
Rnvgate: shutdown
Shutting down application: Rnvch
Rnvch: shutdown
Shutting down application: rb ..
```

   These messages indicate that NetView is not far enough along in its startup for MAT to connect to it. The result is that MAT shuts down. However, the first MAT action that you take through the NetView pull-down menus, will restart the MAT. These messages may appear on slow or overloaded AIX machines.

10. Purple icons in the hub topology

    The Nways Manager colors device icons with a unique color when the device is pingable but has no reporting via SNMP agent. This condition used to show up as blue. When this occurs, first check the community name set up for the device.

11. MAT continuous re-synchronization

    The Application Transporter will automatically attempt to re-synchronize the Nways Device Management submap every time the NetView GUI is restarted.

    To stop this synchronization:

```
cd /usr/lpp/mgtapptran/bin
vi ed.conf
```

    Add the string -NO_SYNC_AT_START to the line that starts with Rvngate (resulting in a line reading Rvngate -NO_SYNC_AT_START).

    If you wish to resynchronize the MAT database at any time, using smit, select **NetView -> Tools -> Application Transporter -> Refresh Device Management submap**.

12. LNM discovery

    There are times when the LNM discovery under NCM LAN does not seem to be finding the agents you would expect. Part of this is due to polling cycles and part is due to slow SNMP GET responses. One way to force all of the LNM discovery daemons to recheck the status of their reporting agents is to do a cmlstop.

13. Multiple LNM views for same segment

    LNM can show multiple segment views for the same segment. There are a number of possibilities that can cause this. LNM will merge views if more than

50% of the adapters reported through a TR surrogate agent match more than 50% of the list reported by another agent.

- RMON non-canonical MAC reporting. Some RMON agents report their NAUN order in canonical order. You can use NCM configuration of surrogate agents (specifically RMON agents) and specify which form you want the MAC addresses displayed in by LNM. This is done by a specific IP address so you should first see which form the RMON agent is reporting in. Once you change the MAC address format, this should cause better merging. An example of this is 8230 SNMP models that report their adapter list through SNMP in non-canonical and their MAC list through RMON in canonical format.
- There are still potential merging problems in LNM caused by bugs in priority merging of reports from different surrogate agents on the same segment. One way to avoid this is to use a new capability and configure a TR surrogate agent and specify Manage Agent = NO for the specific node offering the agent. This option has been added for RMON agents as well as TR surrogate agents and will allow the device to be managed by other NCM LAN applications but the SNMP reporting agent that is normally used for segment views will not be managed by LNM.

14. Device icons not appearing as executable

    There are several situations that can cause Nways device management applications from correctly associating the appropriate application to a device icon and marking it as executable. One is a timing problem when Nways attempts to get the MIB variable that is needed to define the association. There are two paths for correcting this symptom once it has occurred.

    1. If the device is managed with a PSM, you will need to make the icon executable using the **Application Transporter** pull-down menu option.
       - Add public as a read/write community name to the device.
       - Associate the device with the PSM,
       - Open the subsystem, and from the PSM view, select **Edit -> Modify**... from the menu bar and change the **General Parameters** screen to the correct community name.
    2. If the device element management application is either the Hub Manager or the Nways Java Management Application, you must use NetView to make the symbol executable.
       - Select the icon with the left mouse button.
       - With the right mouse button select the **Edit -> Modify/Describe -> Symbol**.
       - Mark the Behavior as **Execute**.
       - If the device is an 8250, 8260 or 8265, set the Application Actions as **IBM Hub Manager: explodeHubView**
       - If the device is a 2210, 2216, 8210, 8273, 8229, 6611 or one of the newer models of the 8271, set the Application Actions as **IBM Nways Java Management: openJavaDeviceView**.
       - Select and add the target object of the device you wish to make executable.

15. TCP socket is already in use

After the installation of Nways Manager for AIX with the MLM application, failure to configure the specific readWrite access authority for the NetView network management station can cause the failure of the TCP socket to become active. The fallowing actions should be taken:

- Stop NetView and Nways Manager daemons by entering:

  ```
  /usr/CML/bin/cmlovstop
  ```

- Edit the /etc/snmpd.conf file and add the following line:

  ```
  community private your_IP_address 255.255.255.255 readWrite
  ```

  where your_IP_address is the IP address or hostname of this network manager station.

- Refresh the snmpd daemon by entering:

  ```
  refresh -s snmpd
  ```

- Start the snmpd configuration utility by entering:

  ```
  smconfig
  ```

  - Change the community name for your_IP_address to private.
  - Choose MLM Trap Reception Setting window.
  - Select **Modify** button.
  - Change TCP Trap Reception and UDP Trap Reception to disabled.
  - Select **Apply.**

- Restart NetView.

16. Timeout problems configuring ELAN

    When changing an ELAN configuration (with MSS as the LECS) it is recommended to increase the time out value when creating new ELANs. The default is picked up from the NetView SNMP configuration. The recommended value seems to be around 300 seconds if the MSS is local. A setting of 120 seconds gets time out errors when issuing configuration changes as does a setting of 600 seconds.

17. Error Bad SNMP Value when configuring the MSS

    A problem occurs when moving an ATM LEC from one ELAN to another when the LECS is set up in the MSS. An error message can pop-up saying Bad SNMP Value which is caused by MSS rejecting an SNMP set due to problems with community name access.

18. Incorrect ATM topology

    Another symptom of incorrect SNMP access to ATM devices is an invalid ATM topology view. If devices show up in the default ATM PNNI group, this can indicate read only access to the MIB on the ATM node. Make sure all CPSWs and MSS servers are supported in the NetView SNMP configuration with correct read/ write access.

10.2.2 Problems with Remote DIA

The following tips cover common Java error messages that may occur and actions to take to correct the cause of the condition.

1. java.net.UnknownHostException

This message usually indicates that the HTTP server cannot be contacted. Verify that the hostname is correct and that the server is online.

2. java.net.ConnectException

   This message usually indicates that the HTTP server can be contacted, but the service is unavailable. Verify that an HTTP server is running on the HTTP server host.

3. java.io.FileNotFoundException

   This message usually indicates that the URL given in the script file is not recognized by the HTTP server. Verify that the URL given is consistent with the name assigned to the Nways Manager Web pages on the HTTP server.

4. java.rmi.ConnectException

   Also shown as "lookup of server failed". This message usually indicates that the Nways Manager host specified is not operating. Make sure that the station is operational and that the Nways Manager programs are operating. The runDIA script will not exit when this message occurs, but will instead keep retrying until the Nways Manager session responds.

10.3 General Tuning Tips

The performance of your network management station is dependent upon a number of factors, including the hardware, operating system (AIX), NetView, and the various Nways components. Below we have outlined several items that can be checked if you are facing performance problems, or trying to do some general tuning:

- **Memory** - NetView, Nways Campus Manager, and other network management programs that run on the network management station have high memory requirements. Depending on the number of objects and number of users accessing concurrently, the memory requirement will increase.
- **Paging Space -** The paging space should be two and a half times your memory for less than 256MB RAM hardware configurations. For physical memory (RAM) and more than 256 MB, the paging should be at least twice this amount. You can check the paging space on your system using the lsps -a command.
- **Name Resolution** - NetView is heavily dependent upon name resolution. If host names are not resolved quickly, the entire system may start to slow down. Check name resolution in both directions:
  - Host to IP address using the host <hostname> command
  - IP address to Host name using the host <ip address> command

  The ideal response should be instantaneous. Also check for hostnames and IP addresses that don’t resolve. If a response is consistently slow, you may considering using a different name server, or even a local /etc/hosts file to maintaining the host name to IP address mapping.
- **Journal Filesystem Cache** - Each Nways process uses a certain amount of cache which is allocated under the /usr/CML/OStore/cache filesystem. If enough space is not allocated, a core dump of the oscmgr process can occur.

  A general formula for determining the minimum cache size you should set is:

  ```
  1-time daemons cache + (EUI daemons * number of operations)
  ```

where 1-time daemons are those started by ovspmd**.** Here 1-time means that there is a single instance of this daemon, whereas the EUI daemons (iubsearchx, ahmeui, ahmledisplay) will have an instance for each NetView EUI that is started. The number of operators means the number of instances of NetView EUI that are running.

The 1-time daemons are those started by ovspmd include:

- ahmdbserver (ATM) = 2.5 Mbytes
- iubd (8250/8260/8265) = 2.5 Mbytes
- ahmtopod (ATM) = 2.5 Mbytes
- lnmbrmon (LAN bridge discovery) = 1.5 Mbytes

EUI daemons include:

- iubsearchx (BASE) = 2.5 Mbytes
- ahmeui (ATM) = 1.5 Mbytes
- ahmledisplay (ATM) = 1.5 Mbytes

You can check and change the journal filesystem space from smit by selections**, System Storage Management(Physical and Logical Storage) --> File Systems -->Add/Change/Show/Delete File Systems --> Journaled File Systems ->Change/Show Characteristics of a Journaled File System**

Select from the list **/usr/CML/OStore/cache**

- **ovwdb Cache -** NetView caches topology objects in memory. You can check the number of objects in your database by entering the command `/usr/OV/bin/ovobjprint -S`. If the ovwdb cache size is not greater than the number of objects, performance of the system is degraded. The default cache size is for 5000 objects.

  One of the major users of ovwdb in Nways is the LAN Network Manager component of NCM LAN. The following provides some guidelines on how many objects are added based on the LNM's managed environment:

  - Each bridge interface = 4 objects
  - Each token-ring workstation = 3 objects
  - Each FDDI workstation = 9 objects
  - Each FDDI concentrator = 10 objects
  - Each 8230 CMOL LAM = 21 objects (via LNM for OS/2)

  You can check and change the cache size by running by running smit nv6000 and selecting **Configure -->Set options for daemons -->Set options for topology, discovery, and database daemons -->Set options for ovwdb daemons.**

  and change the parameter: Number of objects to hold in cache.

- **Filesystems -** Filesystems that are full can degrade performance. Filesystem space is important with NetView. You must maintain at least 20MB of free space in /usr, with the percentage value lower than 96% free. The /root , /var and /tmp directories should maintain alteast 5 megabytes for free space.

  The root filesystem often gets full because the root user is used to start NetView, and the SMIT and nv6000 logs are written to the user's home directory. This can be avoided by keeping the logs cleared regularly, or by changing the root's home directory.

- **NetView Status Polling** - NetView determines the status of the interfaces (IP hosts) on the IP network by polling (pinging) them. By default, each IP host or interface is pinged once every five minutes.

  Status polling can be often customized to ping certain critical resources more frequently, such as routers, hubs and servers, than other less critical resources such as workstations. In large networks, or ones with a short polling interval, there may not be enough time to poll all interfaces in an interval.

  Also over slow WAN links, polling all devices on the other side of a WAN can put extra burden on the link, and slow down other communications. One more thing to note is that because of the increased latency over a normal low-speed WAN link (compared to that of LAN), SNMP timeouts may occur. To overcome this, you may need to increase the SNMP polling timeouts for remote nodes.

  You can change polling intervals for a specific node, a group of nodes using a wildcard, and at the same time have a default polling interval. This is very beneficial as mentioned earlier, where critical nodes may need to polled more often than less-critical nodes.

  You can view and change the polling intervals from the NetView menu bar by selecting **Options--> SNMP Configuration**.

- **Large Object Database** - NetView users will often discover many more objects than they wish to monitor. This is because autodiscovery is turned on and by default, NetView will discover and poll every IP host, which in most cases is not desirable. If the Netview object database is large and contains a lot of workstations that don't require monitoring, you may consider using a seed file for NetView discovery to limit discovery to those network devices and servers that are critical to the network operations. In our labs, we used a seed file to manage only the network devices that were part of our test environment.

- **Incorrectly parented processes** - These processes can tie up resources and temporarily cause performance problems. These are usually a result of EUIs being terminated abnormally, and some processes not shutting down correctly and become parented by init. The most common orphans are iubmap, iubeui, ahmledisplay, and ahmeui. If the parent is init (with a ppid = 1), the are orphans and should be stopped using the kill command.

10.4 Daemons and Executables

This section contains information on the Nways and NetView daemons.

10.4.1 NetView Daemons

The NetView daemons are discussed below:

- **ovspmd -** The ovspmd daemon manages the daemon processes that are part of the Tivoli NetView program, starting, stopping, and reporting status on them in response to requests from the user interface programs (ovstart, ovstop and ovstatus). The ovspmd daemon is normally automatically started by ovstart.

- **netmon -** The netmon daemon attempts to discover nodes on the network. After it has discovered a node, it polls the node regularly to check for status, topology, configuration, and threshold changes.

  In usr/OV/log director there is a file called netmon.trace that will provide you with certain network information. A netmon trace can be started from the

netmon command or via SMIT. From the command line you can select multiple output types or add the individual tracemask values together and enter that number. Examples:

```
netmon -M 16 Trace traps generated
netmon -M 32 Trace traps received
netmon -M 0 Turn off tracing
```

NetView dynamically discover nodes within one hop count, which is the default setting. However, you can increase your range or limit your discover range by creating a seedfile what contains a list of nodes within your administrative domain. Once the discovered nodes have been placed on the map, you can disable automatic layout, which is a feature that prevents new nodes from displaying the map. The nodes will appear in the object holding area and can manually be added to the map.

- **ovwdb -** The ovwdb command starts a background process that maintains the graphical user interface object database used by the NetView application. The -n flag with ovwdb controls the number of objects maintained in the cache. The cache value should be at least 20% larger than the amount of objects that can be determined with the ovmapcount command.

10.4.2 The Nways Daemons

The Nways daemons are listed below:

- **nvot_server -** The nvot_server daemon maintains the LAN topology database.
- **cmld -** The cmld daemon is common to both the NCM LAN and NCM ATM. In NCM LAN the cmld daemon makes the link between the LAN and NetView for AIX background daemons. This daemons also manages lnmtopod and the monitoring applications that are part of LAN Network Manager and provides a communications channel for the LAN Network Manager command line interface. The daemons controlled by cmld are as follows:
  - cmldiscd - The cmldiscd process is common to NCM LAN and NCM ATM, and is the basic topology discovery mechanism. It provides the daemons with the LAN resources discovered by NetView for AIX.
  - iubd - The iubd daemon is the hub topology discovery and maintenance daemon.
  - ahmtopod - is the Nways ATM and LAN Emulation topology discovery and maintenance daemon.
  - lnmtopod - LNM topology services application that builds LAN network topology working with the other lnm daemons, and with the NetView daemon nvot_server.
  - lnmhubint - integrates the hub manager and lnm topology views, working with iubd.
  - lnmtrmon - LNM SNMP token-ring monitor process.
  - lnmbrmon - LNM SNMP bridge monitor application.
  - lnmfddimon - LNM FDDI SNMP Proxy Agent monitor process.
  - lnmlnmemon - LNM OS/2 agent monitor process.
  - jdmd - The monitor process for the java device management.

- **iubmap** - The iubmap process reads/writes the OVw database to manage the symbols and Nways maps.
- **cmlsm** - The cmlsm process is common to both Nways ATM and LAN and is the daemon that runs the symbols manager. Cmlsm makes the link between the NetView for AIX user interface and the iubeui process. Symbols Manager manages the executable symbols and the bitmap display of icons in the IBM Hubs Topology. Cmlsm is automatically started and stopped when NetView for AIX starts and stops.
- **iubovwint** - Provides the interface between the OVw database and ipcservices.
- **ipcservices -** Responsible for inter-EUIs communication (mainly navigation).
- **nwsstatif/iubstat** - The nwsstatif and iubstat processes are common to NCM LAN and NCM ATM. They control the user interface of the statistics application that provides graphical information on all counters and values of resources managed by Nways.
- **iubeui** - Process is the process for displaying the NCM LAN interface. iubeui is started when you double-click on a hub (8250, 8260) icon in the IBM Hubs Topology. Iubeui is automatically stopped when NetView for AIX is stopped.
- **iubsearchx** - Process is common to the NCM LAN and NCM ATM and is the process that provides the user interface with a repository of stations and devices.
- **java** - The java process manages all the Java panels.
- **ahmeui** - Controls the ATM user interface panels.
- **ahmledisplay** - Controls the LAN Emulation Manager topology and end-user interface panels.
- **lnmbrmgr** - Manages the LNM SNMP bridge application.
- **lnmtrmgr** - Manages the LNM SNMP token-ring application.
- **lnmlnmemgr** - Manages the LNM LLC token-ring application.
- **lnmfddimgr** - Manages the LNM FDDI application.
- **lnmexport** - Converts current week performance data collected by the OS/2 agent to a spreadsheet-readable delimited format.
- **cml_agent_found** - initiates the discovery of a specified agent.
- **cml_agent_remove** - stops monitoring of an agent.
- **alertman** - RABM Alert Managers, displays alerts/alarms packaged in SNMP.
- **appntopo** - APPN topology application.
- **dlswmap** - DLSw topology application.
- **Red** - Is the Management Application Transporter event dispatcher.
  - **Rwatch** - Monitors CPU and disk space
  - **Rmibs2** - Generic MIB II PSM.
  - **Rnvch** - NetView SNMP communication handler.
  - **Rnvgate** - NetView to Management Application Transporter gateway interface.
  - **Rpimserv** - PIM server, runs all PIMs.
  - **Rsph** - SNMP poller.
  - **R <device> s10** (specific device PSMs)

10.4.2.1 Nways ReMon Daemons

The following daemons make up Nways Remote Monitor application:

- **viewman** - The main IBM LAN ReMon application which provides the summary screen. This process kicks off other child processes; which are listed in the Child.Ctl file.
- **startup** - Application that displays the AXON logo panel. It is started by the RUN_ME script when ReMon is invoked, delays until the summary screen is displayed and then completes execution.
- **rmonman** - Executable is invoked by viewman and provides configuration dialogs when the following list of buttons are selected from the bottom of the summary screen: Statistics, History, Host Table, Alarms, Matrix, and Ring Station. When run stand alone this will provide a small tool bar with these options.
- **rmonview** - Invoked by viewman and provides the various views that have been requested from the rmonman configuration dialogs.
- **rmonstart** - Provides the integration with NetView and sends messages to the other ReMon executables.
- **capt** - Invoked by viewman and is displayed when the Capture button is selected. This provides a graphical display to set up capture buffers on supported RMON agents.
- **pdisp** - Invoked by viewman and provides the packet display for capt .
- **proto** - Invoked from the Protocol Distribution icon available from the summary screen when ecam is downloaded. It provides either a graphical or tabular display of the protocol distribution seen by the RMON agent.
- **ecam** - Provides the configuration dialogs for selecting ecam views. If run stand alone a small toolbar is displayed.
- **ecamview** - provides the graphical views that have been selected from the ecam configuration dialogs.
- **dlmstart** - Used to pass messages from the summary screen ecam icon to the ecam application. It can be used to request certain ecam configuration dialogs with a certain RMON agent already selected for example.
- **tgen** - Is the Traffic Transmission application. This is a stand-alone application which may be launched from the summary screen icon.

10.4.3 Daemon Relationships

The NetView and Nways processes operate in two general categories: background and foreground. The background daemons run all of the time, and are controlled by /usr/OV/bin/ovstart based upon entries in /usr/OV/conf/ovsuf. Foreground processes are associated with the EUIs brought up when nv6000 is executed and (or) when Nways icons are exploded.

Nways Campus Manager LAN and ATM are automatically started under the control of the NetView for AIX program. Daemons are started through the NV6000 shell script. The NV6000 shell script first executes the netnmrc shell script followed by the ovw command. The netnmrc shell script starts all the daemons registered in the ovsuf file. Each entry in the ovsuf is created from information in the local registration file (.lrf) in the /usr/OV/lrf/ directory. There is one .lrf file for each daemon. During installation, the cmld.lrf file is stored in the

/usr/OV/lrf directory. The ovsuf file is updated at the same time to reflect the startup behavior of the daemon. The lrf file is used to tell the ovstart command what process to start, what the dependencies are and what the arguments are.

The NetView for AIX startup file starts all daemons registered in the ovsuf file. Before you start NCM LAN or AIX, it is recommended that you check the status of the cmld daemon, and if necessary, start it. You do not have to be a root user to check the status of the cmld daemon, but you do have to be a root user to start it. To have the cmld daemon automatically start when you enter the ovstart command, add the daemon to the NetView for AIX ovsuf startup file.

10.5 Useful NetView Files

The following files are created/used by NetView for AIX but may have information useful to problem resolution with the Nways products.

- **snmpd.conf**

  The /etc/snmpd.conf file provides the configuration information for the snmpd agent. This configuration file contains entries for community names and access privileges and allows you to configure snmpd in debug for actions such as logging errors.

- **nettl.log**

  The /usr/OV/log/nettl.LOG00 file is used in debugging netview problem-related issues. This file contain errors with time stamps and can help you in determining which network application(s) may be causing problems. You can access the file by entering the following:

