Nways Manager for AIX

LAN Network Manager/Intelligent Hub Management Program User's Guide

Version 2.0

GA27-4232-00

Nways Manager for AIX

LAN Network Manager/Intelligent Hub Management Program User's Guide

Version 2.0

GA27-4232-00

Note

Before using this information and the product it supports, be sure to read the general information under “Appendix. Notices” on page 443.

Third Edition (May 1999)

This edition applies to Version 2 of the Nways Manager for AIX-LAN Network Manager/Intelligent Hub Management Program.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers’ comments appears at the back of this publication. If the form has been removed, address your comments to:

Department CGF
Design & Information Development
IBM Corporation
PO Box 12195
RESEARCH TRIANGLE PARK NC 27709
U.S.A.

You can also submit comments about this publication online at:
`http://www.networking.ibm.com/support/feedback.nsf/docsoverall`

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

Contents

Tables

Part 1. Introduction

Chapter 1. What's New in Nways Nways Manager-LAN?

This chapter describes the new functions and devices supported by Nways Manager-LAN for AIX Version 3 Release 2 and Version 3 Release 3.

New Functions and Devices Supported by Nways Manager-LAN V3R3

The following new functions and devices are supported in Nways Manager-LAN for AIX Version 3 Release 3:

- Nways Manager-LAN now provides web-based management using Java technology for the following devices:
  - 2210 Nways Multiprotocol router
  - 2216 Nways Multiaccess connector
  - 8210 Nways Multiprotocol Switched Services (MSS) server
  - 8273 Nways Ethernet RouteSwitch
  - IBM Ethernet and Token-Ring adapters
  - Generic Java-based management for any SNMP device in your network, including support for:
    - 6611 network processor
    - 8271 Ethernet LAN Switch (Models 524, 612, 624, and 712)

  Also, Java-based performance functions in Nways Manager-LAN allow you to better manage large networks by providing more precise ways to graphically represent network data. Java-enabled Distributed Intelligent Agents allow you to make better use of the processing power of the management station by moving polling operations closer to where polled devices are located. See the online book **Introduction** for more information on the new Java-based functions.
- Remote Monitor supports the collection and analysis of information on network performance from agents in 827x LAN switches and provides additional capabilities for managing network performance using the Enterprise Communications Analysis Module (ECAM). See the online book **Introduction** for information on the new functions that are supported.
- The 8265 ATM switch can be managed using Nways Manager-LAN. New icons that represent the 8265 have been added to the Nways Manager-LAN user interface and are described in the online book **User Interface**.
- Nways Manager-LAN uses a new color-coded status for 8250 and 8260 hubs and 8265 ATM switches that temporarily do not respond to SNMP requests. See the online book **User Interface** for more information.
- Information on how to navigate between Hub and Module Level views and LAN submaps has been added to the online book **User Interface**.
- Information on the LAN names used to represent LAN subnets and standalone segments in the LAN Network submap has been added to the online book **User Interface**.

- In Bridge submaps, realistic views of SNMP bridges have been replaced by a generic view that allows you to represent multiple segments on the same interface. Realistic views are still available by starting the bridge's Product Specific Module. See the online book **User Interface** for more information.
- When merging LAN submaps, you can use SMIT to disable a token-ring SNMP agent if a fault in the agent prevents LAN submaps from being merged. This new function is described in the online book **User Interface**.
- The Locate function allows you to find a specific network device that is managed by an Nways application (such as Nways Manager-LAN, Nways Manager-ATM, or a Product Specific Module) and highlight it in an IP Internet submap. See the online book **Managing 8250, 8260, and 8265 Devices** for more information.
- Nways Manager-LAN documentation has been updated to help you resolve problems concerning the graphical display of ATM, 8271, and 8272 modules in Hub Level views. See the online book **Troubleshooting 8250, 8260, and 8265 Devices** for more information.
- To improve the response time in the startup of the NetView for AIX graphical interface, you can reset the synchronization priority for the iubmap process. See the online book **Troubleshooting 8250, 8260, and 8265 Devices** for more information.
- Changes you make to the community names of SNMP bridges, token-ring agents, and FDDI agents from NetView for AIX immediately take effect. You no longer need to stop and restart Nways Manager-LAN daemons to activate the change. See the online books **Managing SNMP Token-Ring Resources and SNMP Bridges** and **Managing FDDI Resources** for more information.
- The Resync function has been improved to provide a list of failing token-ring segments. See the online book **Managing SNMP Token-Ring Resources and SNMP Bridges** for more information.
- Nways Manager-LAN documentation has been updated to help you resolve problems concerning the management of LAN resources managed by LNM OS/2, SNMP token-ring, SNMP bridge, and FDDI SNMP proxy agents. See the online book **Troubleshooting Token-Ring and FDDI Resources** for more information.
- The following new modules and devices are supported. You can find information on how to configure and manage these modules in the **online help** for each module.
  - 8260 Distributed Management Module (DMM) Version 5.1
  - 8260 Control Point and Switch module Version 3.1
  - 8260 ATM Carrier module Version 1.5
  - 8260 Switching Modules Series (FDDI, Ethernet) Version 2
  - 8265 Nways ATM Switch
  - 8265 ATM 622 Mbps module
  - 8265 4-port Flex 155 Mbps module
  - 8265 4-Port Multimode Fiber 155 Mbps module
  - ATM 155 Mbps Multimode Fiber Universal Feature Card for use in IBM 8270, 8271, and 8272 LAN switches
  - 8270-800 Nways LAN Switch
  - 8271 EtherStreamer/Nways Ethernet LAN Switch, including new models 524, 612, 624, and 712

- 8271 ATM/Ethernet LAN Switch module
- 8272 LANStreamer/Nways Token-Ring LAN Switch
- 8272 ATM/Token-Ring LAN Switch module
- 8276 Nways Ethernet RoutePort
- E1, T1, E3, DS3, OC3, and SMT1 I/O cards on ATM WAN 2 modules
- 2216 Multiaccess Connector

For the most up-to-date information about what devices and hardware versions are supported by Nways Manager-LAN Version 3.3, refer to the hardware matrix in the Nways Management home page on the web at:
http://www.networking.ibm.com/cma/cmasolut.html

For information on how to start and stop tracing on Nways Manager-LAN applications, refer to the section on tracing on the web at: **http://www.networking.ibm.com/cma**

New Functions and Devices Supported by Nways Manager-LAN V3R2

The following new functions and devices are supported in Nways Manager-LAN for AIX Version 3 Release 2:

- The Nways Traffic Monitor has been added to the IBM Nways Manager suite of products and can be used with Nways Manager-LAN to provide a comprehensive network management solution. Traffic Monitor allows you to graphically display and manage traffic flows in end-to-end connections in your network. See the online book **Introduction** for more information.
- The Switching Module Manager has been integrated into Nways Manager-LAN allowing you to set up virtual switches on Switching modules in 8260 hubs to manage virtual LANs that consist of FDDI, Ethernet, and ATM devices. See the online book **Introduction** for more information.
- New icons are used to represent unmanaged and unknown (generically managed) modules. See the online book **User Interface** for more information.
- In 8260 hubs, ATM resources can be managed by an ATM Switch (A-CPSW) module Version 2.3 (or higher) if no Distributed Management Module (DMM) is installed. See the online book **Managing 8250, 8260, and 8265 Devices** for more information.
- The following new modules and devices are supported. You can find information on how to configure and use these modules in the **online help** for each module.
  - ATM 2-port WAN E3/T3 module
  - ATM 12-port 25 Mbps module with one 155 Mbps port (uplink)
  - ATM Control Point and Switch (A-CPSW) module Version 3.0
  - Distributed Management Module (DMM) Version 4.12
  - Hybrid Fiber Coax (HFC) module
  - Switching modules in 8260 hubs
  - Token-Ring High-End MAC Monitor (H-TMAC) Card with embedded RMON probe
  - Video Distribution module (VDM)
  - New 8260 chassis with PacketChannel backplane

- 8271 Ethernet LAN Switch and 8272 Token-Ring LAN Switch modules in 8260 hubs
- 8273 and 8274 concentrators (managed using IBM Nways RouteSwitch Network Manager)

For the most up-to-date information about what devices and hardware versions are supported by Nways Manager-LAN Version 3.2, refer to the hardware matrix in the Nways Management home page on the web at:
http://www.networking.ibm.com/cma/cmasolut.html

Chapter 2. About Nways Manager-LAN Documentation

The documentation for Nways Manager-LAN for AIX consists of a set of online books designed to help you understand the network management features of the product, and to configure and use it.

How to Use This Online Documentation Set

The online documentation for Nways Manager-LAN is divided into the following parts:

- **Introduction** describes the major functions of Nways Manager-LAN and how it provides a complete management solution for traditional LAN-based networks, such as Ethernet Token Ring, and FDDI. This part also describes how Nways Manager-LAN may be coupled with Nways Manager-ATM, Remote Monitor, and Traffic Monitor to provide a fully integrated management solution for Campus and WAN networks.
- **User Interface** describes how to use the graphical interfaces and navigate through the submaps of Nways Manager-LAN.
- **Managing 8250, 8260 and 8265 Devices** describes how to monitor and manage 8250 and 8260 hubs and 8265 ATM switches, and how to work with traps.
- **Troubleshooting 8250, 8260 and 8265 Devices** describes how to diagnose and resolve problems associated with the operation of 8250 and 8260 hubs and 8265 ATM switches and how to handle logging.
- **Managing LLC Token-Ring Resources** describes how to manage logical link control (LLC) token-ring LAN segments and how to work with LNM OS/2 Agent traps.
- **Managing SNMP Token-Ring Resources and SNMP Bridges** describes how to manage SNMP-based Token-Ring LAN segments and SNMP-managed bridges and how to work with SNMP Token-Ring and SNMP Bridge traps.
- **Managing FDDI Resources** describes how to use LAN Network Manager to manage FDDI segments and how to work with FDDI SNMP Proxy Agent traps.
- **Troubleshooting Token-Ring and FDDI Resources** describes how to diagnose and resolve problems associated with the operation of LLC token-Ring, SNMP token-ring and FDDI devices and SNMP bridges, and how to handle logging and messages.
- **Coupling and Autodiscovery** describes how to couple Nways Manager-LAN with Nways Manager-ATM and how to use the Autodiscovery function.
- **Appendix** provides a glossary of the terms and abbreviations used in the online documentation for Nways Manager-LAN and a bibliography of relevant documentation to which you can refer for further information.

Highlighting Conventions

The following highlighting conventions are used in the online documentation for Nways Manager-LAN:

Bold	Identifies menu choices, push buttons, commands, and shell script

	paths (except in reference information), default values, user selections, daemon paths (on first occurrence), and flags (in parameter lists).
Italics	Identifies parameters whose actual names or values are to be supplied by the user, and terms that are defined in the following text.
Monospace	Identifies subjects of examples, messages in text, examples of portions of program code, examples of text you might see displayed, information you should actually type, and examples used as teaching aids.

Naming Conventions

In the collection of Nways Nways Manager-LAN online books, NetView for AIX is used to mean IBM NetView for AIX V4.1 (5697-NVW) available under the TME 10 Management Server V4R4 (CD-ROM SK2T-6032).

Chapter 3. IBM Nways Manager for AIX Version 1.2

IBM Nways Manager for AIX Version 1.2 provides a comprehensive Campus and WAN management solution and consists of the following components:

- Nways Manager-LAN
- Nways Manager-ATM
- Remote Monitor
- Traffic Monitor

IBM Nways Manager allows you to graphically manage a wide range of IBM LAN and ATM Campus devices, non-IBM devices that support ATM Forum-compliant MIBs, and non-IBM devices that support standard LAN MIBs (for example, RMON MIB).

The common graphical user interface displays realistic views of your network resources and shows the color-coded status of network segments and individual devices. An autodiscovery function automatically updates views of network topologies when configuration changes are made.

Some of the ways in which you can use Nways Manager products to graphically manage your network are as follows:

- Monitor, reset and filter the discovery of network devices.
- Collect realtime and historical statistics.
- Set performance thresholds.
- Use drag and drop graphics to set up and manage virtual LANs and ELANs.
- Automate problem management by configuring a specific fault management task to be run when an alert is received from a critical resource.
- Troubleshoot problems in network operation using a complete set of messages, traps, and events.

Coupling with Nways Manager-ATM

Nways Manager-ATM for AIX allows you to manage ATM networks, including virtual networks created from Emulated LANs (ELANs), and ATM devices that use ATM Forum-compliant MIBs. When you couple Nways Manager-LAN with Nways Manager-ATM, you can manage the following IBM ATM devices together with other non-IBM ATM devices and IBM LAN devices in your Campus network:

- 2210 Nways Multiprotocol router
- 2216 Multiaccess connector
- 6611 Multiprotocol routers
- 8210 Multiprotocol Switched Services (MSS) servers
- 8260 ATM hubs
- 8265 ATM switches
- 8270 LAN switches with ATM Universal Feature Card

- 8271 Ethernet LAN switches
- 8272 Token-Ring LAN switches
- 8281 ATM LAN bridges
- 8282 ATM Workgroup concentrators
- 8285 ATM Workgroup switches
- Other ATM devices that implement the ATM or LAN Emulation (LANE) standard MIBs

Nways Manager-ATM provides a complete management solution for ATM networks that includes:

- Management of virtual networks that consist of emulated LANs
- Autodiscovery of ATM devices and links, including the capacity to filter the discovery of ATM devices and to set the discovery interval to optimize polling
- Expansion of ATM topology views to manage 8260 ATM Switch modules, 8265 ATM Switches, 8281 ATM LAN bridges and integrated Bridge modules, 8282 ATM Workgroup concentrators, and 8285 ATM Workgroup Switches
- Support for web-based management of ATM devices
- Capability for discovering and maintaining PNNI topologies
- Broadcast manager (BCM) capabilities
- Virtual LAN management using ATM-Forum compliant standard for LAN emulation
- Support of non-IBM ATM devices
- Graphical display of ATM connections in the network
- Seamless coupling with Nways Manager-LAN
- Capability for setting permanent virtual connections
- Graphical tracking and configuration of ATM connections
- Management of logical links
- Statistics for ATM interfaces
- Display of ATM port and connection statistics as line, pie, or bar graphs
- Display of events and traps with optional filtering
- Download of microcode updates to ATM devices

Coupling with Remote Monitor

Coupling Nways Manager-LAN with Remote Monitor allows you to collect, monitor, analyze, and display network statistics from RMON and ECAM (RMON2) agents in Token-Ring and Ethernet LAN devices, such as:

- Devices attached to IBM 8225, 8230, 8237, 8238, 8250, and 8260 hubs and concentrators
- 8270, 8271, and 8272 LAN switches
- Devices with OEM RMON agents

Using Remote Monitor, you can view communication patterns and proactively manage the performance of your network. You can watch for emerging problems and short-term

trends, check network performance and utilization, troubleshoot network problems, and set network service objectives using the following features:

- Real-time color-coded graphic views of LAN statistics
- Full RMON support for Ethernet (nine groups) and Token Ring (13 groups)
- Display of alarm locations in LAN segments
- Traffic Transmission Management Module (TTMM) that generates traffic on specific LAN segments and rings and that is downloadable to supporting agents
- Enterprise Communications Analysis Module (ECAM) for ECAM statistics, host, matrix, and protocol distribution (segment or station): collection of data at all seven protocol layers, including segment, host, and host matrix statistics for the major protocols (IP, IPX, DECnet, Banyan, and so on) and application types.

  ECAM allows you to determine communication patterns and evaluate the use of expensive links. Using this information, you can better tune your network and relocate critical resources (such as file servers) as needed. Also, ECAM allows network operators to view internetwork traffic in order to troubleshoot network problems.
- Support for the following agents:
  - 8225 Fast Ethernet Stackable hub
  - 8230 Token-Ring Controlled Access unit
  - 8237 Stackable Ethernet hub
  - 8238 Token-Ring Stackable hub
  - 8250 Ethernet RMON probe
  - 8250 Token-Ring Management Module (TRMM)
  - 8260 Token-Ring and High-End Ethernet Media daughter cards
  - 8260 Switching Modules Series
  - 827x LAN switches
  - Other RMON-compliant probes

RMON and RMON2 are standards from the Internet Engineering Task Force (IETF) that advance the state-of-the-art in open network performance management and fault diagnosis.

- RMON defines a standard set of MAC-layer statistics and the ability to filter and capture data packets for analysis.
- RMON2 allows you to go beyond the previous RMON standard to full seven-layer data collection using Enterprise Communications Analysis Modules (ECAM) support, including segment, host, and conversation statistics for the major protocols and application types.

Remote Monitor takes advantage of ECAM (RMON2) capabilities to provide:

- Address translation of MAC addresses to network-layer addresses
- Views of the protocols and applications being used in the network
- Protocol matrixes to see who is talking to whom in the network and what protocols they are using.

Coupling with Traffic Monitor

Coupling Nways Manager-LAN with Traffic Monitor allows you to graphically display and manage traffic flows in end-to-end connections in your network. You can display the stations in your network according to location, subsets, functional group, and VLAN.

The Traffic Monitor user interface clearly shows how client-server applications are using the network. This allows you to look at data according to user and business-critical application (such as Lotus Notes utilization or order-entry application throughput), instead of tuning your network according to technology type (such as Ethernet utilization or switch throughput).

Traffic Monitor collects and correlates data from multiple RMON and ECAM probes to provide a complete, accurate view of enterprise network traffic for performance management, trend analysis, and troubleshooting. You can display graphical views of the current realtime and historical data. Traffic Monitor functions seamlessly integrate with Remote Monitor functions to provide complete management of your RMON, RMON2, and ECAM probes.

RMON2 is now an approved IETF standard. IBM's RMON2 support is based on the pre-RMON2 standard, the Enterprise Communications Analysis Module (ECAM) that will be migrated to the IETF RMON2 standard.

Traffic Monitor allows you to analyze the protocol-level and application-level traffic patterns in your network for the following IBM networking devices:

- Using RMON agents:
  - 8225 Fast Ethernet Stackable Hub
  - 8230 Token-Ring Controlled Access Unit
  - 8237 Stackable Ethernet Hub 10BASE-T
  - 8238 Nways Token-Ring Stackable Hub
  - 8250 Advanced Token-Ring Management Module
  - 8260 Switching Modules Series
  - 8260 Token-Ring Media Access Daughter Card
  - 8260 Ethernet Media Access Daughter Card
  - 8270 Nways LAN Switch
  - 8270 EtherStreamer/Nways Ethernet LAN Switch (including new models 524, 612, 624, and 712)
  - 8272 LANStreamer/Nways Token-Ring LAN Switch
  - 8273 Nways Ethernet RouteSwitch
  - IBM 8274 Nways LAN RouteSwitch
- Using RMON2 (including RMON) agents:
  - 8250 Ethernet RMON Probe
  - IBM 8260 High-End Token-Ring Media Access Daughter Card
  - IBM 8260 High-End Ethernet Media Access Daughter Card

– Token-Ring RMON universal feature card (UFC) for the 8270 and 8272 LAN switches

Traffic Monitor allows you to display the following information for the protocols and applications used in your network:

- Which clients are accessing which servers
- Which protocols are being carried over your network
- Which remote devices are accessing your network
- Which remote networks are being accessed from devices in your network

You can use this information to maximize performance, manage faults, and set security criteria.

Traffic Monitor provides a high-level graphical representation of your network showing general traffic flows. You can zoom in to monitor traffic on individual segments, protocols, devices, links, and connections. This top-down network view complements the bottom-up views provided by other Nways network management products.

Traffic Monitor collects data from the RMON and RMON2 agents at regular intervals. This information is then graphically presented to accurately display network traffic flows. As more information is collected, older data is consolidated so that less disk space is required. Using report generation facilities, you can display traffic trends using real-time and historical data.

Using representations of the end-to-end traffic flows, you can manage your network based on the protocols and applications you are running. Also, Traffic Monitor allows you to organize and capture data about the entities in your network (for example, according to departments, locations, functions, and virtual networks). This means that you can configure groups of entities to be monitored according to their RMON and RMON2 agents. This avoids the need for defining data collection parameters.

Chapter 4. Introducing Nways Manager-LAN

Nways Manager-LAN for AIX provides a complete management solution for legacy LAN-based networks (Ethernet, Token Ring, and FDDI), including virtual LANs (VLANs), APPN and DLSw networks, and ATM device-specific management in the backbone of campus networks.

Nways Manager-LAN allows you to graphically manage SNMP-enabled IBM networking devices (including IBM ATM devices that were formerly managed by Nways Manager-ATM) from a single AIX management station; for example:

- Multiprotocol intelligent hubs (8250 and 8260)
- ATM switches (8265 and 8285) and concentrators (8282)
- Multiprotocol Switched Services servers (8210)
- Virtual LANs consisting of FDDI, Ethernet, and ATM devices using the Switching Modules Series in 8260 hubs
- LAN switches and ATM/LAN switches (827x), LAN concentrators (8224, 8225, 8230, 8237, 8238, 8240, and 8244), Remote Access LAN devices (8235), and routers and bridges (2210, 2216, 6611, and 8281)
- External routers and bridges (2210, 2216, 6611, 8229, 8281, and OEM) and 8250, 8260, and 8265 integrated routers and bridges
- LAN topologies and media management

Nways Manager-LAN provides its own graphical user interface that is seamlessly integrated into the graphical interface of NetView for AIX. Through its autodiscovery function, Nways Manager-LAN automatically updates status and configuration information on all IBM LAN and ATM devices.