  ```
  netfmt -f -f /usr/OV/log/nettl.LOG00 > /u/home/errors
  ```

- **trapd.conf**

  The file /usr/OV/conf/C/trapd.conf contains definitions for the handling of SNMP traps, including how to format trap log entries and what action to take, if any, when a trap is received. The trapd daemon uses these formats to log a message in the trapd.log file.

- **trapd.log**

  The /usr/OV/log/trapd.log file receives both events and traps. Events are messages that are sent by applications such as netmon. Traps are unsolicited messages sent by SNMP agents to SNMP network management stations.

Appendix A. Nways Devices - Generated Events

This appendix contains a repository for all events that are generated by the Nways management applications.

A.1 Software Generated Events

In addition to the hardware events we can expect to see some events that are generated from the management applications. The ones we looked at are:

- NetView
- Campus Manager

The enterprise IDs are shown in the table below for events generated from the applications.

Table 20. Software Generated Events

ID	Enterprise ID
8260	**ibm8260_ATM {1.3.6.1.4.1.2.6.33.1}**
8260	ibm8260_ATM {1.3.6.1.4.1.2.6.33.2.1}
8260	ibm8260_ATM {1.3.6.1.4.1.2.6.33.2.3}
8260	hmp6000 {1.3.6.1.4.1.2.6.40}
PSM	MAT_1 {1.3.6.1.4.1.2.6.87
NetView	netView6000 {1.3.6.1.4.1.2.6.3}

The descriptions for these events are in the file trapd.conf.

A.2 Nways 2210 Multiprotocol Router

The 2210 uses the ELS to send events. The 2210 (as do other Nways devices) has a message subsystem called Event Logging System (ELS) that can be configured to allow event messages to be displayed at a local or remote console or telnet session, and/or be sent as an SNMP trap to an SNMP manager such as NetView.

The ibm2210.mib file defines two possible SNMP traps; ibmElsTrapV1 and ibmElsTrapV2**.** The 2210 only supports the ibmElsTrapV2 version. The descriptor field within the mib file gives the following information.

When the routing subsystem ELS component is configured to generate SNMP traps, a single trap is generated. It contains a single varBind containing a text string in one of the two following formats.

If ELS timestamping is enabled:hr:min:sec subsys_name.event_num: message_text will be For example - 09:32:56 IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc.

If ELS timestamping is disabled:subsys_name.event_num: message_text

For example - IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc.

A.3 Event Logging System (ELS) Messages

It is possible to enable ELS events by individual messages or by subsystem, for instance ATM, LEC and BBCM. The following table breaks down the message types by subsystem as defined in the *Event Logging System Messages Guide*, SC30-3682.

Table 21 on page 368 shows the subsystems for the 2210.

Table 21. ELS Subsystem

Msg Prefix	Subsystem
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LES (LES/BUS)	LAN Emulation Server and Broadcast Unknown Server
LLC	Logical Link Control
LNM	LAN Network Manager
LSA	Channel Network Interface (LSA)
MARS	Address Resolution Protocol
MCF	MAC Filtering
MLP	Multilink PPP
MPC	Channel Network Interface (MPC)
MSPF	Multicast Sessions to OSPF
NBS	NetBIOS Support System
NDR	Network Dispatcher Router
NHRP	Next Hop Routing Protocol
NOT	Component NOT Present Function
PM	Presence Manager
PPP	Point-to-Point Protocol Network Interface
RIP	Routing Information Protocol
R2MP	AppleTalk Phase 2 Routing Table Maintenance Protocol
SAAL	ATM Signalling ATM Adaption Layer
SCSP	SCSPTRP.MSG Messages
SDLC	SDLC
SEC	Security Protocol
SL	Serial Line Network Interface
SNMP	Simple Network Management Protocol
SPF	Open Shortest Path First (OSPF)
SRLY	SDLC Relay
SRT	Source Routing Transparent

Msg Prefix	Subsystem
TCP	Transmission Control Protocol (TCP)
SVC	ATM Signalling
STP	Spanning Tree Protocol
VN	Banyan Vines
UDP	User Datagram Protocol
TKR	Token-Ring Network Interface
TFTP	Trivial File Transfer Protocol
XN	Xerox Network Core
WRS	WAN Restoral System
V34	V.34 Dialing
V25B	V.25bis Dialing
VLAN	Virtual LAN
XTP	X.25 Transport over TCP/IP
X25	X.25 Network Interface
X251	X.25 Network Interface Physical Layer
X252	X.25 Network Interface Frame Layer
X253	X.25 Network Interface Packet Layer
ZIP2	AppleTalk Phase 2 Zone Information Protocol

At this point in time it has not been established whether the NetView ruleset utility can provide any correlation based on the text-based variable field that will be received as part of the SNMP trap message.

The source MIBs are listed in Table 22 on page 369.

Table 22. List of Source MIBs for Nways 2210 Multiprotocol Router

Trap No.	Trap Name	Description
ibm2210.mib (Enterprise 1.3.6.1.4.1.2.6.72 {ibm2210} - 1.3.6.1.4.1.1 - {proteon})		
1	ibmElsTrapV1	An ELS trap event. Note that this trap is being deprecated and will not be supported in all future releases. The objects proELSTrapVar1 through proElsTrapVar9 are conditionally included in this trap to carry variable data fields from the ELS message. These objects are not carried as object IDs as defined, but in fact are data objects. Their syntax will change depending on the data they carry for a particular trap instance.
2	ibmElsTrapV1	When the routing subsystem ELS component is configured to generate SNMP traps, the following trap is generated. It contains a single varBind containing a text string in one of the two following formats. If ELS timestamping is enabled: hr:min:sec subsys_name.event_num: message_text, for example - 09:32:56 IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc If ELS timestamping is disabled: subsys_name.event_num: message_text, for example - IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc.

Trap No.	Trap Name	Description
ibm2210-V1R2-PART2.mib		
		Same as ibm2210.mib.
rfc1215.mib		
0	cold start	Emitted when SNMP agent has completed initialization after a reload.
1	warm start	Emitted when SNMP agent has completed initialization after a restart.
2	link down	Emitted when a router/bridge interface has transitioned out of the up state. This may be the result of: - User initiated disable of the interface - Hardware failure - Maintenance traffic communications failure
3	link up	Emitted when a router/bridge interface has transitioned into the up state after passing self-test checks.
4	authentication failure.	Emitted when SNMP agent has received a packet that cannot be properly authenticated. This may be the result of: - Invalid community name string - Invalid origin IP address
rfc1315.mib (FrameRelay)		
1	frDLCIStatusChange	This trap indicates that the indicated virtual circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.
rfc1382.mib (X25)		
1	X25Restart	This trap means the X.25 PLE sent or received a restart packet. The restart that brings up the link should not send an x25Restart trap so the interface should send a linkUp trap. Sending this trap means the agent does not send a linkDown and linkUp trap.
2	X25Reset	If the PLE sends or receives a reset, the agent should send an x25Reset trap.
rfc1493.mib (dot1bridge) (Enterprise 1.3.6.1.2.1.17)		
1	newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.
2	topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.
rfc1657.mib (BGP)		
1	bgpEstablished	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.
2	bgpBackwardTransition	The BGPBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.
rfc1747.mib (SDLC)		
1	sdlcPortStatusChange	This trap indicates that the state of an SDLC port has transitioned to active or inactive.

Trap No.	Trap Name	Description
2	sdlcLSStatusChange	This trap indicates that the state of an SDLC link station has transitioned to contacted or discontacted.
rfc2024.mib (DLSW)		
1	dlswTrapTConnPartner Reject	This trap is sent each time a transport connection is rejected by a partner DLSw during Capabilities Exchanges. The emission of this trap is controlled by dlswTrapCntlTConnPartnerReject.
2	dlswTrapTConnProtViol ation	This trap is sent each time a protocol violation is detected for a transport connection. The emission of this trap is controlled by dlswTrapCntlTConnProtViolation.
3	dlswTrapTConnUp	This trap is sent each time a transport connection enters connected state. The emission of this trap is controlled by dlswTrapCntlTConn.
4	dlswTrapTConnDown	This trap is sent each time a transport connection enters disconnected state. The emission of this trap is controlled by dlswTrapCntlTConn.
5	dlswTrapCircuitUp	This trap is sent each time a circuit enters connected state. The emission of this trap is controlled by dlswTrapCntlCircuit.
6	dlswTrapCircuitDown	This trap is sent each time a circuit enters disconnected state. The emission of this trap is controlled by dlswTrapCntlCircuit.
rfc2320.mib (IPOA)		
1	ipoaMtuExceeded	A frame was received that exceeds the negotiated MTU size. The VPI and VCI of the VC for which this condition was detected can be determined from the index values for ipoaVcNegotiatedMtu. In addition, the ifIndex and IP address can be determined as well (refer to the ipoaVcTable).
2	ipoaDuplicateIpAddress	The ATMARP server has detected more than one ATM endpoint attempting to associate the same IP address with different ATM addresses.
3	ipoaLisCreate	Generation of this trap occurs when an ipoaLisEntry is created while the ipoaLisTrapEnable.0 object has the value enabled(1).
4	ipoaLisDelete	Generation of this trap occurs when an ipoaLisEntry is deleted while the ipoaLisTrapEnable.0 object has the value enabled(1).
ibmiroc.mib (IBMROutingCode)		
1	frrcvdFECN	This trap indicates that a frame was received from the network on this virtual circuit and it indicated forward congestion.
2	frrcvdBECN	This trap indicates that a frame was received from the network on this virtual circuit and it indicated backward congestion.
3	frrcvdCLLM	This trap indicates that a CLLM message was received from the network.
1	mosMemLow	This trap indicates that the free heap amount has dropped below a given percentage of the total heap memory available. The default percentage is 10%, however this threshold can be modified by the user via a patch variable.

Trap No.	Trap Name	Description
2	elsTrap	When the routing subsystem ELS component is configured to generate SNMP traps, the following trap is generated. It contains a single varBind containing a text string in one of the two following formats. If ELS timestamping is enabled: hr:min:sec subsys_name.event_num: message_text, for example, 09:32:56 IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc If ELS timestamping is disabled: subsys_name.event_num: message_text, for example - IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc. Note: The following subsystems cannot have their events sent in SNMP traps (ARP, ICMP, UDP, SNMP and IP (excluding IP access control events)). This restriction is due to the fact that these subsystems are involved in sending an SNMP trap and allowing them could cause an infinite loop in the router software.
ibmenet.min (IBMENETDispatcher)		
1	indHighAvailStatus	This trap announces that the value of the high availability status state (hasState) variable has changed. The possible values of hasState and their respective meanings are: -idle, - (0) This machine is routing packets and is not trying to establish contact with its partner Network Dispatcher -listen, - (1) High availability has just started and network dispatcher is listening for partner. -active, - (2) This machine is routing packets. -standby, - (3) This machine is monitoring the active machine. -preempt, - (4) Transitory state during switch from primary to backup. -elect, - (5) Network dispatcher is negotiating with partner for who will primary or backup. -no_exec, - (6) The executor is not running.
2	indSrvrGoneDown	This trap announces that the weight for the server specified by the csAddr, psNum, ssAddr portion of the object identifier has gone to zero, The last known number of active connections for the server is sent in the trap. This trap indicates that, as far as Network Dispatcher can determine, the specified server has gone down.
Novell IPX MIB		
		Mib not found.

A.4 Nways 2216 Multi-access Connector

The following are the traps for the 2216.

Table 23. List of Source MIBs for Nways 2216 Multi-access Connector

Trap No.	Trap Name	Description
rfc1215.mib		
0	cold start	Emitted when SNMP agent has completed initialization after a reload.
1	warm start	Emitted when SNMP agent has completed initialization after a restart.
2	link down	Emitted when a router/bridge interface has transitioned out of the up state. This may be the result of: - User initiated disable of the interface - Hardware failure - Maintenance traffic communications failure

Trap No.	Trap Name	Description
3	link up	Emitted when a router/bridge interface has transitioned into the up state after passing self-test checks.
4	authentication failure.	Emitted when SNMP agent has received a packet that cannot be properly authenticated. This may be the result of: - Invalid community name string - Invalid origin IP address
rfc1269-BGP.mib (BGP)		
1	bgpEstablished	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.
2	bgpBackwardTransition	The BGPBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.
rfc1315.mib (FrameRelay)		
1	frDLCIStatusChange	This trap indicates that the indicated virtual circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.
rfc1382.mib (X25)		
1	X25Restart	This trap means the X.25 PLE sent or received a restart packet. The restart that brings up the link should not send a x25Restart trap so the interface should send a linkUp trap. Sending this trap means the agent does not send a linkDown and linkUp trap.
2	X25Reset	If the PLE sends or receives a reset, the agent should send an x25Reset trap.
rfc1493.mib (dot1bridge) (Enterprise 1.3.6.1.2.1.17)		
1	newRoot	The newRoot trap indicates that the sending agent has become the new root of the spanning tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.
2	topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.
ibmiroc.mib (IBMROutingCode) (Enterprise 1.3.6.1.4.1.2.6.119)		
1	frrcvdFECN	This trap indicates that a frame was received from the network on this virtual circuit and it indicated forward congestion.
2	frrcvdBECN	This trap indicates that a frame was received from the network on this virtual circuit and it indicated backward congestion.
3	frrcvdCLLM	This trap indicates that a CLLM message was received from the network.
1	mosMemLow	This trap indicates that the free heap amount has dropped below a given percentage of the total heap memory available. The default percentage is 10%, however this threshold can be modified by the user via a patch variable.

Trap No.	Trap Name	Description
2	elsTrap	When the routing subsystem ELS component is configured to generate SNMP traps, the following trap is generated. It contains a single varBind containing a text string in one of the two following formats. If ELS timestamping is enabled: hr:min:sec subsys_name.event_num: message_text, for example, 09:32:56 IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc If ELS timestamping is disabled, subsys_name.event_num: message_text, for example - IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc Note: The following subsystems cannot have their events sent in SNMP traps (ARP, ICMP, UDP, SNMP and IP (excluding IP access control events)). This restriction is due to the fact that these subsystems are involved in sending an SNMP trap and allowing them could cause an infinite loop in the router software.
dlsw.mib (DLSW)		
1	dlswTrapTConnPartner Reject	This trap is sent each time a transport connection is rejected by a partner DLSw during Capabilities Exchanges. The emission of this trap is controlled by dlswTrapCntlTConnPartnerReject.
2	dlswTrapTConnProtViol ation	This trap is sent each time a protocol violation is detected for a transport connection. The emission of this trap is controlled by dlswTrapCntlTConnProtViolation.
3	dlswTrapTConnUp	This trap is sent each time a transport connection enters connected state. The emission of this trap is controlled by dlswTrapCntlTConn.
4	dlswTrapTConnDown	This trap is sent each time a transport connection enters disconnected state. The emission of this trap is controlled by dlswTrapCntlTConn.
5	dlswTrapCircuitUp	This trap is sent each time a circuit enters connected state. The emission of this trap is controlled by dlswTrapCntlCircuit.
6	dlswTrapCircuitDown	This trap is sent each time a circuit enters disconnected state. The emission of this trap is controlled by dlswTrapCntlCircuit.
sna-sdlc.mib		
		****** not found
sna-llc.mib		
		********** not found
if.mib		
		********** not found
isdn.mib		
		********** not found

A.5 Nways 8210 MultiProtocol Switched Services Server

The following table shows the MIB listings for the 8210.

Table 24. List of Source MIBs for Nways 8210 MultiProtocol Switched Services Server

Trap No.	Trap Name	Description
ibmMSS8210.mib (Enterprise 1.3.6.1.4.1.2.6.118.2 - mssServer8210)		

Trap No.	Trap Name	Description
2	mssServer8210ELSTrapV2	The trap announces that an event logging system (ELS) event occurred. The variable proElsSubSysEventMsg provides a textual description of the event. The variable is in one of two formats. If ELS timestamping is enabled, the format is hr:min:sec subsys_name.event_num: message_text. An example would be 09:32:56 IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc. If ELS timestamping is disabled, the format is subsys_name.event_num: message_text. An example would be IP.008: no rte 9.7.1.8 -> 9.7.4.3 dsc.
3	mss8210PCAdapTypeChg	The trap announces a change in the type of PC card. It will be sent if the value of the mss8210PCAdapType changes and mss8210NotifyStatus has a value of enabled(1).
4	mss8210TempThresholdChg	The trap announces a change in the temperature of the stand-alone. It will be sent if the value of the mss8210TempThreshold changes and mss8210NotifyStatus has a value of enabled(1).