Nways Manager-LAN gives you:

- Best-of-breed box management for:
  - 2210 multiprotocol routers
  - 6611 network processors
  - 8224, 8230, and 8238 hubs
  - 8225 Fast Ethernet Stackable hubs
  - 8235 DIALs Remote Access servers
  - 8250 and 8260 multiprotocol intelligent hubs
  - 8265 ATM switches
  - 827x LAN switches
  - 8281 ATM LAN bridges
  - 8282 ATM Workgroup concentrators
  - 8285 ATM Workgroup switches
- Enhanced router and bridge management features, including:
  - Management of 2210, 6610, RXR/2, and 8229 standalone devices
  - Management of Bridge and Router modules in 8250 and 8260 hubs

  - Support of selected OEM routers
  - Support of APPN and DLSw topologies
- Virtual bridging on the Switching Modules Series in 8260 hubs
- Integration with NetView for AIX to provide:
  - Protocol switching to views in other applications
  - Correlation of faults and events
  - Topology
- Support for large networks using the distributed polling capabilities of TME 10 Mid-Level Manager (MLM)
- Support for large networks using Java-based performance management and Distributed Intelligent Agents

Nways Manager-LAN's support for web-based management using Java technology allows you to manage the following devices from a local AIX workstation over your intranet or over the Internet:

- 2210 Nways Multiprotocol router
- 2216 Nways Multiaccess connector
- 8210 Nways Multiprotocol Switched Services (MSS) server
- 8273 Nways Ethernet RouteSwitch
- IBM Ethernet and Token-Ring adapters
- Generic Java-based management for any SNMP device in your network including support for:
  - 6611 network processor
  - 8271 Ethernet LAN Switch (Models 524, 612, 624, and 712)

As the status of your network changes, your web browser is automatically updated with the latest information. Web-based management allows you to perform the following tasks:

- Display graphical views of the real-time status of supported devices.
- Configure and manage devices using a hierarchical navigation tree.

Nways Manager-LAN's support for Java-based performance management allows you to monitor, set thresholds, and graphically display (pie and bar charts, line graphs) data for specific MIB objects and collections of objects.

Java-based Distributed Intelligent Agents installed in Java-enabled workstations in the network are used by Nways Manager-LAN's performance functions. You can configure the agents to notify Nways Manager-LAN when thresholds are exceeded. Distributed Intelligent Agents allow you to offload polling information from the AIX management station in order to:

- Free processing capability on the management station.
- Perform polling closer to where the polled devices are located.
- Free bandwidth across WAN links.

Environment-Specific Components

The functions of Nways Manager-LAN are integrated into the NetView for AIX graphical interface to allow you to centralize the management of IP-addressable devices and LAN resources from a single workstation. Because your LAN environment can consist of different types of LANs, Nways Manager-LAN uses a closely integrated group of applications to monitor and manage your LAN resources.

Nways Manager-LAN consists of the following applications:

- LAN Network Manager
- 8250, 8260, and 8265 Device Manager
- Switching Module Manager
- Router and Bridge Manager
- Product Specific Modules (PSMs) and Java web-based management functions

To manage your LAN resources, Nways Manager-LAN uses SNMP, LLC (for token-ring), and SMT (for FDDI). SNMP supports the following types of LAN management:

- Standard SNMP Bridge MIBs (RFC 1213, 1286, and 1493)
- RMON (RFC 1271 and 1513)
- IBM Surrogate MIB
- Private MIBs for box management

Table 1 shows:

- Types of LAN resources that Nways Manager-LAN monitors and manages
- Nways Manager-LAN application that manages each type of LAN resource
- Agents used by each application

Table 1. Environment-Specific Component and Agents

Type of Resource Managed	**Component**	**Agents**
LLC-based token-ring bridges and CMOL-based concentrators	LAN Network Manager (LNM OS/2 Agent application)	LNM OS/2 proxy agent
SNMP token-ring	LAN Network Manager (SNMP Token-Ring application)	• IBM 8230 agent • Token-ring surrogate agent • RMON agent that supports RFC 1513

Table 1. Environment-Specific Component and Agents (continued)

Type of Resource Managed	Component	Agents
SNMP bridges and switches	LAN Network Manager (SNMP Bridge application)	• 2210, 2216, 6611, 8281, and OEM • RFC 1213, 1286, and 1493 • 8229 bridge and 8250 integrated bridge that support RFC 1213, 1286, and 1493 • 827x standard MIB-compliant switches • Switching Modules Series in 8260 hubs
FDDI	LAN Network Manager (FDDI application)	FDDI proxy agent
SNMP 8250 and 8260 multiprotocol hubs	8250, 8260, and 8265 Device Manager	DMM, EMM, FMM, and TRMM
8260 ATM hubs and 8265 ATM switches	8250, 8260, and 8265 Device Manager	Control Point and Switch (CPSW) with DMM subset
Virtual LANs (FDDI and Ethernet with ATM uplink)	Switching Module Manager	DMM that manages 8260 Switching modules
SNMP bridges and routers	RABM	• 2210, 6611, 8229, and 8281 • IBM 8229 bridges • IBM RouteXpander/2 (Version 2) • Router modules and bridge modules in 8250 and 8260 hubs and 8265 ATM switches • Cisco Systems, Proteon, and Wellfleet routers
SNMP workgroup hubs, LAN switches, and ATM LAN bridges	PSMs	2210, 6611, 8224, 8230, 8235, 8238, 8271, 8272, 8281, and 8285
SNMP workgroup hubs, LAN switches, and ATM LAN bridges	Java web-based management	2210, 2216, 8210, and 8273

In addition to the agents listed, the SNMP bridge application can display information from other MIBs if they are present in the bridge.

You can configure Nways Manager-LAN to start only the applications that you need in your network management environment. For example, if you do not have FDDI resources in your network, you can use SMIT to configure Nways Manager-LAN to start only the LNM OS/2 Agent, SNMP Token-Ring, and SNMP Bridge applications.

Managing 8250 and 8260 Hubs and 8265 ATM Switches

Nways Manager-LAN uses 8250, 8260, and 8265 Device Manager to manage 8250 and 8260 hubs and 8265 ATM switches to provide:

- Realistic graphic views of 8250 and 8260 hubs and 8265 ATM switches at system, module, and port levels
- Hub, module, and port configuration using the mouse (point-and-click)
- Graphical display and file storing of realtime and historical statistics for faults and traffic at network, module, and port levels
- Color-coded display of system status based on traps received and polling using the Resource Monitor facility
- Realtime event monitoring for entries in the NetView for AIX event log
- Inband download of microcode
- Balance load over subnetworks by user port assignments across hub segments
- Create workgroups and simplify network segment names by using logical LANs
- Drag and drop facility for configuring network resources and critical resources

You can also manage 8250 and 8260 hubs and 8265 ATM switches in the following ways:

- Analyze the performance and faults of routers and bridges connected to or integrated in 8250 and 8260 hubs and 8265 ATM switches using the Router and Bridge Manager (RABM)
- Full analysis and graphical displays of token-ring and Ethernet RMON statistics
- Navigation between box level views and LAN topology using LAN Network Manager (LNM) to perform media management or to a port on an ATM LAN Bridge module
- Full ATM box management when coupled with Nways Manager-ATM, including navigation between the ATM topology and Hub and LAN topology views

In 8260 hubs, if no Distributed Management Module (DMM) is installed and if an ATM Switch (A-CPSW) module Version 2.3 or higher is installed, hub resources are still managed from Nways Manager-LAN by means of a subset of the DMM MIB in the A-CPSW module. When a DMM module is installed with an A-CPSW module (Version 2.3 or higher), the DMM serves as the master management module.

In 8265 ATM switches, box management is also performed by Nways Manager-LAN using a subset of the DMM MIB in the CPSW module.

Using Virtual Switches to Manage Virtual LANs

Nways Manager-LAN allows you to associate ports on the Switching Modules Series in 8260 hubs using Switching Module Manager to create *virtual switches*. A virtual switch operates as a bridge that allows devices of various media types (Ethernet, FDDI, and ATM) to communicate in a *virtual LAN*.

Switching Module Manager communicates over the PacketChannel backplane in 8260 hubs and provides the following features:

- Scalable bandwidth and performance that allow enterprise networks to migrate from shared LANs to switched LANs and from switched LANs to then to ATM:

  - A high performance switch is provided between Ethernet and FDDI LANs, allowing for future migration to ATM.
  - Each module has its own switching engine or Application Specific Integrated Circuit (ASIC) allowing a 650 000 pps (packets per second) throughput.
  - Each module has its own processor and storage for basic switching functions:
    - Address learning
    - Spanning tree calculations
    - RMON support
    - Packet fragmentation (for FDDI to and from Ethernet).
  - PacketChannel backplane performance: 2Gbps or 3.4 Mpps (mega packets per second)
  - Multiprotocol environment support: 10Mbps and 100Mbps Ethernet, FDDI, and ATM
- High function backbone features:
  - 32 000 MAC addresses per module
  - User defined MAC address filters
  - 64 protocol filters per module
  - Traffic prioritization on the protocol type
- Virtual networking:

  Switching modules allow you to customize user-defined groups of ports called *virtual switches*. Each virtual switch is a logical group of ports from different modules and different interface types, with the following characteristics:
  - Up to 256 virtual switches in each 8260 hub
  - Each virtual switch has its own set of switch capabilities
  - Each virtual switch is configurable and managed by a DMM (at software version 4.11 or later)
- High fault tolerance and reliability
  - Switching modules take advantage of the reliability features of 8260 hubs:
    - Power management
    - Load-sharing power supplies
    - Redundant power supply, controller, and DMM
  - PacketChannel backplane architecture: a passive bus without active components that can fail
  - Switching engine at module level
  - Dynamic side switching: detection of inter-module device moves
  - Hot-pluggable modules with configuration learning
- System management
  - RMON support: an embedded RMON agent (or RMON probe) in each module provides RMON group support for the family of Switching modules and statistics collection at port level.
  - Integrated inventory management data

- Roving port analysis: a method for monitoring network traffic. The traffic on a port is mirrored to another port or the embedded RMON probe on the same Switching module or to another module.
- Inband and out-of-band management from the DMM.

Managing IBM Workgroup Hubs, ATM and LAN Switches, ATM LAN Bridges, and IBM ATM and LAN Routers

Using Product Specific Modules (PSMs) and Java web-based management functions, Nways Manager-LAN provides the following features to manage IBM Workgroup hubs, ATM and LAN switches, ATM LAN bridges, and IBM ATM and LAN routers:

- Realistic graphic views of devices at system, module, and port levels
- Port and box configuration using the mouse (point-and-click)
- Color-coded display of system status based on traps received and polling using the Resource Monitor facility
- Realtime event monitoring for entries in the NetView for AIX event log
- Inband download of microcode
- Balance load over subnetworks by user port assignments across hub segments
- Monitor events in realtime.

Monitoring IBM and OEM Routers and Bridges

Nways Manager-LAN allows you to monitor the following IBM and OEM routers and bridges (source-route, translational, and transparent) using the Router and Bridge Manager (RABM):

- 2210 Nways Multiprotocol Router
- 2216 Multiaccess connector
- 6611 Network Processor
- 8229 Bridge
- 8271 and 8272 LAN switches
- 8281 ATM LAN Bridge
- RouteXpander/2 (Version 2)
- Router modules used in 8250 and 8260 hubs
- Bridge modules used in 8250 and 8260 hubs
- Cisco Systems routers
- Wellfleet routers
- Proteon routers

To manage routers and bridges, Router and Bridge Manager displays the following types of status for a router or bridge network:

- Operational status
- Status of all interfaces

- Status of all supported protocols
- Integration with the graphical views of 8250 and 8260 hubs and 8265 ATM switches
- Logs and graphs performance and faults for routers and bridges

In addition, Router and Bridge Manager provides the following features for router and bridge management:

- Fast path interface to the 2210 and 6611 System Managers
- Limited support of SNMP Set commands (with 6611 MPNP V1.3)
- APPN and DLSw topology
- Advanced Peer-to-Peer Networking
- Data link switching
- Client-server capability
- Distributed polling to support large networks of routers
- Object-oriented data storage in an ObjectStore database that maintains a persistent topology of managed nodes

For more information on the Router and Bridge Manager component of Nways Manager-LAN, see *IBM AIX Router and Bridge/6000: User's Guide* (SC31-6489).

Managing LAN Resources

To manage the LAN resources in your network, Nways Manager-LAN uses the LAN Network Manager component. The functions of LAN Network Manager are integrated into the NetView for AIX graphical interface, enabling you to manage the physical resources in your multiprotocol network from a single workstation. You can monitor and manage IP-addressable devices with NetView for AIX and, using information provided by environment-specific agent programs, expand your scope of management to LLC token-ring, SNMP token-ring, SNMP bridge, and FDDI environments with LAN Network Manager.

LAN Network Manager provides topological views of the LAN, which allows you to correlate different protocol views with the underlying physical topology. LAN Network Manager also provides profile, configuration, fault, and performance information for your LAN resources.

Specifically, LAN Network Manager works with environment-specific agent programs to provide:

- A graphical user interface
- AIX NetView/6000 integration
- Environment-specific applications
- LLC token-ring management
- SNMP token-ring management
- SNMP bridge management
- FDDI network management

- Profile information
- Configuration information
- Fault information
- Performance information
- Statistics for SNMP-managed resources

Each of these applications is described in the following sections.

You can use LAN Network Manager to manage a network environment consisting of LLC token-ring resources, SNMP token-ring resources, SNMP-managed bridges, and FDDI resources.

The proxy agents gather their information from a variety of management information bases (MIBs). More information about LAN Network Manager applications, proxy agents, and the MIBs from which they obtain network data is provided in other online books in the Nways Manager-LAN documentation set.

Managing LLC Token-Ring Resources

With LAN Network Manager you can manage both logical link control (LLC) and SNMP-managed token-ring segments. Using information provided by the OS/2 agent, LAN Network Manager integrates the LAN hardware managed by LAN Network Manager for OS/2 Version 2.0 into the views of the simple network management protocol (SNMP) managed environment. Management of the IBM SNMP 8230 concentrators and multiport bridges is provided by the SNMP Token-Ring and the SNMP Bridge applications, respectively. This management is not provided as part of the LNM OS/2 Agent application.

Although the LLC-based segments are not merged with SNMP segments in the topology views, the flexibility of the graphical interface enables you to manage the LLC-based LAN hardware and SNMP-addressable resources.

LAN Network Manager manages the LLC networks based on solicited and unsolicited requests from the OS/2 agent. The OS/2 agent converts events that are received from the LLC token-ring environment into SNMP traps before passing them to LAN Network Manager. The OS/2 agent provides the capability to:

- Manage stations, LLC bridges, and IBM 8230 Models 1 and 2 controlled access units (concentrators).
- Collect and graph historical data.
- Manage access control for adapters and concentrators.
- Monitor critical resources.

You can double-click on a displayed segment resource to show a detailed submap for that device. LAN Network Manager enables you to perform management actions on resources, such as defining a station as a critical resource, and obtaining profile, configuration, fault, and performance information for a resource.

Managing SNMP Token-Ring Resources

The SNMP token-ring application of LAN Network Manager enables you to monitor and manage the SNMP-addressable token-ring resources in your network. The SNMP token-ring application uses agents that support AWP7607, an RMON agent, or the IBM 8230 MIB to discover the topology information it needs to provide support for SNMP segments and SNMP-managed 8230 concentrators.

As with the other types of LANs managed by LAN Network Manager, you can display SNMP network topology in the Segment and Node submaps. Device views of IBM SNMP-managed Token-Ring concentrators are available through product-specific management applications. Online documentation for these applications can be viewed by entering

```
/usr/lpp/mgtapptran/bin/viewDoc <docname>
```

where *docname* is the name of the online documentation that you want to view.

Managing SNMP Bridges

LAN Network Manager provides an SNMP bridge application that you can use to monitor and manage SNMP bridges. The SNMP bridge application works with SNMP agents that support RFC 1286 and MIB II, or RFC 1493 and MIB II. By communicating with these agents, LAN Network Manager can manage IBM bridges, such as the 8229, 2210, 8250, and 8281 bridges, and bridges from other manufacturers that support RFC 1286 and MIB II, or RFC 1493 and MIB II. In addition, LAN Network Manager can manage switches that implement a bridge MIB, such as the 8271, the 8272, and the Switching Modules Series in 8260 hubs.

You can use LAN Network Manager to view the topology and status of SNMP bridges, which are displayed in the LAN Subnet submap.

You can also display a Bridge submap, which shows a graphical representation of the bridge and its interfaces, and an Interface submap. The Interface submap contains icons that represent a bridge port and the interface protocol operating on the port. When SNMP-managed segments are matched with SNMP-managed bridges, LAN Network Manager merges them into the same submap, enabling direct navigation to the Segment submap.

Note: Define an overlapping token-ring surrogate or RMON agent to enable merging for SNMP-managed 8230 Token-Ring Concentrators within a LAN subnet map.

As with the other applications provided by LAN Network Manager, the SNMP bridge application enables you to perform management operations on the bridges, and to display profile, fault, configuration, performance, and statistics information for the bridges, bridge interfaces, and the bridge ports.

Managing FDDI Resources

LAN Network Manager enables you monitor and manage FDDI networks. Using its FDDI management application, LAN Network Manager provides management for devices that support levels 6.2 and 7.3 of the FDDI station management (SMT) standard, which is defined by the American National Standards Institute (ANSI). You can manage both single- and dual-attached stations, as well as concentrators that support SMT 6.2 or 7.3.

The IBM FDDI SNMP Proxy Agent Program sends instructions from LAN Network Manager to the managed FDDI segment and obtains status and change information pertaining to the FDDI resources. The FDDI agent also converts status reporting frames (SRFs) from the FDDI segment into SNMP traps and sends them to LAN Network Manager. Using LAN Network Manager, you can:

- Manage FDDI stations and concentrators that support parameter management frames (PMFs) and SMT 6.2 and 7.3.
- Monitor your resources more effectively through enhanced logical representation of the FDDI segment.
- Concurrently manage multiple FDDI segments.
- Manage the IBM 8240 and 8244 concentrators using a graphical representation of the concentrators.
- Manage other SMT-compliant FDDI concentrators using a graphical representation of a generic concentrator.

NetView for AIX Integration

By integrating 8250, 8260, and 8265 Device Manager and LAN Network Manager under NetView for AIX, Nways Manager-LAN allows you to perform the following tasks:

- Use management windows to query information and issue instructions for your LAN resources.
- Use protocol switching to easily move from a LAN physical-based view of a resource to IP.
- Manage events from Nways Manager-LAN along with those from other applications.
- Use the NetView for AIX Locate function to find a specific LAN resource.

Management Windows

You can query information and issue instructions using management windows in the same way you perform these tasks in other NetView for AIX applications. Depending on the resource, Nways Manager-LAN provides profile, configuration, fault, performance, and statistics management windows. These windows display information about the resource and, in some cases, enable you to define or change information for a resource.

Protocol Switching and Nways Protocol Switching

The NetView for AIX **protocol switching** function allows you to move from a LAN physical-based view of a resource to a view of the resource in the IP submap.

The **Nways protocol switching** function allows you to move between different Nways topology views, such as an ATM peer group and a LAN Segment view. A list of the protocols running on a device (or interface) is displayed with a list of the submaps in which the device appears. You can then open any of the submaps in the list and switch between them to display different views of the device from different protocol perspectives.

Event Management

Managing events is consolidated in NetView for AIX. Nways Manager-LAN sends events for the resources it is managing to NetView for AIX. These events are logged and displayed with events from other NetView for AIX applications, such as Trouble-Ticket* and Systems Monitor/6000, in the NetView for AIX alarm card display.

The NetView for AIX alarm card display contains information about the date and time the event occurred, the source of the event, and detailed and summarized descriptions of the event. You can also select the **Highlight** button on the alarm card display to show the resource that generated the event highlighted in a submap. For example, if you select **Highlight** when displaying an alarm card for a token-ring station, Nways Manager-LAN displays a segment submap with the token-ring station highlighted.

Locate Function

The integration of Nways Manager-LAN with NetView for AIX enables you to use the NetView for AIX Locate function to find specific LAN resources in your network. You can search for resources using a variety of resource attributes, such as name, status, type, or label. You can also locate submaps and highlight the submap icons that represent a resource.

Part 2. User Interface

Chapter 5. User Interface

This chapter describes how to use the graphical user interface of Nways Manager-LAN to manage your network resources.

Using the Graphical Interface

The NetView for AIX graphical interface displays a logical representation of your network through dynamic topology maps that contain hierarchies of network submaps and hub views. These hierarchies include graphical representations of your network resources at several levels:

- For 8250, 8260, and 8265 resources, there are views at the hub and module levels. This part of the Nways Manager-LAN graphical interface is managed by the 8250, 8260, and 8265 Device Manager application. For more information, see “Navigating through Different Hub Views” on page 39.
- For other devices displayed in the IBM Hubs Topology or integrated in 8250 and 8260 hubs and 8265 ATM switches, device-specific views are available.
- For LAN resources, there are submaps at the network, subnet, segment, interface, and node levels. This part of the Nways Manager-LAN graphical interface is managed by the LAN Network Manager application. For more information, see “Navigating through LAN Submaps” on page 47.

The graphical interface provides an easy way to access LAN submaps and hub views that are lower in the hierarchy by clicking on symbols that represent the lower submaps and views.