5	mss8210PCIAdapStatusChg	The trap announces a change in the status of the PCI adapter. It will be sent if the value of either mss8210PCIAdapConfigType, mss8210PCIAdapOperStatus, mss8210PCIAdapDiagStatus, mss8210PCIAdapNetworkStatus or mss8210PCIAdapFaultStatus changes and mss8210NotifyStatus has a value of enabled(1).
rfc1215.mib		
0	cold start	Emitted when SNMP agent has completed initialization after a reload.
1	warm start	Emitted when SNMP agent has completed initialization after a restart.
2	link down	Emitted when a router/bridge interface has transitioned out of the “up” state. This may be the result of: - User initiated disable of the interface - Hardware failure - Maintenance traffic communications failure
3	link up	Emitted when a router/bridge interface has transitioned into the up state after passing self-test checks.
4	authentication failure.	Emitted when SNMP agent has received a packet that cannot be properly authenticated. This may be the result of: - Invalid community name string - Invalid origin IP address
rfc1269-BGP.mib		
1	bgpEstablished	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.
2	bgpBackwardTransition	The BGPBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state
rfc1493.mib (dot1bridge) (Enterprise 1.3.6.1.2.1.17)		
1	newRoot	The newRoot trap indicates that the sending agent has become the new root of the spanning tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.
2	topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.

Trap No.	Trap Name	Description
sna-sdlc.mib		
		not found
sna-llc.mib		
		not found
if.mib		
		not found

A.6 Nways 8224 Ethernet Stackable Hub

The following table provides a list of source MIBs for the 8224.

Table 25. List of Source MIBs for Nways 8224 Ethernet Stackable Hub

Trap No.	Trap Name	Description
ibm8224.mib		
		No trap output created.

A.7 Nways 8225 Fast Ethernet Stackable Hub

The following table provides a list of source MIBs for the 8225.

Table 26. List of Source MIBs for Nways 8225 Fast Ethernet Stackable Hub

Trap No.	Trap Name	Description
ibm8225.mib		
1	intrusionHappen	The specified port is intruded.
2	masterLinkFailEvent	The master link fails, and the backup link function is activated.
3	backupAgentRelay	The master agent fails, and the backup agent now monitors the system.
4	powerStatusChange	This trap is sent when a change occurs in the power supply of a hub. This occurs when a power supply is removed from a hub, added to a hub, or fails.
5	ipAutoDiscoveryTrap	This trap is sent by SNMP managed device to inform the network management station.

A.8 Nways 8229 Bridge

The following table provides a list of source MIBs for the 8229.

Table 27. List of Source MIBs for Nways 8229 Bridge

Trap No.	Trap Name	Description
ibm8229.mib		
		No trap output created.

A.9 Nways 8230 Token-Ring Concentrator

The following table provides a list of source MIBs for the 8230.

Table 28. List of Source MIBs for Nways 8230 TokenRing Concentrator

Trap No.	Trap Name	Description
ibm8230.mib (Enterprise 1.3.6.1.4.1.2.6.15 - ibm8230)		
1	cauBpOperStatusChg	This trap announces the change of the operational status of this CAU's backup (secondary) path. It will be sent if the value of cauBpOperStatus changes and cauNotifyAdminStatus has a value of enabled(1).
2	cauWrapOperStatusChg	This trap announces the change of the wrap status of this CAU. It will be sent if the value of cauWrapOperStatus changes and cauNotifyAdminStatus has a value of enabled(1).
3	cauInternalError	This trap announces a detected internal error in this CAU. It will be sent if the value of cauDiagErrCode changes and cauNotifyAdminStatus has a value of enabled(1).
4	cauModStatusChg	This trap announces a change to the status of this attachment module. It will be sent if the value of either cauModOperStatus, cauModAdminStatus, or cauModFaultStatus changes and cauNotifyAdminStatus has a value of enabled(1). Note that a change in the value of cauModOperStatus for a module will also imply a possible change in the value of cauLobeOperStatus for each of the lobes on that module. Thus, a separate cauLobeStatusChg trap will not be sent for each lobe on the module.
5	cauLobeStatusChg	This trap announces a change to the status of this lobe. It will be sent if the value of either cauLobeOperStatus, cauLobeAdminStatus, cauLobeInsertStatus, cauLobeFaultStatus, cauLobeMaxMACsExceeded changes and cauNotifyAdminStatus has a value of enabled(1). Note, however, that if the value of cauLobeOperStatus reflects a change in the operational status of a lobe due to a change in the operational status its parent module, this trap will not be sent for each of the lobes on that module. Instead, the cauModStatusChg trap that is sent will imply a change in status of the lobes as well.
6	cauRemovalIgnored	This trap announces that a forced remove command was received and ignored by this CAU. It will be sent if the value of cauNotifyAdminStatus is enabled(1).

Trap No.	Trap Name	Description
7	cauLastSetterChg	This trap announces that the last setter has changed in this CAU. It shall be sent if the value of cauNotifyAdminStatus has a value of enabled(1).
8	cauLobeConfigChg	This trap announces a change in the configuration of this lobe. It will be sent if the value of cauLobeMACAddrs changes and cauNotifyAdminStatus has a value of enabled(1). It shall be sent when cauLobeMACtype assumes a value of nonprotocol(2) and cauNotifyAdminStatus has a value of enabled(1).
9	cauCodeUpdateComplete	This trap announces that a code update for this CAU has completed successfully. It will be sent if the value of cauNotifyAdminStatus is enabled(1).
10	cauModRemoved	This trap announces that one of the CAU attachment modules has been removed. The cauModLocation variable indicates which module has been removed. Note, however, that after generation of this trap, the entry for the attachment module that has been removed will no longer exist in the cauModuleTable. This trap will be sent if the value of cauNotifyAdminStatus is enabled(1).
11	cauNAUNAddrChg	This trap announces that the NAUN of this CAU has changed. It will be sent if the value of cauNotifyAdminStatus has a value of enabled(1).
12	cauRlamControlLinkStabilityChg	This trap announces that the control link between the RLAM and the RLIU has gone up or down. Check the value of cauRemoteLamControlLinkStatus to determine the condition of the link. This trap will be sent if the value of cauNotifyAdminStatus has a value of enabled(1).
13	cauRlamDataCableStatusChg	This trap announces that the data cable between the RLAM and the RLIU has either just been connected or disconnected. Check the value of cauRemoteLamDataCableStatus to determine the condition of the cable. This trap will be sent if the value of cauNotifyAdminStatus has a value of enabled(1).

A.10 Nways 8235 Dial-In Access to LANs Server

The following table provides a list of source MIBs for the 8235.

Table 29. List of Source MIBs for Nways 8235 Dial-In Access to LANs Server

Trap No.	Trap Name	Description
ibm8235.mib (Enterprise - various shiva etc.)		
1	logNewMessage	This trap is generated when an new message of priority at or higher than logTrapPriority is generated, and SNMP trapping is enabled.
1	acctLostRecordTrap	This trap is generated when the system restarts, and determines that there has been accounting records or events stored in volatile memory when the system went down. Those records and events have been lost, and will not be sent to an accounting server.

Trap No.	Trap Name	Description
2	acctMemoryUnavailableTrap	This trap is generated when the accounting system runs out of volatile memory to store accounting records in.
3	acctMemoryAvailableTrap	This trap is generated when the accounting system is no longer out of volatile memory to store accounting records in.
4	acctVolatileTrap	This trap is generated when the system runs out of memory in non-volatile memory for accounting records, and starts using volatile memory that could be lost in a power failure.
1	radAcctServerTrap	This trap is generated when a configured RADIUS accounting server has been determined to have failed, and the agent shifts to a new RADIUS accounting server.
2	dmcModemDownTrap	This trap is generated when the system determines that an individual modem on the Digital Modem Card has gone down, and is failing the self-test.
1	dmcModemUpTrap	This trap is generated when the system determines that an individual modem on the Digital Modem Card that had previously failed diagnostics is operational again. It is not generated when the modem comes up at system startup; that would be too many traps at once!

A.11 Nways 8237 Ethernet Stackable Hub 10BASE-T

The following table provides a list of source MIBs for the 8237.

Table 30. List of Source MIBs for Nways 8237 Ethernet Stackable Hub 10BASE-T

Trap No.	Trap Name	Description
ibm8237.mib (Enterprise 1.3.6.1.4.1.6.134 - ibm8237)		
1	intrusionHappen	The specified port is intruded.
2	masterLinkFailEvent	The master link fails, and the backup link function is activated.
3	backupAgentRelay	The master agent fails, and the backup agent now monitors the system.
4	hubFanFailTrap	This trap is sent by SNMP managed device to inform the hub fan has failed.
5	ipAutoDiscoveryTrap	This trap is sent by SNMP managed device to inform the network management station.

A.12 Nways 8238 Token-Ring Stackable Hub

The following table provides a list of source MIBs for the 8238.

Table 31. List of Source MIBs for Nways 8238 Token-Ring Stackable Hub

Trap No.	Trap Name	Description
ibm8238.mib (Enterprise 1.3.6.1.4.1.49 - chipcom)		

Trap No.	Trap Name	Description
1	ibm8250Hello	A ibm8250Hello trap is sent every minute by an agent with the hello trap enabled. The hello trap will discontinue being sent when either the agent receives an authenticate SNMP request, or after 255 minutes.
2	ibm8250SlotDown	This trap indicates that the module in the indicated slot is down. Usually, this trap is sent when the module has been removed. Sometimes, this trap is sent when management communications with this module have been broken. In this case, it may not be possible to distinguish between a removed and a failed module. The module type (modType) and the module description (modDescr) are also provided in this case.
3	ibm8250SlotUp	This trap indicates that a blade in the indicated slot is up. Usually, this trap is sent when the module is inserted into the hub. Sometimes, this trap is sent when management communications have been restored to a module where they were previously broken. In this case, it may not be possible to distinguish between a module that has just be inserted and a module that has just the. The module type (modType) and the module description (modDescr) are also provided in this case.
4	ibm8250Environment	An ibm8250Environment trap indicates a change in the concentrator's environment has occurred. The variables supplied indicate what exactly changed.
5	ibm8250Hardware	An ibm8250Hardware trap indicates that a soft hardware failure has been detected. An example of a soft hardware failure is too many writes to non-volatile storage. This is an indication to get the unit serviced.
6	ibm8250Software	An ibm8250Software trap indicates that a soft software failure has been detected. This is an indication to get the unit serviced.
7	ibm8250Change	An ibm8250Change trap is used to indicate that a configuration change has occurred. The actual variables that changed are included in the variables section of the PDU.
8	ibm8250Fatal	An ibm8250Fatal trap is used to indicate that a fatal error has occurred. This is an indication to get the unit serviced.
9	ibm8250TrunkDown	An ibm8250TrunkDown trap indicates that trunk's status has changed to an error condition. Multiple ibm8250TrunkDown traps may be sent if the trunk's status changes from one error to another.
10	ibm8250TrunkUp	An ibm8250TrunkUp trap indicates that a trunk's status has changed to a non-error (okay or warning) condition.
11	ibm8250PortDown	An ibm8250PortDown trap indicates that a port's status has changed to an error condition. Multiple ibm8250PortDown traps may be sent if the port's status changes from one error to another.
12	ibm8250PortUp	An ibm8250PortUp trap indicates that a port's status has changed to a non-error (okay or warning) condition.
13	ibm8250Ping	An ibm8250Ping trap is sent after the SNMP-initiated PING command is completed. After the last echo request packet is sent, this trap is sent indicating the ping address, the number of requests sent, and the number of responses received at the time the trap was generated.
14	ibm8250AboveThreshd	An ibm8250AboveThreshd trap indicates that a Counter or Gauge variable has exceeded its threshold. The variable that is above its threshold is the only variable in the varBind list. Its value is taken at the time the threshold calculation is performed and therefore may be greater than the actual threshold value. Another above threshold trap will not be sent until a below threshold trap is sent.

Trap No.	Trap Name	Description
15	ibm8250BelowThreshd	An ibm8250BelowThreshd trap indicates that a Counter or Gauge variable had exceeded its threshold but is now below its threshold. The variable that is below its threshold is the only variable in the varBind list. Its value is taken at the time the threshold calculation is performed and therefore may be less than the actual threshold value. Another below threshold trap will not be sent until an above threshold trap is sent.
16	ibm8250ModuleDown	A ibm8250ModuleDown trap indicates that management communications with the slot indicated by chipModSlotIndex have been broken. This event usually occurs when a module has been physically removed from the concentrator. However, it is possible for this event to occur when the particular module fails.
17	ibm8250ModuleUp	An ibm8250ModuleUp trap indicates that management communications with the slot indicated by chipModSlotIndex has been established. This event usually occurs when a module has physically been inserted into the concentrator. The variable chipModType indicates the module type inserted.
18	ibm8250Security	This trap indicates a change in the security environment. The netSecTrapReason specifies the reason for the trap. Some traps may include additional information, depending upon the reason. If the trap reason is intrusion-attempt(2), then the following objects will also be included in the trap: portSlotIndex and portPortIndex (to specify on which port the intrusion attempt occurred), and portAdminState (to indicate whether the port was automatically disabled). If the MAC address of the intruder is available, either the enetStatsPortLastSrcAddr object (if supported) or the ocNetOCSecIntruderMacAddressIndex object will be included. If the trap reason is net-secured(3), then the following objects will be included in the trap: ocNetOCSecNetOperState, ocModNetwork, ocModSlotIndex, ocModSubSlotIndex, ocModType, and ocModDescr. If the trap reason is net-unsecured(4), then the following objects will be included in the trap: ocNetOCSecNetOperState and ocModNetwork.
23	ibm8250ModulePortDown	An ibm8250ModulePortDown trap indicates that a port's status has changed to an error condition. Multiple ibm8250ModulePortDown traps may be sent if the port's status changes from one error to another.
24	ibm8250ModulePortUp	An ibm8250ModulePortUp trap indicates that a port's status has changed to a non-error (okay or warning) condition.

A.13 Nways 8239 Token-Ring Stackable Hub

The following table provides a list of source MIBs for the 8239.

Table 32. List of Source MIBs for Nways 8239 Token-Ring Stackable Hub

Trap No.	Trap Name	Description
ibm8239.mib (Enterprise 1.3.6.1.4.1.2.6.138 - ibm8239TrHub)		
1	trapPortUp	The state of a port has changed.
2	trapPortDown	The state of a port has changed.
3	trapHubUp	The state of a hub has changed.
4	trapHubDown	The state of a hub has changed.

Trap No.	Trap Name	Description
5	trapIntruderDetected	An intrusion has occurred at the specified port.
6	trapScriptExecuteOk	A script has successfully completed execution.
7	trapScriptExecuteFail	A script has failed execution.
8	trapCodeVersionMismatch	A code version mismatch has been detected on a hub.
9	trapMultipleUsers	This trap announces the presence of multiple users logged into the stack.
10	trapRingIOStatusUpDown	The state of ring_in/ring_out has changed.
11	trapDataIOStatusUpDown	The state of the data_in/data_out has changed.
12	trapControlIOStatusUpDown	The state of the control_in/control_out has changed.

A.14 Nways 8250 Multiprotocol Intelligent Hub

The following table provides a list of source MIBs for the 8250.

Table 33. List of Source MIBs for Nways 8250 Multiprotocol Intelligent Hub

Trap No.	Trap Name	Description
ibm8250.mib (Enterprise 1.3.6.1.4.1.49 - chipcom)		
1	ibm8250Hello	An ibm8250Hello trap is sent every minute by an agent with the hello trap enabled. The hello trap will discontinue being sent when either the agent receives an authenticate SNMP request, or after 255 minutes.
2	ibm8250SlotDown	This trap indicates that the module in the indicated slot is down. Usually, this trap is sent when the module has been removed. Sometimes, this trap is sent when management communications with this module have been broken. In this case, it may not be possible to distinguish between a removed and a failed module. The module type (modType) and the module description (modDescr) are also provided in this case.
3	ibm8250SlotUp	This trap indicates that a blade in the indicated slot is up. Usually, this trap is sent when the module is inserted into the hub. Sometimes, this trap is sent when management communications have been restored to a module where they had previously been broken. In this case, it may not be possible to distinguish between a module that has just be inserted and a module that has just the. The module type (modType) and the module description (modDescr) are also provided in this case.
4	ibm8250Environment	An ibm8250Environment trap indicates a change in the concentrator's environment has occurred. The variables supplied indicate what exactly changed.
5	ibm8250Hardware	An ibm8250Hardware trap indicates that a soft hardware failure has been detected. An example of a soft hardware failure is too many writes to non-volatile storage. This is an indication to get the unit serviced.
6	ibm8250Software	An ibm8250Software trap indicates that a soft software failure has been detected. This is an indication to get the unit serviced.

Trap No.	Trap Name	Description
7	ibm8250Change	An ibm8250Change trap is used to indicate that a configuration change has occurred. The actual variables that changed are included in the variables section of the PDU.
8	ibm8250Fatal	An ibm8250Fatal trap is used to indicate that a fatal error has occurred. This is an indication to get the unit serviced.
9	ibm8250TrunkDown	An ibm8250TrunkDown trap indicates that trunk's status has changed to an error condition. Multiple ibm8250TrunkDown traps may be sent if the trunk's status changes from one error to another.
10	ibm8250TrunkUp	An ibm8250TrunkUp trap indicates that a trunk's status has changed to a non-error (okay or warning) condition.
11	ibm8250PortDown	An ibm8250PortDown trap indicates that a port's status has changed to an error condition. Multiple ibm8250PortDown traps may be sent if the port's status changes from one error to another.
12	ibm8250PortUp	An ibm8250PortUp trap indicates that a port's status has changed to a non-error (okay or warning) condition.
13	ibm8250Ping	A ibm8250Ping trap is sent after the SNMP initiated PING command is completed. After the last echo request packet is sent, this trap is sent indicating the ping address, the number of requests sent, and the number of responses received at the time the trap was generated.
14	ibm8250AboveThreshd	An ibm8250AboveThreshd trap indicates that a Counter or Gauge variable has exceeded its threshold. The variable which is above its threshold is the only variable in the varBind list. Its value is taken at the time the threshold calculation is performed and therefore may be greater than the actual threshold value. Another above threshold trap will not be sent until a below threshold trap is sent.
15	ibm8250BelowThreshd	An ibm8250BelowThreshd trap indicates that a Counter or Gauge variable had exceeded its threshold but is now below its threshold. The variable that is below its threshold is the only variable in the varBind list. Its value is taken at the time the threshold calculation is performed and therefore may be less than the actual threshold value. Another below threshold trap will not be sent until an above threshold trap is sent.
16	ibm8250ModuleDown	An ibm8250ModuleDown trap indicates that management communications with the slot indicated by chipModSlotIndex has been broken. This event usually occurs when a module has been physically removed from the concentrator. However, it is possible for this event to occur when the particular module fails.
17	ibm8250ModuleUp	An ibm8250ModuleUp trap indicates that management communications with the slot indicated by chipModSlotIndex have been established. This event usually occurs when a module has physically been inserted into the concentrator. The variable chipModType indicates the module type inserted.

Trap No.	Trap Name	Description
18	ibm8250Security	This trap indicates a change in the security environment. The netSecTrapReason specifies the reason for the trap. Some traps may include additional information, depending upon the reason. If the trap reason is intrusion-attempt(2), then the following objects will also be included in the trap: portSlotIndex and portPortIndex (to specify on which port the intrusion attempt occurred), and portAdminState (to indicate whether the port was automatically disabled). If the MAC address of the intruder is available, either the enetStatsPortLastSrcAddr object (if supported) or the ocNetOCSecIntruderMacAddressIndex object will be included. If the trap reason is net-secured(3), then the following objects will be included in the trap: ocNetOCSecNetOperState, ocModNetwork, ocModSlotIndex, ocModSubSlotIndex, ocModType, and ocModDescr. If the trap reason is net-unsecured(4), then the following objects will be included in the trap: ocNetOCSecNetOperState and ocModNetwork.
23	ibm8250ModulePortDown	An ibm8250ModulePortDown trap indicates that a port's status has changed to an error condition. Multiple ibm8250ModulePortDown traps may be sent if the port's status changes from one error to another.
24	ibm8250ModulePortUp	An ibm8250ModulePortUp trap indicates that a port's status has changed to a non-error (okay or warning) condition.

A.15 Nways 8260 Multiprotocol Switching Hub

The following table provides a list of source MIBs for the 8260.

Table 34. List of Source MIBs for Nways 8260 Multiprotocol Switching Hub

Trap No.	Trap Name	Description
ibm8260.mib (Enterprise 1.3.6.1.4.1.49 - chipcom)		
1	ibm8250Hello	An ibm8250Hello trap is sent every minute by an agent with the hello trap enabled. The hello trap will discontinue being sent when either the agent receives an authenticate SNMP request, or after 255 minutes.
2	ibm8250SlotDown	This trap indicates that the module in the indicated slot is down. Usually, this trap is sent when the module has been removed.Sometimes, this trap is sent when management communications with this module have been broken. In this case, it may not be possible to distinguish between a removed and a failed module. The module type (modType) and the module description (modDescr) are also provided in this case.
3	ibm8250SlotUp	This trap indicates that a blade in the indicated slot is up. Usually, this trap is sent when the module is inserted into the hub. Sometimes, this trap is sent when management communications have been restored to a module where they were previously been broken. In this case, it may not be possible to distinguish between a module that has just be inserted and a module that has just the. The module type (modType) and the module description (modDescr) are also provided in this case.
4	ibm8250Environment	An ibm8250Environment trap indicates a change in the concentrator's environment has occurred. The variables supplied indicate what exactly changed.
5	ibm8250Hardware	An ibm8250Hardware trap indicates that a soft hardware failure has been detected. An example of a soft hardware failure is too many writes to non-volatile storage. This is an indication to get the unit serviced.

Trap No.	Trap Name	Description
6	ibm8250Software	An ibm8250Software trap indicates that a soft software failure has been detected. This is an indication to get the unit serviced.
7	ibm8250Change	An ibm8250Change trap is used to indicate that a configuration change has occurred. The actual variables that changed are included in the variables section of the PDU.
8	ibm8250Fatal	An ibm8250Fatal trap is used to indicate that a fatal error has occurred. This is an indication to get the unit serviced.
9	ibm8250TrunkDown	An ibm8250TrunkDown trap indicates that trunk's status has changed to an error condition. Multiple ibm8250TrunkDown traps may be sent if the trunk's status changes from one error to another.
10	ibm8250TrunkUp	An ibm8250TrunkUp trap indicates that a trunk's status has changed to a non-error (okay or warning) condition.
11	ibm8250PortDown	An ibm8250PortDown trap indicates that a port's status has changed to an error condition. Multiple ibm8250PortDown traps may be sent if the port's status changes from one error to another.
12	ibm8250PortUp	An ibm8250PortUp trap indicates that a port's status has changed to a non-error (okay or warning) condition.
13	ibm8250Ping	An ibm8250Ping trap is sent after the SNMP initiated PING command is completed. After the last echo request packet is sent, this trap is sent indicating the ping address, the number of requests sent, and the number of responses received at the time the trap was generated.
14	ibm8250AboveThreshd	An ibm8250AboveThreshd trap indicates that a Counter or Gauge variable has exceeded its threshold. The variable that is above its threshold is the only variable in the varBind list. Its value is taken at the time the threshold calculation is performed and therefore may be greater than the actual threshold value. Another above threshold trap will not be sent until a below threshold trap is sent.
15	ibm8250BelowThreshd	A ibm8250BelowThreshd trap indicates that a Counter or Gauge variable had exceeded its threshold but is now below its threshold. The variable which is below its threshold is the only variable in the varBind list. Its value is taken at the time the threshold calculation is performed and therefore may be less than the actual threshold value. Another below threshold trap will not be sent until an above threshold trap is sent.
16	ibm8250ModuleDown	An ibm8250ModuleDown trap indicates that management communications with the slot indicated by chipModSlotIndex has been broken. This event usually occurs when a module has been physically removed from the concentrator. However, it is possible for this event to occur when the particular module fails.
17	ibm8250ModuleUp	An ibm8250ModuleUp trap indicates that management communications with the slot indicated by chipModSlotIndex has been established. This event usually occurs when a module has physically been inserted into the concentrator. The variable chipModType indicates the module type inserted.

Trap No.	Trap Name	Description
18	ibm8250Security	This trap indicates a change in the security environment. The netSecTrapReason specifies the reason for the trap. Some traps may include additional information, depending upon the reason. If the trap reason is intrusion-attempt(2), then the following objects will also be included in the trap: portSlotIndex and portPortIndex (to specify on which port the intrusion attempt occurred), and portAdminState (to indicate whether the port was automatically disabled). If the MAC address of the intruder is available, either the enetStatsPortLastSrcAddr object (if supported) or the ocNetOCSecIntruderMacAddressIndex object will be included. If the trap reason is net-secured(3), then the following objects will be included in the trap: ocNetOCSecNetOperState, ocModNetwork, ocModSlotIndex, ocModSubSlotIndex, ocModType, and ocModDescr. If the trap reason is net-unsecured(4), then the following objects will be included in the trap: ocNetOCSecNetOperState and ocModNetwork.
23	ibm8250ModulePortDown	An ibm8250ModulePortDown trap indicates that a port's status has changed to an error condition. Multiple ibm8250ModulePortDown traps may be sent if the port's status changes from one error to another.
24	ibm8250ModulePortUp	An ibm8250ModulePortUp trap indicates that a port's status has changed to a non-error (okay or warning) condition.

A.16 Nways 8265 ATM Switch

The following table provides a list of source MIBs for the 8265.

Table 35. List of Source MIBs for Nways 8265 ATM Switch

Trap No.	Trap Name	Description
ibm8265v23.mib (Enterprise 1.3.6.1.4.1.6.33 - atmSw)		
1	hello	A hello trap is sent: - When the system re-initializes: it is sent every minutes until an SNMP request is received or until 255 minutes have passed. - When one of the following parameters is changed: -- agent IP address(es) -- agent subnet mask(s) -- ATM address of the IP ARP server -- IP address of the default gateway The value of ifPhysAddress is the ATM address of the hub. The hello trap may be disabled.
2	lock	A lock trap is sent when a set request is rejected because it is suspected that this may cause to break the link between the agent and the manager. This may occur when: - Isolating a slot - Disabling a port if the request is received through this specific port/module/slot.

Trap No.	Trap Name	Description
3	change	A change trap is sent when one of the following MIB variables or group of variables is changed: - Date and Time reset - System Parameters (name, contact, location) changed - Interface changed: -- Administrative State (enabled/disabled) - Module changed: -- Administrative State (isolate/attach). When one of this variable is changed, the lastChange MIB object is also updated with the current date and time. When the Date and Time or the System Parameters changed, the interface number of the hub virtual interface is returned. This trap may be disabled.
4	pvcFailure	A PVC failure trap is sent when a PVC becomes inoperational.
6	callLoggingOverflow	A callLoggingOverflow trap is sent when the call logging table is about to wrap.
7	moduleInstalled	An ATM module has been detected in the hub.
8	moduleRemoved	An ATM module is no longer detected in the hub.
9	lesMaxClientsReached	The maximum number of LAN emulation clients has been connected to the given LAN emulation server.
10	lesMaxClientsThresholdDown	The number of operational clients of the given emulated LAN is now equal to lesMaxNumberOfClients - 10. This trap is sent only if the traplesMaxClientsReached has been sent previously. lesIndex is the index of the lesConfTable defined above.
102	chassisSlotDown	This trap indicates that a module is down. Usually, this trap is sent when the module has been removed. Sometimes, this trap is sent when management communications with this module have been broken. In this case, it may not be possible to distinguish between a removed and a failed module.
103	chassisSlotUp	This trap indicates that a module is up. Usually, this trap is sent when the module is inserted into the hub. Sometimes, this trap is sent when management communications have been restored to a module where they had previously been broken.
104	chassisEnvironment	A chassisEnvironment trap indicates a change in the concentrator's environment has occurred. The variables supplied indicate what exactly changed.
107	chassisChange	A chassisChange trap is used to indicate that a configuration change has occurred. The actual variables that changed are included in the variables section of the PDU.
116	chassisModuleDown	A chassisModuleDown trap indicates that management communications with a slot has been broken. This event usually occurs when a module has been physically removed from the concentrator. However, it is possible for this event to occur when the particular module fails.
117	chassisModuleUp	A chassisModuleUp trap indicates that management communications with a slot has been established. This event usually occurs when a module has physically been inserted into the concentrator. The variable chipModType indicates the module type inserted.

A.17 Nways 8270 LAN Switch

The following table provides a list of source MIBs for the 8270.

Table 36. List of Source MIBs for Nways 8270 LAN Switch

Trap No.	Trap Name	Description
tr_b51.trp (Enterprise 1.3.6.1.4.1.2.6.66 - ibm8272TsSys/port/Dmns)		
1	ibm8272TsTempThreshold	This trap is generated when the system temperature either exceeds 50 C or when it returns to normal(45 C) after exceeding the temperature. The variable ibm8272Ts2SysTemperature indicates the temperature condition at the time of the event.
2	ibm8272TsPwrSupChange	This trap is generated when the power supply status of the switch is inError or returns to normal. This trap is only generated if the switch has more than one power supply and at least one of the other power supplies is operational.
3	ibm8272TsFanChange	This trap is generated when the fan status of the switch is inError or returns to normal.
4	ibm8272TsVoltageChange	This trap is generated when the voltage status of the switch is low or returns to normal.
1	ibm8272TsPortCfgLossTrap	This trap occurs when a port is disabled because it has exceeded its Configuration Loss Threshold within the configured Sampling Period.
2	ibm8272TsBeaconStart	This trap is generated when a port or a station local to a port begins to beacon. It is sent out only when a ring status change indicates that a station is beaconing.
3	ibm8272TsBeaconEnd	This trap is generated when the ring status change indicates that a ring is no longer beaconing. This trap only occurs only once when the status actually changes.
4	ibm8272TsMaxFrameSizeExceeded	This trap is generated when there has been a change in the number of oversized frames received (>4540 bytes) on the port. This trap is only sent once every ten minutes for any given port.
5	ibm8272TsPortSwitchModeChange Trap	This trap is generated only when the port changes from cut-through mode to store-and-forward mode based on the error trend calculations.
1	ibm8272TsDmnNewRoot	This trap is a domain specific version of the newRoot trap as described in RFC1493. The newRoot trap indicates that the sending agent has become the new root of the spanning tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.
2	ibm8272TsDmnTopologyChange	This trap is a domain-specific version of the topologyChange trap as described in RFC1493. A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.

A.18 Nways 8271 EtherStreamer Ethernet LAN Switch

The following table provides a list of source MIBs for the 8271.

Table 37. List of Source MIBs for Nways 8271 EtherStreamer Ethernet LAN Switch

Trap No.	Trap Name	Description
rfc1215.mib		
0	cold start	Emitted when SNMP agent has completed initialization after a reload.
1	warm start	Emitted when SNMP agent has completed initialization after a restart.
2	link down	Emitted when a router/bridge interface has transitioned out of the up state. This may be the result of: - User initiated disable of the interface - Hardware failure - Maintenance traffic communications failure