In addition, Nways Manager-LAN allows you to use separate submap hierarchies for different protocols. This means that for LAN resources, you can quickly switch from one protocol view to another (for example, from an IP to a token-ring submap), depending on the protocols running in the network resource. For hub resources, you can switch between a hub view and the LAN submap for the protocol used by the resource. (for example, from an 8260 module view to an Ethernet submap). The protocol switching function in Nways Manager-LAN allows to display different network views of the same LAN or hub resource. For more information, see “Switching Between Different Protocol Views” on page 51.

As part of the NetView for AIX graphical interface, Nways Manager-LAN offers extended network information in a consistent and familiar format. Working with windows, menus, and icons and navigating through submaps is similar to using NetView for AIX. For information about these topics, refer to the *NetView for AIX User’s Guide*.

Important: When starting multiple user interfaces, you may find that you cannot start **more than two** NetView for AIX sessions. This limitation is caused by insufficient disk space in the file system **/usr/CML/OStore/cache** used to start Nways Manager-LAN daemons and processes. For information on

how to resolve this problem, refer to ″Problems When Running Multiple NetView Sessions″ in the online book **Troubleshooting 8250, 8260, and 8265 Devices**.

Using the Mouse

You can perform many of the functions of the graphical interface with the mouse, such as displaying menus, selecting menu options, and executing actions for network devices.

Nways Manager-LAN accommodates either a 2-button or 3-button mouse. If you are using a 2-button mouse, you can simulate button 3 by pressing button 1 and button 2 at the same time.

Some of the main ways to use the mouse are as follows:

- Single click the leftmost button (MB1) to:
  - Display a pull-down menu from the menu bar.
  - Start the action for a selected menu item.
  - Display information about a selected hub resource in the Information Area at the bottom of the hub view.
  - Display hub resources that belong to a selected network.
- Double-click the leftmost button (MB1) to:
  - Open a new LAN submap for a selected LAN or LAN resource.
  - Open a new hub view for a selected hub or hub resource.
  - Open the Configuration panel for certain hub resources.
- Press and hold down the middle button (MB2) to drag and drop icons of LAN and hub resources. See “Dragging and Dropping Icons” on page 31 for more information.
- Single click the rightmost button (MB3) to display the context menu for a LAN or hub resource.

For more information about using the mouse, refer to the *NetView for AIX User's Guide Version 2* (SC31-7024).

Executable Devices

In NetView for AIX, devices are by default executable when you double-click on their icons. This is how you navigate through network views of LAN and hub resources. For example, if you double-click on a hub icon, an expanded Hub Level graphical view is displayed showing the contents of the hub.

The Nways Manager-LAN process that manages executable devices is called the *Symbols Manager*. The Symbols Manager determines which devices are to be discovered according to the Nways Manager-LAN applications that are installed. When a device is discovered, its icon appears on a Nways Manager-LAN submap. For more

information on the Nways Manager-LAN applications you can install and how they discover devices, see the online book, **Coupling and Autodiscovery**.

Dragging and Dropping Icons

In a LAN submap, you can use the mouse to drag LAN resources and reposition them. See “Customizing LAN Submaps” on page 55 for more information.

In a Hub Level view, you can use the mouse to drag and drop hub resources to:

- Change the network assignment of a resource.
- Manage a critical resource.

For more information, see ″Defining a Logical LAN″ and ″Monitoring Hub Resources″ in the online book **Managing 8250, 8260, and 8265 Devices**.

To drag and drop an icon:

1. Point to the resource and hold down MB2.

   The selected resource is outlined by a white border and its icon is displayed. The Information Area at the bottom of a hub view displays information about the resource.
2. Move the mouse until the icon is over the object on which you want to drop it.

   When you drag an icon over an object that is a possible drop site, the icon and the drop site change color. If the object is not a possible drop site, the resource icon changes to a ’Do Not Enter’ icon.

   If you drop an icon on a drop site that is not permitted, no operation is performed. In hub views, the reason is displayed on the bottom line of the Information Area.
3. Release MB2.

   In Hub Level views, the result of the drag and drop is shown on the bottom line of the Information Area. The result depends on the icon you dragged and the object on which you dropped it. If the operation that is performed takes more time, the message `In Progress` appears.

Note: In a Hub Level view, after you drop a resource on an object, the Information Area sometimes waits a few seconds before displaying the results of the operation. If you drag another resource while the first operation is being performed, information on the results of the operation may appear when information on the second resource is being displayed.

Menus

In Nways Manager-LAN, menus contain options relevant for the currently selected object. Options which are not available for the selected object are shown in reduced highlight.

Nways Manager-LAN uses two types of menus:

- Pull-down menus from the menu bar that are displayed when you press MB1 on the menu name.
- Context menus displayed when you press MB3 on an icon. Context menus are only present when the cursor changes to a small hand when over an object icon.

  Functions contained in context menus are performed on the object that the context menu is attached to and are different for each type of object icon.

Using LAN and Hub Management Panels

When you use Nways Manager-LAN to configure and monitor network resources or troubleshoot problems, management data is displayed in a set of panels that contain information about a selected object. The panels may include tables, graphs, and data entry forms. You can also navigate from one resource management panel to another without returning to a submap.

The menu bar provides access to functions relevant for a resource, such as enabling and disabling a port or starting and stopping a diagnostic routine. Information to identify the resource, such as a MAC address or segment number, and resource name are displayed below the menu bar.

The Attributes section contains a mixture of read-only and read-write fields that display the current values of the parameters. When you click on the name of a field, context-sensitive information about the field is displayed in the Information area.

The following pushbuttons are displayed in the action line at the bottom of the panel:

- **OK** - Accepts the information in the panel (including any changes) and closes the panel.
- **Apply** - Accepts the information in the panel (including any changes) but does not close the panel. Data entered in a configuration panel has no effect until you click on the **Apply** button.
- **Reset** - Changes any parameter values that were modified to the values that were last saved by clicking on **Apply**.
- **Refresh** - Updates information on the panel with information obtained from the latest poll.

  Configuration information is polled regularly or on request. If the information in a panel is not current, click on **Refresh** to update it.
- **Close** - Quits a panel with read-only information.
- **Cancel** - Quits a panel with read-write information. You lose changes that you did not save by clicking on **Apply**.
- **Help** - Displays help information about the panel.

Depending on the information in the panel, some of the pushbuttons may not be displayed in the action line.

Using Pushbuttons to Navigate Between Panels

To navigate between management panels containing configuration information on hub modules, ports, and trunks, use the following pushbuttons:

- On Module Configuration panels, the navigation pushbuttons are **Port Form** and **Trunk Form**. Click on these buttons to display the configuration panel for the first port (or the first trunk) on the selected module.
- On Port Configuration panels, the navigation pushbuttons are **<< Port >>**. Click on **<<** to display the configuration panel for the previous port. Click on **>>** to display the configuration panel for the next port.

  If the panel for the first port is displayed, clicking on **<<** displays the panel for the last port on the module. Similarly, if the panel for last port is displayed, clicking on **>>** displays the panel for the first port.
- On Trunk Configuration Forms, the navigation pushbuttons are **<< Trunk >>**. Click on **<<** to display the configuration panel for the previous trunk. Click on **>>** to display the configuration panel for the next trunk.

  If the panel for the first trunk is displayed, clicking on **<<** displays the panel for the last trunk on the module. Similarly, if the panel for last trunk is displayed, clicking on **>>** displays the panel for the first trunk.

You can access configuration information for ports and trunks on the backplane (not visible on the faceplate of the module) as follows:

1. Click on the **Port Form** or **Trunk Form** pushbutton on the Module Configuration panel.
2. Click on **<<** or **>>** in the **<< Port >>** or **<< Trunk >>** buttons until the configuration panel for the port or trunk is displayed.

Getting Help

Nways Manager-LAN help information is available at three levels:

- Field help

  Context-sensitive field help is available by clicking on the name of the field in a panel. Information about the selected field is displayed in the Description area at the bottom of the panel.
- Panel help

  Context-sensitive panel help is available by clicking on the Help pushbutton at the bottom of the panel. Information about the purpose of the panel, each field in the panel, and how to use the panel to perform a task is displayed in a separate window.
- NetView for AIX indexes

  Help information about all applications currently installed in NetView for AIX, including all Nways Manager-LAN applications, is available by selecting **Help -> Indexes -> Applications**. from the menu bar.

  To display a list of help topics about the management tasks you can perform on LAN resources, select **Help -> Indexes -> Tasks**.

To display a list of help topics for the functions you can access to manage 8250, 8260, and 8265 resources, select **Help -> Indexes -> Functions**.

- Online documentation

  To display online documentation on Nways Manager-LAN, select: **Help -> Campus Manager - LAN User's Guide**.

For some Nways Manager-LAN executables, daemons, and processes, you can display online reference information (called a *man page*) using the AIX **man** command. The **man** command displays a man page for a specified topic.

To display a man page for a Nways Manager-LAN topic, enter the following command from an AIX operating system shell:

```
man <topic>
```

where `<topic>` is the AIX name (for example, `cmld`) of the executable, daemon, or process.

For more information on the daemons and processes used by the Nways Manager-LAN applications, 8250, 8260, and 8265 Device Manager and LAN Network Manager, see the online books **Troubleshooting 8250, 8260, and 8265 Devices** and **Troubleshooting Token-Ring and FDDI Resources**.

Legend Panel

To get help on the icons and color-coded statuses used in Nways Manager-LAN, select **Help -> Legend** from the menu bar in a Hub Level or Module Level view. This displays the Legend panel.

The Legend panel displays all the icons used to represent modules, daughter cards, connectors, LAN networks, devices, hub objects, and operational statuses. Use the scroll bar to view the remaining icons on the panel.

Hub Icons

Besides the icons displayed in "Legend Panel", Nways Manager-LAN also uses the icons shown in this section to represent 8250 and 8260 hubs and 8265 ATM switches. Icons for the following hubs are used to configure and manage network resources:

- 8250 Model 006
- 8250 Model 6HC
- 8250 Model 06S
- 8250 Model 6PS
- 8250 Model 017
- 8250 Model 017LS
- 8260 Model 007

- 8260 Model 010
- 8260 Model 017
- 8265 Model 17S

In addition, if you have installed the corresponding PSM with Nways Manager-LAN, the icons of PSM-managed hubs and switches also appear in the user interface.

8250 Hub Model 006

The 8250 Hub Model 006 is a basic, six-slot IBM 8250 chassis represented in the IBM Hubs Topology:

By clicking on the icon, you can open the hub.

8250 Hub Model 6HC

The 8250 Hub Model 6HC is a basic, six-slot IBM 8250 chassis with a hidden controller which can be with or without redundancy. It is represented in the IBM Hubs Topology.

By clicking on the icon, you can open the hub.

8250 Hub Model 6PS

The 8250 Hub Model 6PS is a six-slot IBM 8250 chassis with an integrated IBM PS/2. It is represented in the IBM Hubs Topology.