3	link up	Emitted when a router/bridge interface has transitioned into the up state after passing self-test checks.
4	authentication failure.	Emitted when SNMP agent has received a packet that cannot be properly authenticated. This may be the result of: - Invalid community name string - Invalid origin IP address
ibm8271_e.trp		
1	ibm8271eEsTempChange	This trap is generated when the temperature in a switch exceeds normal or returns to normal.
1	ibm8271eEsPortStrNFwdEntry	This trap is genearted when a port automatically enters store and forward mode when the error rate exceeds the threshold.
1	ibm8271eEsDmnNewRoot	This trap is a domain-specific version of the newRoot trap as described in RFC1493. The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.
2	ibm8271eEsDmnTopologyChange	This trap is a domain specific version of the topologyChange trap as described in RFC1493. A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.
1	ibm8271eEsEtherPipeFailed	This trap is sent when one of the links in an EtherPipe fail. The variable ibm8271eEsEPPorts contains the ports which are operational in the EtherPipe.
3com0006.mib		
		not found
3com0007.mib		
		not found
3com0010.mib		
		not found
3com0014.mib		

<table>
<tr><th>Trap No.</th><th>Trap Name</th><th>Description</th></tr>
<tr><td>43</td><td>resResilienceSwitch</td><td>This trap is generated when a change of state of one of the ports in a resilient pair does not result in a switch of active port. If such a switch were to occur the resResilienceSwitch would be generated. Generation of this trap is summarized in the following table:

<table>
<tr><th colspan="2">State</th><th colspan="4">Event</th></tr>
<tr><th>Main</th><th>Backup</th><th>Main Fail</th><th>Main OK</th><th>Standby Fail</th><th>Standby OK</th></tr>
<tr><td>Active</td><td>OK</td><td>switch</td><td>-----</td><td>state</td><td>-----</td></tr>
<tr><td>Active</td><td>Fail</td><td>state</td><td>-----</td><td>-----</td><td>state</td></tr>
<tr><td>OK</td><td>Active</td><td>state</td><td>-----</td><td>switch</td><td>-----</td></tr>
<tr><td>Fail</td><td>Active</td><td>-----</td><td>state</td><td>state</td><td>-----</td></tr>
<tr><td>Fail</td><td>Fail</td><td>-----</td><td>switch</td><td>-----</td><td>state</td></tr>
</table>
In this table ----- indicates no trap is sent, switch indicates the resResilienceSwitch trap is sent and state indicates resStateChange is sent. Note: The agent in the MSH does not suppress any traps that caused the state change. For example if the active link is lost then both a loss-of-link trap and a resilienceSwitch trap are generated.</td></tr>
<tr><td>44</td><td>resStateChange</td><td>This trap is generated when a change of state of one of the ports in a resilient pair does not result in a switch of active port. If such a switch were to occur, the resResilienceSwitch would be generated. Generation of this trap is summarized in the following table:

<table>
<tr><th colspan="2">State</th><th colspan="4">Event</th></tr>
<tr><th>Main</th><th>Backup</th><th>Main Fail</th><th>Main OK</th><th>Standby Fail</th><th>Standby OK</th></tr>
<tr><td>Active</td><td>OK</td><td>switch</td><td>-----</td><td>state</td><td>-----</td></tr>
<tr><td>Active</td><td>Fail</td><td>state</td><td>-----</td><td>-----</td><td>state</td></tr>
<tr><td>OK</td><td>Active</td><td>state</td><td>-----</td><td>switch</td><td>-----</td></tr>
<tr><td>Fail</td><td>Active</td><td>-----</td><td>state</td><td>state</td><td>-----</td></tr>
<tr><td>Fail</td><td>Fail</td><td>-----</td><td>switch</td><td>-----</td><td>state</td></tr>
</table>
In this table ----- indicates no trap is sent, switch indicates the resResilienceSwitch trap is sent and state indicates resStateChange is sent. Note: The agent in the MSH does not suppress any traps that caused the state change. For example if the active link is lost then both a loss-of-link trap AND a resilienceSwitch trap are generated.</td></tr>
<tr><td colspan="3">3com0018.mib</td></tr>
<tr><td></td><td></td><td>not found</td></tr>
<tr><td colspan="3">3com0019.mib</td></tr>
<tr><td>74</td><td>remPollSuccessTrap</td><td>This trap is generated by the EventTable (if the eventEntry is configured to send traps) when the remPollTable receives a reply to a poll after a sequence of un-successful polls.</td></tr>
<tr><td>75</td><td>remPollFailureTrap</td><td>This trap is generated by the EventTable (if the eventEntry is configured to send traps) when the remPollTable fails to receive a reply to a poll.</td></tr>
</table>

Trap No.	Trap Name	Description
3com0020.mib		
		not found
3com0021.mib		
71	secureAddressLearned	This trap is sent when a new station has been learned. The slot and port on which the address was received are in the first and second index of secureAddrRowStatus, and the MAC address of the learned station is in the third index.
78	secureViolation2	This trap is sent whenever a security violation has occured. The slot and port on which the violation occured are in the first and second index of secureAddrRowStatus, and the MAC address of the offending station is in the third index. rptrPortAdminSTATUS indicates if the port has been disabled because of the violation. The implementation may not send violation traps from the same port at intervals of less than 5 seconds.
3com0024.mib		
		not found
3com0039.mib		
65	brDatabaseFull	This trap indicates that either the Filtering database, the permanent database or the ATM Downlink database has become full. If the database occupancy exceeds 90% this trap will be sent also. The variable bindings enable the trap to be identified as referring to the filtering, permanent, or ATM Downlink database, and to differentiate between 90% or 100% full.
rfc1493.mib (dot1bridge)		
1	newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional
2	topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional
rfc1757 (RMON)		
1	risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
2	fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

A.19 Nways 8272 LANStreamer TokenRing LAN Switch

The following table provides a list of source MIBs for the 8272.

Table 38. List of Source MIBs for Nways 8272 LANStreamer TokenRing LAN Switch

Trap No.	Trap Name	Description
rfc1493.mib - dot1bridge (Enterprise 1.3.6.1.2.1.17)		
1	newRoot	The newRoot trap indicates that the sending agent has become the new root of the spanning tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.
2	topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.
rfc1757 - RMON		
1	risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
2	fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.
tr_a51.trp (Enterprise 1.3.6.1.4.1.2.6.66 - ibm8272TsSys/port/Dmns)) ** Same as 8270 Tr_b51.trp		
1	ibm8272TsTempThreshold	This trap is generated when the system temperature either exceeds 50 C or when it returns to normal(45 C) after exceeding the temperature. The variable ibm8272Ts2SysTemperature indicates the temperature condition at the time of the event.
2	ibm8272TsPwrSupChange	This trap is generated when the power supply status of the switch is inError or returns to normal. This trap is only generated if the switch has more than one power supply and at least one of the other power supplies is operational.
3	ibm8272TsFanChange	This trap is generated when the fan status of the switch is inError or returns to normal.
4	ibm8272TsVoltageChange	This trap is generated when the voltage status of the switch is low or returns to normal.
1	ibm8272TsPortCfgLossTrap	This trap occurs when a port is disabled because it has exceeded its Configuration Loss Threshold within the configured Sampling Period.
2	ibm8272TsBeaconStart	This trap is generated when a port or a station local to a port begins to beacon. It is sent out only when a ring status change indicates that a station is beaconing.
3	ibm8272TsBeaconEnd	This trap is generated when the ring status change indicates that a ring is no longer beaconing. This trap only occurs only once when the status actually changes.

Trap No.	Trap Name	Description
4	ibm8272TsMaxFrameSizeExceeded	This trap is generated when there has been a change in the number of oversized frames received (>4540 bytes) on the port. This trap is only sent once every ten minutes for any given port.
5	ibm8272TsPortSwitchModeChangeTrap	This trap is generated only when the port changes from cut-through mode to store-and-forward mode based on the error trend calculations.
1	ibm8272TsDmnNewRoot	This trap is a domain specific version of the newRoot trap as described in RFC1493. The newRoot trap indicates that the sending agent has become the new root of the spanning tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.
2	ibm8272TsDmnTopologyChange	This trap is a domain specific version of the topologyChange trap as described in RFC1493. A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.

A.20 Nways 8273 Ethernet RouteSwitch

The following table provides a list of source MIBs for the 8273.

Table 39. List of Source MIBs for Nways 8273 Ethernet RouteSwitch

Trap No.	Trap Name	Description
xylan-pizza-trap.mib (Enterprise 1.3.6.1.4.1.800.3.1.1.3 - pizzaswitch)		
1	tempAlarm3	A tempAlarm indicates a temperature sensor has changed its state from underThreshold(4) to overThreshold(3).
2	moduleChange3	A moduleChange trap occurs when a module is inserted or removed from the chassis.
3	powerEvent3	A powerEvent trap occurs when a power supply is inserted or removed from the chassis, or a problem condition is recognized on a power supply.
4	controllerEvent3	A controlEvent trap occurs when a chassis controller (MPM) loses or gains the state of master(3). If this is due to chassis controller being inserted or removed from the slot, a moduleChange trap will also be sent.
5	loginViolation3	A loginViolation trap occurs when a login attempt fails due to an incorrect login ID or password.
6	macVlanViolation3	A macVlanViolation trap occurs when a frame is received from a port with a VLAN ID different from the VLAN where the frame previously has received.
7	macDuplicatePort3	A macDuplicatePort trap occurs when a frame is received from a source port different from the port where the frame previously has received although they both ports belong to the same VLAN.
8	portLinkUpEvent3	A portLinkTrap occurs whenever a phy, log, or virt port is enabled.
9	portLinkDownEvent3	A portLinkTrap occurs whenever a phy, log, or virt port is disabled.

Trap No.	Trap Name	Description
10	portPartitioned3	A portPartioned trap occurs when the physical port has transitioned thru enable/disable states faster than 10 times in the past second...indicative of a flakey cable.
11	portRecordMismatch3	A portRecordMismatch trap occurs when the specified port data is found to be different than the previous configuration. Typically this will be generated when a NIC of one type is swapped out for a DIFFERENT type. IE Ethernet for FDDI, ATM for token-ring, etc.
14	groupChange3	A groupChange trap occurs whenever a group is created or deleted from the system via the UI or SNMP. The group and status code are sent as part of the variable binding. The status codes are: 1 - disable 2 - enable 3 - delete 4 - create 5 - modify (see xylan-vport MIB)
15	vlanChange3	A vlanChange trap occurs whenever a VLAN is created or deleted from the system via the UI or SNMP. The group, VLAN and status code are sent as part of the variable binding. See groupChange for the status codes.
16	portMove3	A portMove trap occurs when the specified port is moved from a group/VLAN or has had its configuration changed.
17	moduleResetReload3	A moduleResetReload trap occurs when the specified module has been reset or reloaded by the chassis mgr.
18	systemEvent3	A systemEvent trap occurs when a potentially fatal system error occurs. Such as: out of FLASH/memory space. The event type is in the var bind.
19	vlanRouteTableFull3	A vlanRouteTableFull trap occurs when either the IP or IPX route table is full. (discovered on insertion attempt).
20	sapTableFull3	A sapTableFull trap occurs when the IPX SAP table is found to be full on insertion.
21	atmSSCOPstate3	A atmSSCOPstate trap occurs when the signalling state for the specified physical port changes.
22	ilmiState3	A ilmiState trap occurs when the ILMI state for the specified physical port changes.
23	atmConnection3	A atmConnection trap occurs when the specified ATM Vcc is created or deleted.
24	atmService3	A atmService trap occurs when the specified ATM service is created or deleted.
27	dlciNew3	FrameRelay Dlci Just Created.
28	dlciDel3	FrameRelay Dlci Just Deleted.
29	dlciUp3	FrameRelay Dlci Just Changed to Active.
30	dlciDn3	FrameRelay Dlci Just Changed to InActive.
31	portManualForwarding Mode3	A portManualForwardingMode trap occurs when the specified port is placed into manual mode forwarding as its default setting whenever the port is assigned to a group that is participating in the IBM spanning tree algorithm.

A.21 Nways 8274LAN RouteSwitch

The following table provides a list of source MIBs for the 8274.

Table 40. List of Source MIBs for Nways 8274LAN RouteSwitch

Trap No.	Trap Name	Description
xylan-5slot-trap.mib (Enterprise 1.3.6.1.4.1.800.3.1.1.1- omniswitch5)		
1	tempAlarm5	A tempAlarm indicates a temperature sensor has changed its state from underThreshold(4) to overThreshold(3).
2	moduleChange5	A moduleChange trap occurs when a module is inserted or removed from the chassis.
3	powerEvent5	A powerEvent trap occurs when a power supply is inserted or removed from the chassis, or a problem condition is recognized on a power supply.
4	controllerEvent5	A controlEvent trap occurs when a chassis controller (MPM) loses or gains the state of master(3). If this is due to chassis controller being inserted or removed from the slot, a moduleChange trap will also be sent.
5	loginViolation5	A loginViolation trap occurs when a login attempt fails due to an incorrect login-id or password.
6	macVlanViolation5	A macVlanViolation trap occurs when a frame is received from a port with a VLAN ID different from the VLAN where the frame previously has received.
7	macDuplicatePort5	A macDuplicatePort trap occurs when a frame is received from a source port different from the port where the frame previously has received although they both ports belong to the same VLAN.
8	portLinkUpEvent5	A portLinkTrap occurs whenever a phy, log, or virt port is enabled.
9	portLinkDownEvent5	A portLinkTrap occurs whenever a phy, log, or virt port is disabled.
10	portPartitioned5	A portPartioned trap occurs when the physical port has transitioned thru enable/disable states faster than 10 times in the past second...indicative of a flakey cable.
11	portRecordMismatch5	A portRecordMismatch trap occurs when the specified port data is found to be diferent than the previous configuration. Typically this will be generated when a NIC of one type is swapped out for a different type. IE ethernet for fddi, atm for token-ring, etc...
14	groupChange5	A groupChange trap occurs whenever a group is created or deleted from the system via the UI or SNMP. The group and status code are sent as part of the variable binding. The status codes are: 1 - disable 2 - enable 3 - delete 4 - create 5 - modify (see xylan-vport MIB).
15	vlanChange5	A vlanChange trap occurs whenever a VLAN is created or deleted from the system via the UI or SNMP. The group, vlan and status code are sent as part of the variable binding. See groupChange for the status codes.
16	portMove5	A portMove trap occurs when the specified port is moved from a group/vlan or has had its configuration changed.
17	moduleResetReload5	A moduleResetReload trap occurs when the specified module has been reset or reloaded by the chassis mgr.
18	systemEvent5	A systemEvent trap occurs when a potentially fatal system error occurs, such as: out of FLASH/ memory space. The event type is in the var bind.

Trap No.	Trap Name	Description
19	vlanRouteTableFull5	A vlanRouteTableFull trap occurs when either the IP or IPX route table is full, (discovered on insertion attempt).
20	sapTableFull5	A sapTableFull trap occurs when the IPX SAP table is found to be full on insertion.
21	atmSSCOPstate5	An atmSSCOPstate trap occurs when the signalling state for the specified physical port changes.
22	ilmiState5	An ilmiState trap occurs when the ILMI state for the specified physical port changes.
23	atmConnection5	An atmConnection trap occurs when the specified ATM Vcc is created or deleted.
24	atmService5	An atmService trap occurs when the specified ATM service is created or deleted.
27	dlciNew5	Frame relay Dlci Just Created.
28	dlciDel5	Frame relay Dlci Just Deleted.
29	dlciUp5	Frame relay Dlci Just Changed to Active.
30	dlciDn5	Frame relay Dlci Just Changed to InActive.
31	portManualForwardingMode5	A portManualForwardingMode trap occurs when the specified port is placed into manual mode forwarding as its default setting whenever the port is assigned to a Group that is participating in the IBM spanning tree algorithm.
xylan-9slot-trap.mib (Enterprise 1.3.6.1.4.1.800.3.1.1.2 - omniswitch9)		
1	tempAlarm9	A tempAlarm indicates a temperature sensor has changed its state from underThreshold(4) to overThreshold(3).
2	moduleChange9	A moduleChange trap occurs when a module is inserted or removed from the chassis.
3	powerEvent9	A powerEvent trap occurs when a power supply is inserted or removed from the chassis, or a problem condition is recognized on a power supply.
4	controllerEvent9	A controlEvent trap occurs when a chassis controller (MPM) loses or gains the state of master(3). If this is due to chassis controller being inserted or removed from the slot, a moduleChange trap will also be sent.
5	loginViolation9	A loginViolation trap occurs when a login attempt fails due to an incorrect login ID or password.
6	macVlanViolation9	A macVlanViolation trap occurs when a frame is received from a port with a VLAN ID different from the VLAN where the frame previously has received.
7	macDuplicatePort9	A macDuplicatePort trap occurs when a frame is received from a source port different from the port where the frame previously has received although they both ports belong to the same VLAN.
8	portLinkUpEvent9	A portLinkTrap occurs whenever a phy, log, or virt port is enabled.
9	portLinkDownEvent9	A portLinkTrap occurs whenever a phy, log, or virt port is disabled.

Trap No.	Trap Name	Description
10	portPartitioned9	A portPartioned trap occurs when the physical port has transitioned thru enable/disable states faster than 10 times in the past second. Indicative of a flakey cable.
11	portRecordMismatch9	A portRecordMismatch trap occurs when the specified port data is found to be diferent than the previous configuration. Typically this will be generated when a NIC of one type is swapped out for a different type. IE Ethernet for FDDI, ATM for token-ring, etc.
14	groupChange9	A groupChange trap occurs whenever a group is created or deleted from the system via the UI or SNMP. The group and status code are sent as part of the variable binding. The status codes are: 1 - disable 2 - enable 3 - delete 4 - create 5 - modify (see xylan-vport MIB).
15	vlanChange9	A vlanChange trap occurs whenever a VLAN is created or deleted from the system via the UI or SNMP. The group, vlan and status code are sent as part of the variable binding. See groupChange for the status codes.
16	portMove9	A portMove trap occurs when the specified port is moved from a group/vlan or has had its configuration changed.
17	moduleResetReload9	A moduleResetReload trap occurs when the specified module has been reset or reloaded by the chassis mgr.
18	systemEvent9	A systemEvent trap occurs when a potentially fatal system error occurs. Such as: out of FLASH/ memory space. The event type is in the var bind.
19	vlanRouteTableFull9	A vlanRouteTableFull trap occurs when either the IP or IPX route table is full (discovered on insertion attempt).
20	sapTableFull9	A sapTableFull trap occurs when the IPX SAP table is found to be full on insertion.
21	atmSSCOPstate9	A atmSSCOPstate trap occurs when the signalling state for the specified physical port changes.
22	ilmiState9	A ilmiState trap occurs when the ILMI state for the specified physical port changes.
23	atmConnection9	A atmConnection trap occurs when the specified ATM Vcc is created or deleted.
24	atmService9	A atmService trap occurs when the specified ATM service is created or deleted.
27	dlciNew9	Frame relay Dlci Just Created.
28	dlciDel9	Frame relay Dlci Just Deleted.
29	dlciUp9	Frame relay Dlci Just Changed to Active.
30	dlciDn9	Frame relay Dlci Just Changed to InActive.
31	portManualForwardingMode9	A portManualForwardingMode trap occurs when the specified port is placed into manual mode forwarding as its default setting whenever the port is assigned to a group that is participating in the IBM spanning tree algorithm.

A.22 Nways 8275 Ethernet Desktop Switch

The following table provides a list of source MIBs for the 8275.

Table 41. List of Source MIBs for Nways 8275 Ethernet Desktop Switch

Trap No.	Trap Name	Description
ibm8275.mib (Enterprise 1.3.6.1.4.1.2.6.148 - sw)		
1	hello	A hello trap is sent. When the system re-initializes: it is sent every n minutes (n is defined by the ipAutoDiscoveryInterval object) until an SNMP request is received or until 255 minutes have passed. The hello trap may be disabled by disabling the ipAutoDiscoveryStatus object.
2	swPortAddrSecuViolationEvent	This trap is generated when a port address security violation occurs.
3	swLBridgenewRoot	The swLbnewRoot trap indicates that the sending agent has become the new root of the spanning tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.
4	swLbridgetopologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.
5	swBcastStormAlarmEvent	A swBcastStormAlarmEvent trap is sent by the switch when the broadcast packets exceed the broadcast storm alarm level specified in swPortBcastAlarmLevel.
6	swFanFailureEvent	A fanFailure trap is sent by the switch when the fan of switch device is out of function.
rfc1215.mib		
0	cold start	Emitted when SNMP agent has completed initialization after a reload
1	warm start	Emitted when SNMP agent has completed initialization after a restart
2	link down	Emitted when a router/bridge interface has transitioned out of the “up” state. This may be the result of: - User initiated disable of the interface - Hardware failure - Maintenance traffic communications failure
3	link up	Emitted when a router/bridge interface has transitioned into the up state after passing self-test checks.
4	authentication failure.	Emitted when SNMP agent has received a packet that cannot be properly authenticated. This may be the result of 8271 MIB listing: - Invalid community name string - Invalid origin IP address

A.23 Nways 8282 ATM Workgroup Concentrator

The following table provides a list of source MIBs for the 8282.

Table 42. List of Source MIBs for Nways 8282 ATM Workgroup Concentrator

Trap No.	Trap Name	Description
ibm8282.mib		
		No trap output created.

A.24 Nways 8285 ATM Workgroup Switch

The following table provides a list of source MIBs for the 8285.

Table 43. List of Source MIBs for Nways 8285 ATM Workgroup Switch

Trap No.	Trap Name	Description
ibm8285.mib (Enterprise 1.3.6.1.4.1.6.33 - atmSw)		
1	hello	A hello trap is sent: - When the system re-initializes: it is sent every minutes until an SNMP request is received or until 255 minutes have passed. - When one of the following parameters is changed: -- agent IP address(es) -- agent subnet mask(s) -- ATM address of the IP ARP server -- IP address of the default gateway The value of ifPhysAddress is the ATM address of the hub.The hello trap may be disabled.
2	lock	A lock trap is sent when a set request is rejected because it is suspected that this may cause to break the link between the agent and the manager. This may occur when: - Isolating a slot - Disabling a port if the request is received through this specific port/module/slot.
3	change	A change trap is sent when one of the following MIB variables or group of variables is changed: - Date and Time reset - System Parameters (name, contact, location) changed - Interface changed: -- Administrative State (enabled/disabled) - Module changed: -- Administrative State (isolate/attach) When one of these variable is changed, the lastChange MIB object is also updated with the current date and time. When the Date and Time or the System Parameters changed, the interface number of the hub virtual interface is returned. This trap may be disabled.
4	pvcFailure	A PVC failure trap is sent when a PVC becomes inoperational.
6	callLoggingOverflow	A callLoggingOverflow trap is sent when the call logging table is about to wrap.
7	moduleInstalled	An ATM module has been detected in the hub.
8	moduleRemoved	An ATM module is no longer detected in the hub.

Trap No.	Trap Name	Description
9	lesMaxClientsReached	The maximum number of LAN emulation clients has been connected to the given LAN emulation server.
10	lesMaxClientsThresholdDown	The number of operational clients of the given emulated LAN is now equal to lesMaxNumberOfClients - 10. This trap is sent only if the trap lesMaxClientsReached has been sent previously. lesIndex is the index of the lesConfTable defined above.
102	chassisSlotDown	This trap indicates that a module is down. Usually, this trap is sent when the module has been removed. Sometimes, this trap is sent when management communications with this module have been broken. In this case, it may not be possible to distinguish between a removed and a failed module.
103	chassisSlotUp	This trap indicates that a module is up. Usually, this trap is sent when the module is inserted into the hub. Sometimes, this trap is sent when management communications have been restored to a module where they had previously been broken.
104	chassisEnvironment	A chassisEnvironment trap indicates a change in the concentrator's environment has occurred. The variables supplied indicate what exactly changed.
107	chassisChange	A chassisChange trap is used to indicate that a configuration change has occurred. The actual variables that changed are included in the variables section of the PDU.
116	chassisModuleDown	A chassisModuleDown trap indicates that management communications with a slot has been broken. This event usually occurs when a module has been physically removed from the concentrator. However, it is possible for this event to occur when the particular module fails.
117	chassisModuleUp	A chassisModuleUp trap indicates that management communications with a slot has been established. This event usually occurs when a module has physically been inserted into the concentrator. The variable chipModType indicates the module type inserted.

Appendix B. Microcode Levels Supported by Nways Manager

The following table is the list of Microcode Levels Supported by Nways Manager for AIX v1.2.2 and Nways Workgroup Manager for NT V1.1. For more information please refer to Microcode Levels Supported by Nways Manager for AIX V1.2.1 and Nwyas Workgroup Manager.

Table 44. Microcode Levels Supported by Nways Manager1

Module	Feature Code	Faceplate	Microcode Level	Date
8260 Module Microcode Levels				
Control Point and Switch (8Meg)	FC 5000	A-CPSW	Boot: v2.10 Oper: v2.08 FPGA: 9	05/96
Control Point and Switch (16Meg)	FC 5100 or FC 5000 + MES 5001 FC 5511	A-CPSW	NO PNNI Boot: v2.5.2 Oper: v2.5.2 FPGA: B50 PNNI Boot: v3.1.8 Oper: v3.1.8 FPGA: B52	06/97 06/97 06/97 12/96 03/98 03/98 03/98 09/97
4-Port 100Mbps (MIC)	FC 5004	A4-FB100	FPGA: B50	01/97
4-Port 100Mbps (SC)	FC 5104	A4-SC100	FPGA: B50	01/97
2-Port 155Mbps Flexible Concentration	FC 5002	A2-MB155	FPGA: B50	01/97
3-Port 155Mbps	FC 5003	A3-MB155	FPGA: C31	01/97
8282 12-Port 25Mbps Concentrator	FC 5012	A12-TP25	FPGA: C30	01/97
8281 ATM-TR/Ethernet LAN Bridge	FC 5204	A04MB-BRG	FPGA: B50	01/97
ATM Carrier	FC 5102 FC 5202	A-CMU1 A-CMU2	FPGA: B50	01/97
8210 MSS Server	FC 5300 FC 5400	A-MSS	MSS 2.01 MSS 2.1	01/97
WAN	FC 5302	A2-WAN	FPGA: B50	01/97
WAN 2	FC 5602	A8-WAN	E1/T1/J1: v2.6 E3: v5.2 T3/DS3: v.5.1 OC3: v4.1 STM-1: v4.1 FPGA: C32	02/98 02/98 01/98 01/98 01/98 11/97
1-Port 622 Mbps	FC 5101 FC 5201	A1-MF622 A1-SF622	FPGA: 2D03	01/97
Video Distribution Module	FC 5008	A8-MPEG	Oper: v1.01	04/97
Ethernet 24-Port 10BASE-T Module	FC 1024	E24PS-6	Boot: v1.02 Oper: v1.04	08/95

Module	Feature Code	Faceplate	Microcode Level	Date
Ethernet 36-Port 10BASE-T Module	FC 1036	E36CS-TP	Boot: v1.00 Oper: v1.01	08/95
Ethernet 20/40-Port 10BASE-T Modules	FC 1020 FC 1040	E20PS-TP E40PS-TP	Boot: v1.00 Oper: v1.00	08/95
Ethernet 10-Port 10BASE-FB Modules	FC 1110 FC 1210 FC 1310	E10PS-FB	Boot: v1.00 Oper: v1.05	03/95
Ethernet Flexible Concentration Module	FC 1004	E04M-MOD	Boot: v1.00 Oper: v1.01	06/96
Ethernet Network Interconnect Modules	FC 7106 FC 7206	E06XR	Boot: v1.00 Oper: v1.00	08/95
Ethernet MAC Card	FC 8918	E-MAC	Boot: v1.01 Oper: v3.00	02/97
Ethernet High End MAC Card	FC 8924	HEMAC	Boot: v1.00 Oper: v2.10	02/97
Ethernet Security Card	FC 8915	E-SEC	Boot: v1.00 Oper: v1.01	04/95
Token-Ring 20-Port Passive Media Module	FC 3020	T20MS	Boot: v1.00 Oper: v1.50	10/97
Token-Ring 18-Port Active Per Port-Switching Media Module	FC 3018	T18PSA	Boot: v1.00 Oper: v1.50	10/97
Token-Ring 18-Port Active Per Module-Switching Media Module	FC 3118	T18MSA	Boot: v1.00 Oper: v1.50	10/97
Token-Ring Dual Fiber Repeater Module	FC 3010	T10R-F	Boot: v1.00 Oper: v1.50	10/97
Token-Ring MAC Card	FC 8913	T-MAC	Boot: v2.00 Oper: v4.00 Chip: v4.00	08/97
High End Token-Ring MAC Card	FC 8925	HTMAC	Boot: v1.01 Oper: v2.10 Chip: v1.00	08/97
Token-Ring Jitter Attenuator Card	FC 8914	T-JIT	No Support	n/a
8271 Ethernet LAN Switch Modules	FC 6212 FC 6312	E12-LS2 E12-LS4	V4.0.0 V4.0.0	03/98
8271 ATM/Ethernet LAN Switch Modules	FC 5212 FC 5312	A-E12LS2 A-E12LS4	V4.0.0 V4.0.0	03/98
8271 ATM/Ethernet UFC	FC 6988		V1.14.0	03/98
8272 Token-Ring LAN Switch Modules	FC 6208 FC 6308	TR8-LS2 TR8-LS4	V3.6.1 V3.6.1	03/98
8272 ATM/Token-Ring LAN Switch Modules	FC 5208 FC 5308	A-TR8LS2 A-TR8LS4	V4.0.0 V4.0.0	03/98
8272 ATM/Token-Ring UFC	FC 5076		V1.14.0	03/98

Module	Feature Code	Faceplate	Microcode Level	Date
12/24-Port 10BASE-T Switching Modules	FC 7312 FC 7324	SWE12-TP SWE24-TP	Boot: v1.12 Oper: v2.00	11/97
10/20-Port 10BASE-FB/FL Switching Modules	FC 7310 FC 7320	SWE10-F SWE20-F	Boot: v1.12 Oper: v2.00	11/97
12-Port 10BASE-T and DAS FDDI Switching Module	FC 7314	SWE12F2-TPF	Boot: v1.12 Oper: v2.00	11/97
10-Port 10BASE-FB/FL and DAS FDDI Switching Module	FC 7412	SWE10F2-FF	Boot: v1.12 Oper: v2.00	11/97
4-Port DAS FDDI Switching Module	FC 7304	SWF4-F	Boot: v1.12 Oper: v2.00	11/97
4-Port 100BASE-Tx Switching Module	FC 7504	SWE4-TX	Boot: v1.12 Oper: v2.00	11/97
4-Port 100BASE-Fx Switching Module	FC 7404	SWE4-FX	Boot: v1.12 Oper: v2.00	11/97
LAN Access Switching Module	FC 7016	SWE16-TP	Boot: v1.12 Oper: v2.00	11/97
PacketChannel/ATM Switching Module	FC 7302	SWA2-MOD	Boot: v2.02 Oper: v2.00	11/97
24-Port Telco FDDI Switching Module	FC 7524	SWA24-T	Boot: v2.02 Oper: v2.00	11/97
Distributed Management Module	FC 1000	DMM	Boot: v1.01 Oper: v2.30	01/96
Distributed Management Module with Ethernet Carrier	FC 1100	EC-DMM	Boot: v1.01 Oper: v2.30	01/96
Distributed Management Module	FC 1200	DMM	Boot: v1.03 Oper: v5.10	08/97
Distributed Management Module with Ethernet Carrier	FC 1300	EC-DMM	Boot: v1.03 Oper: v5.10	08/97
Advanced DMM/Controller Module	FC 1700	DMM-CTLR	DMM: Boot: v1.03 Oper: v5.10 Controller: Boot: v1.03 Oper: v1.14	08/97
Redundant Controller Module	FC 8000	8000-RCTL	Boot: v1.03 Oper: v1.14	08/97
ATM Hardware Microcode Levels				
ATM Bridge	FC 8281	8281	IBM LANE: V1.16 ATM Forum: V2.4	09/96 06/97

Module	Feature Code	Faceplate	Microcode Level	Date
ATM Concentrator	FC 8282	8282	V10.1	10/96
MSS Server	FC 8210	8210	MSS 2.01 MSS 2.1	01/97
8265 Hardware Microcode Levels				
3-Port 155Mbps Flexible Concentration	5003	A3-MB 155	C31	
2-Port 155Mbps Flexible Concentration	5002	A2-MB 155	B50	
4-Port 100Mbps (SC)	5104	A4-SC100	B50	
MSS Server Module	5300	A-MSS	MSS 2.01 MSS 2.1	
8281 TR/Ethernet LAN Bridge	5204	A04MB-BRG	B50	
8282 12-Port 25Mbps Concentrator	5012	A12-TP25	C30	
8272 ATM/Token-Ring LAN Switch Modules	5208/5308	A-TR8LS2 / A-TR8LS4	See 8260 chart	
8271 ATM/Ethernet LAN Switch Modules	5212/5312	A-E12LS2 / A-E12LS4	See 8260 chart	
ATM WAN 2 Module	5602	A8-WAN	C32	
ATM WAN Module	5302	A2-WAN	B50	
Video Distribution Module	5008	A8-MPEG	B50	
Control Point/Switch Module TFTP Download Packages And PCMCIA Images 6501	CPSW	Boot: v.3.3.0 Oper: v.3.3.0 FPGA: 1D12 MIB: v.2.3	03/98	
155 Mbps 4P Flex Module	6543	A4-MB155	2D03	02/98
155 Mbps 4P MMF Integrated Module	6540	A4-MF155	2D03	02/98
622 Mbps 1P MMF Module	6511	A1-MF622	2D03	02/98
622 Mbps 1P SMF Module	6512	A1-SF622	2D03	02/98
8285 Hardware Microcode Levels				
Base Unit			No PNNI Boot: v1.5.2 Oper: v1.5.2 FPGA: C30 PNNI Boot: v3.18 Oper: v3.18 FPGA: C32 MIB v.2.1	06/97 01/97 03/98 01/98 03/98
ATM 4-Port 100Mbps Module (MIC)	FC 5004	A4-FB100	FPGA: B50	01/97
4-Port 100Mbps (SC)	FC 5104	A4-SC100	FPGA: B50	01/97

Module	Feature Code	Faceplate	Microcode Level	Date
2-Port 155Mbps Flexible Concentration	FC 5002	A2-MB155	FPGA: B50	01/97
3-Port 155Mbps	FC 5003	A3-MB155	FPGA: C31	01/97
12-Port 25Mbps Concentration	FC 5012	A12-TP25	FPGA: C30	01/97
TR/Ethernet LAN Bridge	FC 5204	A04MB-BRG	IBM LANE: Oper: v1.16 ATM Forum: Oper: v2.3 FPGA: B50	10/96 06/97 01/97
ATM Carrier	FC 5102 FC 5202	A-CMU1 A-CMU2	FPGA: B50	01/97
WAN	FC 5302	A2-WAN	FPGA: B50	01/97
WAN 2	FC 5602	A8-WAN	FPGA: B50	01/97
Switch Hardware Microcode Levels				
Ethernet Switch	FC 8270-800	8270	V4.0B	03/98
Ethernet Switch	FC 8271-001	8271	V1.1.0	03/98
Ethernet Switch	FC 8271-108 ,216	8271	V4.0.0	03/98
Ethernet Switch	FC 8271-524 ,624	8271	V3.10	03/98
Ethernet Switch	FC 8271-612 ,712	8271	V3.10	03/98
Token-Ring Switch	FC 8272-108 ,216	8272	V4.0.0	03/98
ATM Switch UFC for 8270,8271,8272	FC ???	ATM	V1.14.0	03/98
ATM Switch UFC for 8271-524,624,612,712	FC ???	ATM	V1.05	03/98
Ethernet RouteSwitch	FC 8273	8273	V3.16	04/98
LAN RouteSwitch	FC 8274	8274	V3.16	04/98
Ethernet RoutePort	FC 8276	8276	V1.04	01/98
Token-Ring CMOL and FDDI Proxy Agent Hardware Microcode Levels				
LNM OS/2 Proxy Agent	FC	OS/2 2.0	V2.05 CSD UR46843 or greater with TCP/IP for OS/2 PTF UN64092	05/96
Token-Ring Concentrator	FC 8230-001 ,002 003,013 ,213	8230	V2.4	01/97

Module	Feature Code	Faceplate	Microcode Level	Date
Token-Ring Concentrator	FC 8230-4A ,4P	8230	V2.4	01/97
FDDI Concentrator and OS/2 Proxy Agent	FC 8240 or FC 8244	8240 8244	V6.4 TCP/IP PTF UN64092	01/97
DOS Bridge	FC	n/a	V2.24	01/97
Token-Ring/Ethernet Bridge	FC 8229	8229	V2.2	04/97
OS/2 RoutXpander	FC	n/a	V2.04 PTF IP20456	01/97
Concentrator Hardware Microcode Levels				
10BaseT Ethernet	FC 8224	8224	V1.31	08/96
100BaseT Ethernet	FC 8225-002 8225-003	8225	V119 V126	08/96
Token-Ring	FC 8230-003 ,013,213	8230	V5.32	08/96
Token-Ring	FC 8230-04A ,04P	8230	V1.1.3	12/96
Ethernet Stackable	FC 8237-001 ,002,003	8237	V1108 V2112 V3127	09/97
Token-Ring Stackable	FC 8238	8238	V1.15	04/98
Router/Remote Access Hardware Microcode Levels				
Remote Access	FC 8235-001 ,002 011,012 021,022 031 ,032 051,052	8235	V4.54	03/97
Remote Access	FC 8235-I40	8235	V4.53	03/97
2210 Router	FC 2210	2210	MRS 2.0 MRS 2.1 MRS 2.2 MRS 3.1	03/98
6611 Router	FC 6611	6611	MPNP V1R3	06/97
2216 Router	FC 2216-400	2216	MAS V1R1.1 MAS V2R1.0 MAS V3R1.0 MAS V3R2.0	01/97
8210 MSS Server	FC 8210-001 FC 8210-002	8210	MSS 1.1 MSS 2.01 MSS 2.1	01/97
DMI Adapter Microcode Levels				
Turbo 16/4 ISA	FC	85H3628	NT:1.31 OS/2:1.30	03/98

Module	Feature Code	Faceplate	Microcode Level	Date
16/4 PCI	FC	75H9800	NT:1.31 OS/2:1.30	03/98
16/4 PCI WOL	FC	86H1886	NT:1.3 OS/2:1.30	03/98
Turbo 16/4 PCMCIA Card	FC	85H3628	NT:1.31 OS/2:1.30	03/98