8250 Hub Model 017

The 8250 Hub Model 017 is a 17-slot IBM 8250 chassis that is represented in the IBM Hubs Topology.

By clicking on the icon, you can open the hub.

8260 Hub Model 007

The 8260 Hub Model 007 is a 7-slot IBM 8260 chassis and is represented in the IBM Hubs Topology.

By clicking on the icon, you can open the hub.

8260 Hub Model 010

The 8260 Hub Model 010 is a 10-slot IBM 8260 chassis and is represented in the IBM Hubs Topology.

By clicking on the icon, you can open the hub.

8260 Hub Model 017

The 8260 Hub Model 017 is a 17-slot IBM 8260 chassis and is represented in the IBM Hubs Topology.

By clicking on the icon, you can open the hub.

8260 Hubs Managed by an ATM Switch

If no DMM module is installed in an 8260 hub, the hub can be managed by an ATM Switch module (Version 2.3 or later) that contains a subset of the DMM MIB. This allows the ATM Switch module to act as the master management module. In this case, the hub is displayed in the IBM Hubs Topology.

8265 ATM Switch Model 17S

The 8265 ATM Switch is a 17-slot chassis with ATM backplane and is represented in the IBM Hubs Topology.

By clicking on the icon, you can open the device.

Unreachable Hubs

When a hub becomes unreachable, it is displayed with a red icon.

Hubs With Failed Critical Resources

When a hub has one or more critical resources that have failed, it is displayed with the failure icon.

Status of Hub and LAN Resources

The network resources that you manage with Nways Manager-LAN are represented graphically by icons. The NetView for AIX graphical interface displays these icons on submaps.

The status of the managed resource is indicated by the color of its icon on the submap. You can control how the icon color is set by specifying the status aggregation scheme for the object. For more information, see “Defining Status Aggregation” on page 37.

Also, you can customize how you want individual hub resources to be monitored. The values you set affect how the compound hub status is calculated. For more information, see ″Monitoring Hub Resources″ in the online book **Managing 8250, 8260, and 8265 Devices**.

Color-coded Status of Icons

The current status of network resources is indicated by the color of their icons. Table 2 describes what each status means and which color is, by default, associated with it.

Table 2. Color-coded Status of Hub and LAN Resources

Status (Color)	**Meaning**
Unknown (Blue)	The status of the resource cannot be determined or the resource is not being monitored either because it has not been discovered or because the connection with its managing agent has been lost.
Normal (Green)	The resource is in a normal operational state.
Unmanaged (Brown)	The resource has been removed from network management by an operator action.
Marginal (Yellow)	The operation of a resource is impaired but still functional.
Critical (Red)	The resource has lost its network connection and is not functional.
Disabled (Grey)	The resource has been de-activated by an operator action or an agent request. The resource's status is not taken into account when a compound status is calculated.
User1 (default color defined by NetView for AIX)	The resource is temporarily not responding to SNMP requests, but is still connected to the network and responds to a ping. To display the current color, open the Legend window by selecting **Help -> Legend**. To customize the color, log on as root and follow these steps: 1. Open the file /usr/OV/app-defaults/OVw. 2. Scroll to the field `OVw*user1StatusColor` and enter a new value for the color. 3. Restart the NetView for AIX interface to activate the change.

The default colors for Nways Manager-LAN icons are the same as for NetView for AIX.

Using NetView for AIX, you can change the color that represents each status, except for Unknown which is always shown in blue. For information about how to change the default colors, see the *NetView for AIX User's Guide*.

Defining Status Aggregation

The status of an icon represents an aggregation of the resources that constitute that icon. For example, the icon for an FDDI segment in a LAN Network submap displays the compound status of the workstations, concentrators, and bridges that constitute the segment. Similarly, the icon for an individual resource, such as a workstation, represents the status of the workstation's MAC, ports, and other internal components.

Through NetView for AIX, you can customize the status aggregation policy for your network environment. You can also generate compound status for icons. The following list describes the types of status you can generate when you customize the status aggregation policy:

- Default compound status is the default status policy used by NetView for AIX to determine how to represent a parent icon when the icons in its child submap change status. For example, if the status of some of the icons in the child submap are normal and others become marginal, the parent icon changes to marginal. If at least one icon in the child submap is critical and no icon is normal, then the parent icon changes to critical.
- Propagate most severe compound status indicates that the aggregation policy bases its color according to the most severe status among the collected objects.
- Propagate at threshold value compound status indicates that the aggregation policy bases its color according to the percent of aggregated objects with a status of marginal or critical.

To specify the compound status policy, use the NetView for AIX graphical interface. When you set a status aggregation policy, it applies to all submaps that are displayed by NetView for AIX, including those that are generated by Nways Manager-LAN. For information about changing the compound status policy, refer to the *NetView for AIX User's Guide*.

Resources that have an unknown or unmanaged status do not affect status aggregation. For example, if one workstation in a Segment submap displays a critical status and the rest of the resources on that segment are unknown or unmanaged, the segment displays a critical status.

Chapter 6. Using Submaps

Nways Manager-LAN provides a variety of submaps that display detailed views of the network resources you are managing. The top-level, or Root submap, displays icons representing the communication protocols and IBM hubs used in your network.

From the Root submap, you can navigate through hierarchies of submaps to manage your network resources. Each submap provides an increasingly detailed view of network resources.

- To manage hub resources, double-click on the IBM Hubs Topology icon. This allows you to access the submap hierarchy for 8250, 8260, and 8265 Device Manager. For more information, see “Navigating through Different Hub Views”.
- To manage resources according to the LAN subnet or standalone segment to which they belong, double-click on the LAN icon. This allows you to access the submap hierarchy for LAN Network Manager. For more information, see “Navigating through LAN Submaps” on page 47.

To manage network resources that use other communication protocols, such as IP or SNA, double-click on the appropriate protocol icon in the Root submap. This allows you to access the submap hierarchies provided by NetView for AIX and other AIX applications.

Note: To configure SNMP parameters for hub agents, select **Options -> SNMP Configuration** from the menu bar of the Root Submap. Any changes you make to hub agents are displayed in the Configuration panels for the corresponding hub view.

Navigating through Different Hub Views

Nways Manager-LAN displays the following views for managing your 8250, 8260, 8265, PSM-managed, and Java web-managed devices:

Type of View	Resources Displayed
IBM Hubs Topology	All 8250, 8260, 8265, PSM-managed, and Java web-managed devices
Hub level	Modules and power supplies installed in 8250, 8260, or 8265 devices with the status of fans, temperature, and power supplies.
Module level	Ports, trunks, and devices attached to an 8250, 8260, or 8265 module

To move between different views, double-click the left mouse button on an object in the view. For example, start from the IBM Hubs Topology, double-click on a hub to explode the hub and display a Hub Level view. In the Hub Level view, double-click on the icon of a module to explode the module and display a Module Level view.

Each type of hub view is described in the following sections.

IBM Hubs Topology

After you double-click on the IBM Hubs Topology icon in the Root submap, the IBM Hubs Topology is displayed. This view displays all the 8250, 8260, 8265, and PSM-managed and Java web-managed devices with the inter-hub links in the network that you manually added.

New hubs are placed in the submap as soon as they are discovered.

- To create connections between hubs shown in the IBM Hubs Topology, use the **Add Object Connection** function in NetView for AIX.
- To change the names of hubs in the IBM Hubs Topology, you must enter a new parameter in the Hub Label field in the Hub Configuration panel. See the online book **Managing 8250, 8260, and 8265 Devices** for details.
- To reorder the hubs in the IBM Hubs Topology, turn off the automatic layout function. See the *NetView for AIX User's Guide* for details.

Managing Hubs

You can explode a hub only when the hub is *managed*. For managed hubs, all menu items and configuration panels for the hub are available. If the polling policy is *regular*, the hub is polled according to the number of seconds configured for its polling interval. The hub symbol in the IBM Hubs Topology changes color to reflect changes in hub status as reported by the poll.

To manage one or more hubs:

1. Open the IBM Hubs Topology with read-write access.
2. Select the hub you want to manage by clicking it with the left mouse button. To select two or more hubs, hold down the left mouse button and drag the mouse so that the hub icons are highlighted.
3. Select **Options -> Manage** from the menu bar. The color of the selected hub(s) changes to blue (unknown) until the next poll is performed. As polling results are received, managed hubs change color to report their status.

Unmanaging Hubs

An unmanaged hub is not managed by Nways Manager-LAN. This means that the hub is not polled despite the polling policy (for example, *regular*) that is currently configured. All configuration panels are disabled and the Hub Level view cannot be opened. The hub icon in the IBM Hubs Topology does not report the hub's status because it is not known. The hub icon, however, remains visible.

To unmanage one or more hubs:

1. Open the IBM Hubs Topology with read-write access.
2. Select the hub you want to unmanage by clicking it with the left mouse button. To select two or more hubs, use a left mouse drag.

3. Select **Options -> Unmanage** from the menu bar. The color of the selected hub(s) changes to brown (unmanaged).

When the next poll is performed, the hub is discovered as *unmanaged* and is polled once. The hub, however, remains in the unmanaged state. No menu options are available on its context menu.

Managing and Unmanaging All Hubs

To manage or unmanage all hubs in the IBM Hubs Topology:

1. Click the left mouse button on the IBM Hubs Topology icon in the Root submap to select it.
2. Select **Options -> Manage** or **Options -> Unmanage** from the menu bar.

Executable Devices

8250, 8260, 8265, PSM-managed, and Java web-managed devices are executable when there is a square, three-dimensional frame around their icons in the IBM Hubs Topology.

- For 8250, 8260, and 8265 devices, you can display the Hub Level view by double-clicking on the hub icon. See “Hub Level View” on page 42 for more information.
- For other PSM-managed hubs and switches, you can start the PSM by double-clicking on the icon.

If an error message is displayed the first time you double-click on a PSM-managed icon, this means that you have not yet registered the device to the Management Application Transporter. To do so, follow these steps:

1. Select the Device icon.
2. From the menu bar, select **Tools->Management Application Transporter->Change Subsystem**.
3. In the Change Subsystem Panel, click on **Device IP Address**. The PSM associated to this icon is highlighted.
4. Click on the PSM to register it for this device.

For more information on using the Management Application Transporter, refer to the documentation stored in **/usr/lpp/mgtapptran/doc**. To display online help for a particular PSM, enter the following command:

```
/usr/lpp/mgtapptran/bin/viewDoc docname
```

where `docname` is the name of the online document (for example, R8224UG).

Note: If you double-click on a hub icon that is not executable (that does not have the three-dimensional square frame around it), the NetView for AIX view of the hub’s interfaces is displayed. See the *NetView for AIX User’s Guide* for more information.