100/10 EtherJet PCI	FC	86H2432	NT:1.31 OS/2:1.30	03/98
100/10 EtherJet PCI WOL	FC	86H2432	NT:1.31 OS/2:1.30	03/98

Appendix C. Java Performance MIBS

This appendix contains all the defined MIB values for the JPM.

Table 45. Default Performance Objects Defined for JPM

Performance Objects	Expression	Unit
Interface Utilization	((((r 1.3.6.1.2.1.2.2.1.10.* + r 1.3.6.1.2.1.2.2.1.16.*) * 8) / (1.3.6.1.2.1.2.2.1.5.*) * 2) * 100)	Percent
Interface Good Input Pkts	(r 1.3.6.1.2.1.2.2.1.11.* + r 1.3.6.1.2.1.2.2.1.12.*)	Packets/Second
Interface Bad Input Pkts	(r 1.3.6.1.2.1.2.2.1.14.* + r 1.3.6.1.2.1.2.2.1.15.*)	Packets/Second
Interface Discarded Input Pkts	(r 1.3.6.1.2.1.2.2.1.13.*)	Packets/Second
Interface Good Output Pkts	(r 1.3.6.1.2.1.2.2.1.17.* + r 1.3.6.1.2.1.2.2.1.18.* - r 1.3.6.1.2.1.2.2.1.19.* - r 1.3.6.1.2.1.2.2.1.20.*)	Packets/Second
Interface Bad Output Pkts	(r 1.3.6.1.2.1.2.2.1.20.*)	Packets/Second
Interface Discarded Output Pkts	(r 1.3.6.1.2.1.2.2.1.19.*)	Packets/Second
Interface Unicast Input Pkts	(r 1.3.6.1.2.1.2.2.1.11.*)	Packets/Second
Interface Multicast Input Pkts	(r 1.3.6.1.2.1.31.1.1.1.2.*)	Packets/Second
Interface Broadcast Input Pkts	(r 1.3.6.1.2.1.31.1.1.1.3.*)	Packets/Second
Interface Unicast Output Pkts	(r 1.3.6.1.2.1.2.2.1.17.*)	Packets/Second
Interface Multicast Output Pkts	(r 1.3.6.1.2.1.31.1.1.1.4.*)	Packets/Second
Interface Broadcast Output Pkts	(r 1.3.6.1.2.1.31.1.1.1.5.*)	Packets/Second
IInput Pkts	(r 1.3.6.1.2.1.4.3.0 - r 1.3.6.1.2.1.4.6.0)	Packets/Second
IOutput Pkts	(r 1.3.6.1.2.1.4.10.0)	Packets/Second
IForwarded Pkts	(r 1.3.6.1.2.1.4.6.0)	Packets/Second
IGood Input Pkts	(r 1.3.6.1.2.1.4.9.0 + r 1.3.6.1.2.1.4.6.0 - r 1.3.6.1.2.1.4.11.0 - r 1.3.6.1.2.1.4.12.0)	Packets/Second
IBad Input Pkts	(r 1.3.6.1.2.1.4.4.0 + r 1.3.6.1.2.1.4.5.0 + r 1.3.6.1.2.1.4.7.0)	Packets/Second
IDiscarded Input Pkts	(r 1.3.6.1.2.1.4.8.0)	Packets/Second
IGood Output Pkts	(r 1.3.6.1.2.1.4.6.0 + r 1.3.6.1.2.1.4.10.0 - r 1.3.6.1.2.1.4.11.0 - r 1.3.6.1.2.1.4.12.0)	Packets/Second
IBad Output Pkts	(r 1.3.6.1.2.1.4.12.0)	Packets/Second
IDiscarded Output Pkts	(r 1.3.6.1.2.1.4.11.0)	Packets/Second
SNMInput Queries	(r 1.3.6.1.2.1.11.1.0)	Packets/Second
SNMOutput Traps	(r 1.3.6.1.2.1.11.29.0)	Packets/Second
SNMNo Authority Queries	(d 1.3.6.1.2.1.11.4.0)	Packets
SNMBad Authority Queries	(d 1.3.6.1.2.1.11.5.0)	Packets
AAL5 VCC CRC Errors	(d 1.3.6.1.2.1.37.1.12.1.3.*)	Errors

Performance Objects	Expression	Unit
AAL5 VCC Reassembly Timeouts	(d 1.3.6.1.2.1.37.1.12.1.4.*)	Errors
AAL5 VCC SDUs Too Large	(d 1.3.6.1.2.1.37.1.12.1.5.*)	Errors
ATM OCD Events	(d 1.3.6.1.2.1.37.1.4.1.1.*)	Events
Frame Relay Input Traffic	(r 1.3.6.1.2.1.10.32.2.1.9.*)	Octets/Second
Frame Relay Output Traffic	(r 1.3.6.1.2.1.10.32.2.1.7.*)	Octets/Second
Frame Relay Forward Congestion	(d 1.3.6.1.2.1.10.32.2.1.4.*)	Events
Frame Relay Backward Congestion	(d 1.3.6.1.2.1.10.32.2.1.5.*)	Events
X.25 Input Circuit Traffic	(r 1.3.6.1.2.1.10.5.5.1.6.*)	Octets/Second
X.25 Output Circuit Traffic	(r 1.3.6.1.2.1.10.5.5.1.11.*)	Octets/Second
X.25 Calls Successful	(d 1.3.6.1.2.1.10.5.3.1.11.* - d 1.3.6.1.2.1.10.5.3.1.12.*)	Calls
X.25 Calls Failed	(d 1.3.6.1.2.1.10.5.3.1.12.*)	Calls
Token-Ring Hard Errors	(d 1.3.6.1.2.1.10.9.2.1.10.*)	Errors
Token-Ring Soft Errors	(d 1.3.6.1.2.1.10.9.2.1.11.*)	Errors
Token-Ring Station Congestion	(d 1.3.6.1.2.1.10.9.2.1.8.*)	Events
Ethernet Media Busy Delays	(d 1.3.6.1.2.1.10.7.2.1.7.*)	Events
Ethernet Excessive Collisions	(d 1.3.6.1.2.1.10.7.2.1.9.*)	Events
Ethernet Collision Frequencies	(d 1.3.6.1.2.1.10.7.5.1.3.*)	Frequency
ISDN Incoming Calls Connected	(d 1.3.6.1.2.1.10.20.1.3.3.1.2.*)	Calls
ISDN Incoming Calls Not Connected	(d 1.3.6.1.2.1.10.20.1.3.3.1.1.* - d 1.3.6.1.2.1.10.20.1.3.3.1.2.*)	Calls
ISDN Outgoing Calls Connected	(d 1.3.6.1.2.1.10.20.1.3.3.1.4.*)	Calls
ISDN Outgoing Calls Not Connected	(d 1.3.6.1.2.1.10.20.1.3.3.1.3.* - d 1.3.6.1.2.1.10.20.1.3.3.1.4.*)	Calls
ISDN Charged Units	(d 1.3.6.1.2.1.10.20.1.3.3.1.5.*)	Charged Units
ISDN LAPD Peer-Initiated New Connections	(d 1.3.6.1.2.1.10.20.1.3.4.1.3.*)	Connections
ISDN LAPD Framing Errors	(d 1.3.6.1.2.1.10.20.1.3.4.1.4.*)	Connections
SDLC Port Input IFrames	(r 1.3.6.1.2.1.41.1.1.3.1.10.*)	Frames/Second
SDLC Port Output IFrames	(r 1.3.6.1.2.1.41.1.1.3.1.11.*)	Frames/Second
SDLC Port Physical Failures	(d 1.3.6.1.2.1.41.1.1.3.1.1.*)	Failures
SDLC Link Station Traffic	(r 1.3.6.1.2.1.41.1.2.3.1.3.* + r 1.3.6.1.2.1.41.1.2.3.1.4.*)	Octets/Second
Bridge Excessive Delay Discards	(d 1.3.6.1.2.1.17.1.4.1.4.*)	Discards
Bridge Transparent Input Frames	(r 1.3.6.1.2.1.17.4.4.1.3.*)	Frames/Second
Bridge Transparent Output Frames	(r 1.3.6.1.2.1.17.4.4.1.4.*)	Frames/Second

Performance Objects	Expression	Unit
Bridge Transparent Forwarding Database Discards	(r 1.3.6.1.2.1.17.4.1.0)	Discards
Bridge Transparent Input Frames Discarded	(d 1.3.6.1.2.1.17.4.4.1.5.*)	Frames
Bridge Source Route Input Frames	(r 1.3.6.1.2.1.17.3.1.1.8.*)	Frames/Second
Bridge Source Route Output Frames	(r 1.3.6.1.2.1.17.3.1.1.9.*)	Failures
AppleTalk Input Datagrams	(r 1.3.6.1.2.1.13.4.1.0)	Datagrams/Second
AppleTalk Output Datagrams	(r 1.3.6.1.2.1.13.4.6.0)	Datagrams/Second
AppleTalk Forwarded Datagrams	(r 1.3.6.1.2.1.13.4.5.0)	Datagrams/Second
AppleTalk No Protocol Handler Drops	(d 1.3.6.1.2.1.13.4.7.0)	Errors
AppleTalk No Route Drops	(d 1.3.6.1.2.1.13.4.8.0)	Errors
AppleTalk Too Short Errors	(d 1.3.6.1.2.1.13.4.9.0)	Errors
AppleTalk Too Long Errors	(d 1.3.6.1.2.1.13.4.10.0)	Errors
AppleTalk Broadcast Errors	(d 1.3.6.1.2.1.13.4.11.0)	Errors
AppleTalk Short DDErrors	(d 1.3.6.1.2.1.13.4.12.0)	Errors
AppleTalk HoCount Errors	(d 1.3.6.1.2.1.13.4.13.0)	Errors
AppleTalk Checksum Errors	(d 1.3.6.1.2.1.13.4.14.0)	Errors
TR MAC Octets	(r 1.3.6.1.2.1.16.1.2.1.4.*)	Packets/Second
TR MAC DroEvents	(r 1.3.6.1.2.1.16.1.2.1.3.*)	Events/Second
TR MAC Ring Purge Events	(r 1.3.6.1.2.1.16.1.2.1.6.*)	Events/Second
TR MAC Beacon Events	(r 1.3.6.1.2.1.16.1.2.1.8.*)	Events/Second
TR MAC Claim Token Events	(r 1.3.6.1.2.1.16.1.2.1.11.*)	Events/Second
TR MAC NAUN Changes	(r 1.3.6.1.2.1.16.1.2.1.13.*)	Events/Second
TR MAC Poll Events	(r 1.3.6.1.2.1.16.1.2.1.25.*)	Events/Second
TR MAC Pkts	(r 1.3.6.1.2.1.16.1.2.1.5.*)	Packets/Second
TR MAC Ring Purge Pkts	(r 1.3.6.1.2.1.16.1.2.1.7.*)	Packets/Second
TR MAC Beacon Pkts	(r 1.3.6.1.2.1.16.1.2.1.10.*)	Packets/Second
TR MAC Claim Token Pkts	(r 1.3.6.1.2.1.16.1.2.1.12.*)	Packets/Second
TR MAC Line Errors	(r 1.3.6.1.2.1.16.1.2.1.14.*)	Errors/Second
TR MAC Internal Errors	(r 1.3.6.1.2.1.16.1.2.1.15.*)	Errors/Second
TR MAC Burst Errors	(r 1.3.6.1.2.1.16.1.2.1.16.*)	Errors/Second
TR MAC AC Errors	(r 1.3.6.1.2.1.16.1.2.1.17.*)	Errors/Second
TR MAC Abort Errors	(r 1.3.6.1.2.1.16.1.2.1.18.*)	Errors/Second
TR MAC Lost Frame Errors	(r 1.3.6.1.2.1.16.1.2.1.19.*)	Errors/Second

Performance Objects	Expression	Unit
TR MAC Congestion Errors	(r 1.3.6.1.2.1.16.1.2.1.20.*)	Errors/Second
TR MAC Frame Copied Errors	(r 1.3.6.1.2.1.16.1.2.1.21.*)	Errors/Second
TR MAC Frequency Errors	(r 1.3.6.1.2.1.16.1.2.1.22.*)	Errors/Second
TR MAC Token Errors	(r 1.3.6.1.2.1.16.1.2.1.23.*)	Errors/Second
TR MAC Soft Error Reports	(r 1.3.6.1.2.1.16.1.2.1.25.*)	Errors/Second
TR Prom DroEvents	(r 1.3.6.1.2.1.16.1.3.1.3.*)	Events/Second
TR Prom Data Util	((r 1.3.6.1.2.1.16.1.3.1.4.* * 8) / (1.3.6.1.2.1.2.2.1.5.*))	Percent
TR Prom Data Pkts	(r 1.3.6.1.2.1.16.1.3.1.5.*)	Packets/Second
TR Prom Data Broadcast Pkts	(r 1.3.6.1.2.1.16.1.3.1.6.*)	Packets/Second
TR Prom Data Multicast Pkts	(r 1.3.6.1.2.1.16.1.3.1.7.*)	Packets/Second
TR Prom 18-63 Octets	(r 1.3.6.1.2.1.16.1.3.1.8.*)	Packets/Second
TR Prom 64-127 Octets	(r 1.3.6.1.2.1.16.1.3.1.9.*)	Packets/Second
TR Prom 128-255 Octets	(r 1.3.6.1.2.1.16.1.3.1.10.*)	Packets/Second
TR Prom 256-511 Octets	(r 1.3.6.1.2.1.16.1.3.1.11.*)	Packets/Second
TR Prom 512-1023 Octets	(r 1.3.6.1.2.1.16.1.3.1.12.*)	Packets/Second
TR Prom 1024-2047 Octets	(r 1.3.6.1.2.1.16.1.3.1.13.*)	Packets/Second
TR Prom 2048-4095 Octets	(r 1.3.6.1.2.1.16.1.3.1.14.*)	Packets/Second
TR Prom 4096-8191 Octets	(r 1.3.6.1.2.1.16.1.3.1.15.*)	Packets/Second
TR Prom 8192-18000 Octets	(r 1.3.6.1.2.1.16.1.3.1.16.*)	Packets/Second
TR Prom > 18000 Octets	(r 1.3.6.1.2.1.16.1.3.1.17.*)	Packets/Second
Ethernet Utilization	((r 1.3.6.1.2.1.16.1.1.1.4.* * 8) / (1.3.6.1.2.1.2.2.1.5.*))	Percent
Ethernet Pkts	(r 1.3.6.1.2.1.16.1.1.1.5.*)	Packets/Second
Ethernet Broadcast Pkts	(r 1.3.6.1.2.1.16.1.1.1.6.*)	Packets/Second
Ethernet Multicast Pkts	(r 1.3.6.1.2.1.16.1.1.1.7.*)	Packets/Second
Ethernet DroEvents	(r 1.3.6.1.2.1.16.1.1.1.3.*)	Events/Second
Ethernet CRC Alignment Errors	(r 1.3.6.1.2.1.16.1.1.1.8.*)	Errors/Second
Ethernet Undersize Pkts	(r 1.3.6.1.2.1.16.1.1.1.9.*)	Errors/Second
Ethernet Oversize Pkts	(r 1.3.6.1.2.1.16.1.1.1.10.*)	Packets/Second
Ethernet Fragments	(r 1.3.6.1.2.1.16.1.1.1.11.*)	Events/Second
Ethernet Jabbers	(r 1.3.6.1.2.1.16.1.1.1.12.*)	Events/Second
Ethernet Collisions	(r 1.3.6.1.2.1.16.1.1.1.13.*)	Packets/Second
Ethernet 64 Octets	(r 1.3.6.1.2.1.16.1.1.1.14.*)	Packets/Second

Performance Objects	Expression	Unit
Ethernet 65-127 Octets	(r 1.3.6.1.2.1.16.1.1.1.15.*)	Packets/Second
Ethernet 128-255 Octets	(r 1.3.6.1.2.1.16.1.1.1.16.*)	Packets/Second
Ethernet 256-511 Octets	(r 1.3.6.1.2.1.16.1.1.1.17.*)	Packets/Second
Ethernet 512-1023 Octets	(r 1.3.6.1.2.1.16.1.1.1.18.*)	Packets/Second
Ethernet 1024-1518 Octets	(r 1.3.6.1.2.1.16.1.1.1.19.*)	Packets/Second
Token-Ring Hard Errors	(d 1.3.6.1.2.1.10.9.2.1.10.*)	Errors
Token-Ring Soft Errors	(d 1.3.6.1.2.1.10.9.2.1.11.*)	Errors
Token-Ring Congestion Failures	(d 1.3.6.1.2.1.10.9.2.1.8.*)	Failures
BGInput Messages	(r 1.3.6.1.2.1.15.3.1.12.*)	Messages/Second
BGOutput Messages	(r 1.3.6.1.2.1.15.3.1.13.*)	Messages/Second
HeaMemory Utilization	(((1.3.6.1.4.1.1.6.1.1.1.4.0 + 1.3.6.1.4.1.1.6.1.1.1.5.0) / (1.3.6.1.4.1.1.6.1.1.1.1.0)) * 100)	Percent
Memory Buffer Utilization	(((1.3.6.1.4.1.1.6.1.2.1.2.0) / (1.3.6.1.4.1.1.6.1.2.1.1.0)) * 100)	Percent
Escon Output Data Pkts	(r 1.3.6.1.4.1.2.5.17.3.1.1.13.*)	Packets/Second
Escon Data Pkts Acknowledged	(((d 1.3.6.1.4.1.2.5.17.3.1.1.16.*) / (d 1.3.6.1.4.1.2.5.17.3.1.1.13.*)) * 100)	Percent
Iover ATM Logical Subnet Active SVCs	(1.3.6.1.3.78.1.2.1.12.*)	SVCs
IPX Input Pkts	(r 1.3.6.1.4.1.23.2.5.1.1.1.11.*)	Packets/Second
IPX Output Pkts	(r 1.3.6.1.4.1.23.2.5.1.1.1.13.*)	Packets/Second
IPX Forwarded Pkts	(r 1.3.6.1.4.1.23.2.5.1.2.1.8.*)	Packets/Second
IPX Input Pkts Filtered	(d 1.3.6.1.4.1.23.2.5.1.2.1.5.*)	Packets
IPX Output Pkts Filtered	(d 1.3.6.1.4.1.23.2.5.1.2.1.9.*)	Packets
IPX Circuit Delay	(1.3.6.1.4.1.23.2.5.2.1.1.25.*)	Milliseconds
OSPF Interface Events	(d 1.3.6.1.2.1.14.7.1.15.*)	Events
OSPF Virtual Interface Events	(d 1.3.6.1.2.1.14.9.1.8.*)	Events
OSPF Neighbor Events	(d 1.3.6.1.2.1.14.10.1.7.*)	Events
OSPF Virtual Neighbor Events	(d 1.3.6.1.2.1.14.11.1.6.*)	Events
NHRPositive Resolution Replies	(((d 1.3.6.1.3.9999.1.2.3.1.2.*) / (d 1.3.6.1.3.9999.1.2.3.1.1.*)) * 100)	Percent
NHRError Indication Packets Sent	(d 1.3.6.1.3.9999.1.2.3.1.14.*)	Packets
NHRAvailable Clients Registered	(((1.3.6.1.3.9999.1.3.1.1.9.*) / (1.3.6.1.3.9999.1.3.1.1.10.*)) * 100)	Percent
Ethernet MARepeater Available State Exits	(d 1.3.6.1.2.1.26.1.1.1.7.*)	Exits

Performance Objects	Expression	Unit
Ethernet MAInterface Available State Exits	(d 1.3.6.1.2.1.26.2.1.1.6.*)	Exits
Ethernet Repeater Port Readable Octets	(r 1.3.6.1.2.1.22.2.3.1.1.4.*)	Octets/Second
Ethernet Repeater Port Errors	(d 1.3.6.1.2.1.22.2.3.1.1.15.*)	Errors
LLC Port Physical Failures	(d 1.3.6.1.3.51.1.1.3.1.1.*)	Failures
LLC Link Station Input Octets	(r 1.3.6.1.3.51.1.1.3.3.1.5.*)	Octets/Second
LLC Link Station Output Octets	(r 1.3.6.1.3.51.1.1.3.3.1.6.*)	Octets/Second
LEC Output Pkts	(r 1.3.6.1.4.1.353.5.3.1.1.4.1.1.* + r 1.3.6.1.4.1.353.5.3.1.1.4.1.3.* + r 1.3.6.1.4.1.353.5.3.1.1.4.1.5.*)	Packets/Second
LEC Input Pkts	(r 1.3.6.1.4.1.353.5.3.1.1.4.1.2.* + r 1.3.6.1.4.1.353.5.3.1.1.4.1.4.* + r 1.3.6.1.4.1.353.5.3.1.1.4.1.6.*)	Packets/Second
LEC SVC Failures	(d 1.3.6.1.4.1.353.5.3.1.1.4.1.7.*)	Failures
LES Successful Join Responses	(d 1.3.6.1.4.1.353.5.3.3.2.1.1.1.*)	Responses
LES Registration Failures	(d 1.3.6.1.4.1.353.5.3.3.2.1.1.12.*)	Failures
LES ARAccepted	(r 1.3.6.1.4.1.353.5.3.3.2.1.1.13.*)	Packets/Second
LES ARForwarded	(r 1.3.6.1.4.1.353.5.3.3.2.1.1.14.*)	Packets/Second
LES LEC Input Requests	(r 1.3.6.1.4.1.353.5.3.3.3.1.1.1.*)	Packets/Second
LES LEC Output Pkts	(r 1.3.6.1.4.1.353.5.3.3.3.1.1.3.*)	Packets/Second
BUS Input Octets	(r 1.3.6.1.4.1.353.5.3.4.2.1.1.2.*)	Octets/Second
BUS Unicast Input Frames	(r 1.3.6.1.4.1.353.5.3.4.2.1.1.3.*)	Frames/Second
BUS Multicast Input Frames	(r 1.3.6.1.4.1.353.5.3.4.2.1.1.4.*)	Frames/Second
BCM Octets Returned To BUS	(r 1.3.6.1.4.1.2.6.118.1.2.1.3.2.1.1.4.*)	Octets/Second
BCM Octets Discarded	(r 1.3.6.1.4.1.2.6.118.1.2.1.3.2.1.1.6.*)	Octets/Second
BCM Octets Transmitted	(r 1.3.6.1.4.1.2.6.118.1.2.1.3.2.1.1.8.*)	Octets/Second
BCM Octets In Error	(r 1.3.6.1.4.1.2.6.118.1.2.1.3.2.1.1.10.*)	Octets/Second
APPN Link Station Delay	(1.3.6.1.2.1.34.4.1.1.5.1.1.25.*)	Milliseconds
APPN Directory Services Cache Used	(((1.3.6.1.2.1.34.4.1.4.1.2.0) / (1.3.6.1.2.1.34.4.1.4.1.1.0)) * 100)	Percent
APPN Directory Services Locates Received	(d 1.3.6.1.2.1.34.4.1.4.1.5.0 + d 1.3.6.1.2.1.34.4.1.4.1.6.0)	Locates
APPN Directory Services Locates Not Found	(d 1.3.6.1.2.1.34.4.1.4.1.9.0 + d 1.3.6.1.2.1.34.4.1.4.1.10.0)	Locates
APPN Directory Services Locates Outstanding	(1.3.6.1.2.1.34.4.1.4.1.11.0)	Locates
APPN HPR RTSend Rate	(1.3.6.1.2.1.34.6.1.4.2.1.18.*)	Bytes/Second

Performance Objects	Expression	Unit
APPN NALResponse Time Average	(1.3.6.1.2.1.34.1.3.1.1.19.*)	1/10th Seconds
APPN APPC LActive Sessions	(1.3.6.1.2.1.34.1.2.2.1.11.*)	Sessions
DLSw TConn Input Octets	(r 1.3.6.1.2.1.46.1.2.3.1.23.*)	Octets/Second
DLSw TConn Output Octets	(r 1.3.6.1.2.1.46.1.2.3.1.24.*)	Octets/Second
TN3270RsTime 1	(d 1.3.6.1.2.1.34.9.1.2.1.14.*)	Transactions
TN3270RsTime 2	(d 1.3.6.1.2.1.34.9.1.2.1.15.*)	Transactions
TN3270RsTime 3	(d 1.3.6.1.2.1.34.9.1.2.1.16.*)	Transactions
TN3270RsTime 4	(d 1.3.6.1.2.1.34.9.1.2.1.17.*)	Transactions
TN3270RsTime 5	(d 1.3.6.1.2.1.34.9.1.2.1.18.*)	Transactions
BRS Bytes Transmitted	(r 1.3.6.1.4.1.1.1.7.1.1.3.1.4.*)	Bytes/Second
BRS Bytes Discarded	(d 1.3.6.1.4.1.1.1.7.1.1.3.1.6.*)	Bytes
CPUtilization	(1.3.6.1.4.1.2.6.4.5.1.0)	Percent
APPN Memory Utilization	(1.3.6.1.4.1.2.6.2.13.1.7.2.0 / 1.3.6.1.4.1.2.6.2.13.1.7.1.0)	Percent
8275 Unknown Unicast Pkts	(d 1.3.6.1.4.1.2.6.148.3.1.5.1.0)	Packets
8275 Unknown Multicast Pkts	(d 1.3.6.1.4.1.2.6.148.3.1.5.2.0)	Packets
8275 Secured Violations	(d 1.3.6.1.4.1.2.6.148.3.1.5.3.0)	Violations
8275 Input Octets	(r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.1.*)	Octets/Second
8275 Filtered Input Pkts	(d 1.3.6.1.4.1.2.6.148.3.1.5.4.1.3.*)	Packets
8275 Overrun Input Pkts	(d 1.3.6.1.4.1.2.6.148.3.1.5.4.1.4.*)	Packets
8275 Output Octets	(r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.5.*)	Octets/Second
8275 Ucast Output Pkts	(r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.6.* - r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.7.* - r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.8.* - r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.9.*)	Packets/Second
8275 Bcast Output Pkts	(r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.7.*)	Packets/Second
8275 Mcast Output Pkts	(r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.8.*)	Packets/Second
8275 Bad Output Pkts	(r 1.3.6.1.4.1.2.6.148.3.1.5.4.1.9.*)	Packets/Second
8245 GrouError Pkts	(((d 1.3.6.1.2.1.22.2.2.1.1.4.*) / (d 1.3.6.1.2.1.22.2.2.1.1.2.*)) * 100)	Percent
8245 Port Error Pkts	(((d 1.3.6.1.2.1.22.2.3.1.1.15.*) / (d 1.3.6.1.2.1.22.2.3.1.1.3.*)) * 100)	Percent

Appendix D. Special Notices

This publication is intended to help service professionals to implement the Nways Management applications. The information in this publication is not intended as the specification of any programming interfaces that are provided by Nways or Tivoli applications. See the PUBLICATIONS section of the IBM Programming Announcements for Nways Campus Manager and Tivoli NetView 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.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

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:

IBM ®
NetView
DB2
AIX
Nways Campus Manager

The following terms are trademarks of other companies:

TIvoli Systems Incorporated, TME 10, Tivoli Management Environment are trademarks of Tivoli Systems, an IBM Company.

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.

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 E. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

E.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 421.

- *Understanding and Using MSS Release 1.1 and 2.0*, SG24-2115
- *IBM Nways RouteSwitch Implementation Guide,* SG24-4881
- *Campus ATM Configuration Examples*, SG24-2126

E.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
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

E.3 Other Publications

These publications are also relevant as further information sources:

- *Nways Manager for AIX Version 1.2.2*, SK2T-0420
- *Nways Campus Manager Remote Monitor For AIX, Version 2,* G325-3631
- *Nways Workgroup Manager for Windows NT User’s Guide,* SA27-4194
- *Nways Workgroup Manager and Remote Monitor for Windows NT,* SK2T-0417
- *Nways Campus Manager LAN for AIX, Version 3*, 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:

- **Redbooks Web Site on the World Wide Web**

  `http://w3.itso.ibm.com/`

- **PUBORDER** – to order hardcopies in the United States
- **Tools Disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLCAT REDPRINT
  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 the following command:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1998
  ```