Hubs Managed by Nways Manager-LAN

Each type of hub managed by Nways Manager-LAN is displayed in the IBM Hubs Topology by an icon that represents the physical characteristics of the hub. For example, you can see icons for the following:

- IBM 8250 Model 006 - Basic IBM 8250 six-slot hub (horizontal)
- IBM 8250 Model 006HC - IBM 8250 six-slot hub with a hidden controller and redundancy (horizontal)
- IBM 8250 Model 6PS - IBM 8250 six-slot hub with an integrated IBM PS/2 and redundancy (horizontal)
- IBM 8250 Model 017 - Basic IBM 8250 17-slot hub (vertical)
- IBM 8250 Model 017LS - IBM 8250 17-slot hub with load sharing power distribution board (vertical)
- IBM 8260 Model P07 - IBM 8260 seven-slot hub.
- IBM 8260 Model 010 - IBM 8260 10-slot hub (vertical) with TriChannel backplane
- IBM 8260 Model A10 - IBM 8260 10-slot hub (vertical) with TriChannel and ATM backplane
- IBM 8260 Model P10 - IBM 8260 10-slot hub (vertical) with TriChannel and PacketChannel backplane
- IBM 8260 Model 017 - IBM 8260 17-slot hub (vertical) with TriChannel backplane
- IBM 8260 Model A17 - IBM 8260 17-slot hub (vertical) with TriChannel and ATM backplane
- IBM 8260 Model G17 - IBM 8260 17-slot hub (vertical) with TriChannel, PacketChannel, and ATM backplane
- IBM 8260 Model P17 - IBM 8260 17-slot hub (vertical) with TriChannel and PacketChannel backplane
- IBM 8265 Model 17S - IBM 8265 17-slot ATM switch containing DMM subset with TriChannel and ATM backplane

The icons used to represent each of these hubs are displayed either horizontally or vertically.

Hub Level View

The Hub Level view displays the modules installed in a selected hub and is opened when you:

- Double-click on a hub icon in the IBM Hubs Topology or the IP Internet Submap.
- Select **Open View** from the HubManager menu.

The status of modules is color-coded in compliance with NetView for AIX.

When you open a Hub Level view, a forced poll is performed.

A pop-up window is displayed if you open the Hub Level view for a hub that is in one of the following states:

- The first poll is running.
- There is an error in the first poll.
- The hub is unmanaged.
- The master agent is no longer the master.

Depending on whether the hub is an 8250, 8265, or an 8265 ATM switch, the number and type of icons displayed at the bottom of the view differs:

- 8250 Hubs have the following icons displayed:
  - One Power Supply icon for each power supply installed.
  - One fan icon to reflect the overall fan status.
  - One temperature icon to reflect the overall temperature.

    The hub temperature is not necessarily related to the status of the fans. It reflects the overall temperature as collected by the various temperature probes.
  - For IBM 8250 17-slot hub with load sharing (that is, containing a load sharing power distribution board) a PDB icon is shown to reflect the LS-PDB status.
  - For IBM 8250 6-slot hub with an integrated PS/2, a PS/2 icon is shown that displays the status of the cards in the PS/2.
- 8260 hubs and 8265 ATM switches have the following icons displayed:
  - One Power Supply icon for each power supply installed.
  - One fan icon to reflect the overall status of the cooling fans.
  - One temperature icon to reflect the overall temperature.

A special icon is displayed to identify broken connections. When this icon appears, the corresponding hub icon becomes red in the Network Level View. When a connection no longer exists with a hub, you can still expand the hub by double-clicking on the hub icon and displaying the Hub Level View. The information displayed is the last known configuration of the hub. A logo is displayed that reflects the chassis's type.

Double-clicking on the icon above a module in the Hub Level view or selecting **Open View** from the module's context menu displays the Module Level view.

Information Area

To display information about a color-coded hub resource, click MB1 on an icon. Information about the resource and polling information are displayed in the Information area at the bottom of an expanded Hub Level View.

If the resource is configured for Regular Polling, the polling interval set in the Polling Policy panel is displayed with the date and time of the previous poll. If the resource is configured for Polling on Request, the date and time of the previous poll is displayed.

Network Area

Using the Network area on the right side of an expanded Hub Level View, you can list the network segments attached to the hub according to network type. To do so, click

MB1 on one of the Network icons. For example, if you click on Token-Ring, a second box opens showing the Token-Ring segments attached to the hub.

To highlight the hub resources assigned to a specific network, click MB1 on one of the icons in the second box. All other resources, except for fans, power supplies, temperature, PS/2, and power distribution boards, are displayed in reduced highlight.

To redisplay all highlighted hub resources, click on the **Show All** button. To display the context menu for a network segment, click MB3 on one of the Network icons in the second box.

Also, you can use the Network area as a drop site for assigning hub resources to a network segment. To do so, drag an icon (for example, a port) in the Hub Level view and drop it on the icon of a network segment.

Unrecognized Modules

Unrecognized modules installed in 8250 and 8260 hubs and 8265 ATM switches are displayed in a Hub Level view and are represented by the icon for `Unrecognized Module` shown in the Legend panel.

There are three categories of unrecognized modules:

1. The master agent cannot recognize the module because the version of the module is not supported. To check this:
   a. Open a telnet session with the master management module.
   b. Enter the command `show module all`.
   c. See if the name of the unrecognized module appears in the list. If not, the master agent does not support the module.
2. The version of Nways Manager-LAN that you are running does not support the module.
3. The module is not an ATM module and is installed in an 8260 hub managed by an ATM Switch (A-CPSW) module Version 2.3 (or higher) that contains a subset of the Distributed Module Management (DMM) functionality. The A-CPSW module recognizes only the slot number of non-ATM media modules.

You can perform a limited set of management functions on unrecognized modules and view only a limited amount of configuration information:

- You can set unrecognized modules of Types 1 and 3 only to their DIP switch settings.
- You can reset unrecognized modules of Types 1 and 2 by means of the master management module using telnet.
- You can configure unrecognized modules of Type 2 using telnet.

Generically Managed Modules

Modules installed in 8250 and 8260 hubs and 8265 ATM switches may be managed in a generic way and are represented by the icon for `Generic Support`.

Modules may be generically supported for either of the following reasons:

1. The module is not fully supported by the version of the master agent. The version of the master agent is displayed in the Module Configuration panel and in the information area of the Hub Level view by clicking on the master agent module's icon.
2. The module is a newly released module that is supported by the version of the master agent, but not yet supported by the version of Nways Manager-LAN that you are running.

The generic functions that you can perform on these modules are as follows:

- Display the slot index, version, vendor, module class, and whether or not this module has been configured using the telnet function.
- Enable and disable ports and trunks (if the Enable and Disable functions are supported).
- Display all configuration parameters in the Module Configuration panel or by selecting **Hub -> Show -> Show Modules**.
- Reset the module (if the Reset function is supported).
- Display the operational status in the Hub Level view.

Note that in a Hub Level view:

- The icons displayed for generically supported modules are empty.
- The ports and trunks of generically supported modules are not displayed. To view configuration information, you must display the Module Configuration panel.
- No Module Level views exist for generically managed modules.

Module Level View

The Module Level view displays an expanded view of the selected module. It provides module-specific information and information about the devices attached to the module.

The Module Level view is dynamically updated according to the MAC address polling policy when stations are moved, added, or removed.

The Module Level view contains:

- A background picture of the selected module which occupies the whole window but which does not have an icon on the top.

  Note: The module is shown either horizontally or vertically depending on the type of chassis.
- Icons representing the ports and trunks belonging to the module. A triangle shown over a port icon indicates that the port is a redundant backup port.

These ports and trunks are the same as those shown in the unexpanded view of the module including the same port menu structure and the same status. For modules which contain banks, all the banks are automatically expanded to show all the ports they contain.

- Icons representing devices (workstations, routers, bridges, or others) that are connected to the module ports.

  Notes:

  1. Attached devices may not be shown if the network to which a bridge or router is connected is managed by a TRMM for which you have not defined read-write access in the TRMM's Community Table for the management station running Nways Manager-LAN.
  2. Attached devices may also not be shown if the segments in the hub are not correctly attached. For example, two segments in a hub must be bridged and not connected by trunks.
  3. Station or device icons can only be seen if a Token-Ring or Ethernet management module is connected to the segment.
  4. Station or device icons are not supported on FDDI media modules.
  5. If an Ethernet station is moved from one port to another port, the original port position is kept until the agent is reset or a new station is connected to the original port. Both addresses are shown in the Search panel and in the Module Level view.

A line is shown between the device icon and the port it is connected to, representing the connection between the port and the device.

You can associate names to different devices to help in problem determination and to easily locate resources using the Search function.

You can display other views associated with the device by double-clicking on the device icon. The status of the ports is updated when the corresponding port status is updated in the Hub Level view. There is no particular relationship between port status and station status. The device status is the status reported by either the 8250, 8260, and 8265 Device Manager or (if installed) the LAN Network Manager application of Nways Manager-LAN.

Management Modules

The network icon representing the type of protocol used in the LAN segment is displayed in the bottom righthand corner. To open the submap of the segment managed by the module, select **LAN** from the icon's context menu.

Bridge Modules

In the Module Level view of a Bridge module, the network icon representing the type of protocol used in the LAN subnet is displayed in the bottom righthand corner. To open the submaps in which the bridge is displayed, select **LAN** from the icon's context menu.

ATM Switch Modules

You can open the Nways Manager-ATM view of the ATM cluster managed by the A-CPSW switch by selecting **Open Device** from the icon's context menu.

Navigating through LAN Submaps

Nways Manager-LAN displays the following submaps for managing your LAN resources:

Type of Submap	Resources Displayed
LAN Network	LAN subnets, including stand-alone segments
LAN Subnet	Segments and bridges that make up a particular subnet
Segment	Bridges, concentrators, and stations, including proxy agent stations
Bridge	Bridge interfaces and attached segments
FDDI Station	Managed elements of an FDDI station, including ports, SMT, attachment, MAC, path, and path class
Interface	Bridge ports and the interface protocol operating on those bridge ports
Node	The protocol operating on the selected station or bridge interface
Concentrator	Managed elements of concentrators, such as lobe attachment modules, lobe insertion units, ports, and adapters

To navigate from one submap to another, double-click on an explodable icon that represents a network resource. Double-clicking on an explodable icon opens a submap associated with the icon. For example, if you double-click on a segment icon in a LAN Subnet submap, a Segment submap for the selected segment is displayed.

The following sections describe the hierarchy of LAN submaps used in Nways Manager-LAN.

LAN Network Submap

After you double-click on the LAN icon in the Root submap, the LAN Network submap is displayed. This submap displays the subnets managed by the LAN Network Manager application of Nways Manager-LAN.

- Each triangular icon represents a LAN subnet that is an aggregation of LAN segments interconnected with bridges or switches that run the same Spanning Tree (ST) algorithm.

- Each circular icon represents a stand-alone segment that is not connected to another segment by a known bridge or switch. Undiscovered SNMP bridges are also grouped in a triangular subnet icon.