- **REDBOOKS Category on INEWS**
- **Online** – send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL

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.html`). 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 Publications Customer Support P.O. Box 29570 Raleigh, NC 27626-0570 USA	IBM Publications 144-4th Avenue, S.W. Calgary, Alberta T2P 3N5 Canada	IBM Direct Services Sortemosevej 21 DK-3450 Allerød Denmark

- **Fax** – send orders to:

United States (toll free)	1-800-445-9269
Canada	1-800-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1) 408 256 5422 (Outside USA)** – ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **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

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.html`). 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.

List of Abbreviations

IBM	International Business Machines Corporation
ITSO	International Technical Support Organization
ATM	Asynchronous Transfer Mode
BCM	Broadcast Manager
BUS	Broadcast and Unknown Server
ELAN	Emulated LAN
ELS	Event Logging System
ILMI	Interim Local Management Interface
JMA	Java Management Application
JPM	Java Performance Monitor
LAN	Local Area Network
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LES	LAN Emulation Server
MAC	Medium Access Control
PVC	Permanent Virtual Circuit
RMON	Remote Monitor
SNMP	Simple Network Management Protocol
SVC	Switched Virtual Circuit
TCP/IP	Transmission Control Protocol/Internet Protocol
VLAN	Virtual LAN

Index

Numerics

A

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

ITSO Redbook Evaluation

Network Management Using Nways Management Applications
SG24-5302-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.ibm.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?
_ **Customer** _ **Business Partner** _ **Solution Developer** _ **IBM employee**
_ **None of the above**

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

_____

_____

_____

_____

_____

SG24-5302-00

Printed in the U.S.A.

Network Management Using Nways Management Applications

SG24-5302-00