The naming conventions used in the LAN names below each icon are as follows:

- For a LAN subnet (circular icon) in which the Spanning Tree algorithm is running in all bridges and switches used to interconnect segments in the subnet, the LAN name is the MAC address of the *root bridge*. The root bridge is one of the bridges in the subnet. The MAC address used as the LAN name is one of the MAC addresses of the root bridge.

  When a segment is managed by a token-ring RMON agent, the name is in the format: `RMON <agent_IP_address>-<segmentIndex>`

  When a segment is managed by a token-ring 8230 agent, the name is in the format: `CAU <agent_IP_address>`

  When a segment is managed by a token-ring surrogate agent, the name is in the format: `<surrSegmentNumber>`

  When a segment is managed by an FDDI proxy agent, the name is in the format: `<agent_IP_address>-<segmentIndex>`
- The icon named `Standalone subnet` contains the bridges and switches that interconnect segments in which the Spanning Tree algorithm is not running.
- The icon named `Undiscovered bridges` contains the bridges that have not been successfully discovered or polled by Nways Manager-LAN.
- For a LAN subnet (triangular icon) managed by an LNM OS/2 agent, the name is either the IP address of the agent or the LAN name defined for the OS/2 agent.

For some types of LAN subnets, you can select the subnet icon and then select **Configuration** from the LAN pull-down menu to display and change configuration parameters. From the LAN Network submap, you can also double-click on a subnet icon to open the LAN Subnet submap that displays the network resources in the subnet.

Notes:

1. In order to display the status of all stations connected to a standalone segment in the LAN Segment submap, an agent (probe), such as token-ring surrogate, 8230, or RMON, must be active on the segment.
2. The lnmbrmon daemon reports the status of SNMP bridges taken into account to generate the compound status of a LAN subnet. The status of a LAN subnet is displayed by its color-coded icon. To check the status of the lnmbrmon daemon, enter the command:

   ```
   /usr/CML/bin/cmlstatus lnmbrmon
   ```

LAN Subnet Submap

The LAN Subnet submap provides a detailed view of a selected subnet. The different types of LAN segments (token-ring, FDDI, and Ethernet) and the bridges and switches that connect them are represented with icons.

You can display the resources in a particular segment by double-clicking on a segment icon to open a Segment submap.

You can display the ports and attached segments of a particular bridge by double-clicking on the bridge icon to open a Bridge submap.

Segment Submap

The LAN Subnet submap can display segment icons for LLC token-ring, SNMP token-ring, and FDDI segments. If the stations on a segment have been discovered, you can double-click on the segment icon to open a Segment submap.

Other segment types, such as Ethernet, X.25, and Frame-Relay, can also be represented by icons in the LAN Subnet submap, but because they are not managed by the LAN Network Manager application, you cannot display a Segment submap for these types of segments.

For LLC token-ring, SNMP token-ring, and FDDI segments, the Segment submap shows a detailed view of the resources on a specific segment. Stations, bridges, and concentrators are represented by icons placed around a ring. Stations that are operating a proxy agent program, such as the OS/2 agent or the FDDI SNMP Proxy Agent, are displayed with a oval icon to distinguish them from other stations, which are represented by square or diamond-shaped icons.

The Segment submap for LLC token-ring segments shows the stations, bridges, and 8230 Model 1 and Model 2 concentrators on the selected segment, displayed in nearest active upstream neighbor (NAUN) order, according to their adapters. (Adapters integrated in an 8230 Model 1 or Model 2 concentrator are not displayed in the Segment submap; they are displayed in the Concentrator submap.)

The Segment submaps for FDDI and SNMP token-ring segments are similar to the Segment submap for LLC token-ring segments. Stations, bridges, and concentrators are displayed in NAUN order clockwise, according to their MAC addresses.

Note that the station 08005ADB0044 has an oval icon to indicate that the station is running the proxy agent program.

From any type of LAN Segment submap, you can determine the current status of a resource by its color, obtain profile, configuration, fault, and performance information for a resource, and navigate to a Node, Bridge, or Concentrator submap for a detailed view of a particular resource.

FDDI Station Submap

For FDDI networks, you can open an FDDI Station submap to display the managed elements of an FDDI station. To do so, double-click on an FDDI station in an FDDI Segment submap. The FDDI Station submap opens to display a graphical representation of a computer workstation. Icons representing the SMT, attachment, MAC, path, path class, and ports are displayed in the submap.

From the FDDI Station submap, you can determine the current status of a resource by its color, and obtain profile, configuration, fault, and performance information for a resource. You can also double-click on the MAC icon to open a Node submap for the selected station.

Node Submap

The Node submap displays icons that represent the contents of a station or a bridge port, according to protocol. Each Node submap contains one or more icons: one icon to represent the selected station or bridge port, and one icon to represent each protocol present in the station or bridge port.

From the Node submap, you can determine the current status of a resource by its color, and obtain profile, configuration, fault, and performance information for a resource.

Bridge Submap

Nways Manager-LAN uses a Bridge submap to represent bridges, such as the IBM 8229 and 8250. The Bridge submap displays a graphical representation of the bridge, with icons representing the bridge port interfaces, the segments to which the bridge is attached, and the bridge itself.

From the Bridge submap, you can determine the current status of each bridge port interface by its color, and obtain profile, configuration, fault, and performance information for these elements using the management windows. Double-clicking on the icons that represent a bridge port interface opens a Node submap for the bridge port.

Note: In Bridge submaps, realistic views of SNMP bridges have been replaced by a generic view that allows you to represent multiple segments on the same interface. Realistic views are still available by double-clicking on the bridge icon to start the Product Specific Module.

Concentrator Submap

To represent the IBM 8230 Model 1 and Model 2, the IBM 8240 and 8244 concentrators, and generic FDDI concentrators, Nways Manager-LAN uses a Concentrator submap.

The Concentrator submap displays a graphical representation of the concentrator itself. Points of attachment and other physical features of the hardware are recognizable in the submap, and all managed elements of the concentrator are represented by icons. The icons give you access to the managed elements of the device and to the stations inserted into the device.

For the SNMP-managed IBM 8230, Nways Manager-LAN invokes the Product Specific Management applications. Online documentation of applications associated with these devices can be viewed by entering

```
/usr/lpp/mgtapptran/bin/viewDoc <docname>
```

where *docname* is the name of the online documentation that you want to view.

Switching Between Different Protocol Views

In Nways Manager-LAN, you can switch between any of the following views according to the protocols that are running in a selected hub or LAN resource:

- IP Internet submap
- LAN submaps
- 8250, 8260, and 8265 views
- Nways Manager-ATM submaps

To switch between different protocol views of a network resource,

1. Do one of the following:
   - Display the context menu for a selected hub or LAN resource and select **Nways Protocols**.
   - From the menu bar of the hub view, LAN submap, or IP submap, select **View -> Nways -> Nways Protocols**.

   Nways Protocols allows you to switch between the following submaps: IP Internet submap, Nways Manager-ATM, LAN, or hub view.
2. In the dialog box, select a protocol and the submap that you want to display.
3. Click **Open**.

For example, if you switch to a view of a hub according to its IP address, a submap is displayed.

From the IBM Hubs Topology view and IP and LAN submaps, you can manage network resources in the following ways:

- Click on a hub or LAN resource to select it and select an operation from the **Administer** menu.
- Press **Ctrl** and click the left mouse button (MB1) on each resource you want to manage. Then select an operation from the **Administer** menu.

Note that you can also select operations from the context menu of a selected hub. To display a context menu, click the right mouse button (MB3) on a resource icon.

Navigation Between Hub Views and LAN Submaps

To navigate between hub or module views and LAN submaps, do one of the following:

1. From a LAN submap to a Hub Level view:
   - Double-click on a hub icon in the LAN Segment submap to display the Hub Level view of the hub. The modules attached to the segment are highlighted.
   - Double-click on the hub icon displayed at the top of an integrated 8250/8260 SNMP bridge in a Bridge Device submap to open the Hub Level view.

2. From a Module Level view to a LAN submap:
   - Double-click on the resource (station, bridge, or segment icon) attached to a port in the Module Level view.
   - Display the context menu of a resource (station, bridge, or segment) in the Module Level view and select **Nways Protocols**. Then select and open the LAN submap that you want to view.

     Note: Navigation between LAN submaps and hub views is not supported for token-ring segments discovered by the LNM OS/2 proxy agent.
   - For the 8260 Switching Module Series, display the context menu of a port on the module and select **Nways Protocols**. Then select and open the LAN submap that you want to view.

Merging LAN Submaps

Nways Manager-LAN receives information from a variety of sources in the network, such as SNMP proxy agent programs and SNMP bridges. In many cases an agent can operate in the same LAN environment as another agent and not be aware of the other agent's function. Nways Manager-LAN processes information from both agents, building separate topological submaps of the agent-reported resources.

To create a more accurate depiction of the network, Nways Manager-LAN checks for this kind of overlap, and if the program discovers a match, it merges the submaps that are represented through the respective agents into a single submap. When this happens, it is common for a duplicate icon that represents a merged segment to be removed from a higher-level submap. This does not mean you lose access to the merged resources; the updating of the submaps simply provides a cleaner and more comprehensive navigation path to the resources in your network.

The merging process occurs automatically when Nways Manager-LAN detects a situation that requires it. Nways Manager-LAN records all merges in the event display.

Note: The reporting policy of each agent can be in canonical or non-canonical format and may impact the automatic merging process that normally occurs. You can change the format in which token-ring RMON agents report their MAC address as follows:

1. Start SMIT by selecting **Administer -> Campus Manager SMIT** from the NetView for AIX menu bar.
2. Select **Configure -> Configure SNMP token-ring capability -> Configure IBM SNMP token-ring proxy agent -> RMON**.
3. Enter the IP address of the RMON agent and press Enter or select **OK**.
4. Enter a new value (canonical or non-canonical) for the **RMON agent MAC address display policy** parameter.

For more information, see the online book **Managing SNMP Token-Ring Resources and SNMP Bridges**.

Disabling a Token-Ring SNMP Agent

For token-ring segments managed by different types of SNMP proxy agents, you may sometimes want to disable the discovery of one or more agents in the following situations:

- When a fault in the agent prevents LAN submaps to be merged
- When you want to disable an agent with a higher priority so that the information supplied by an agent with a lower priority is used when the segment is discovered. The priority in which token-ring SNMP agents are discovered is:
  1. Token-ring surrogate
  2. RMON
  3. SNMP-managed 8230

For example, you may have dual reporting on the same token-ring segment if the following devices are running:

- 8230 Model 4 concentrator with RMON capability enabled
- 8260 hub with TMAC installed and token-ring surrogate and RMON capabilities enabled

If the two submaps generated by the different agents do not merge, you can solve the problem by disabling one or more of the SNMP token-ring agents that report information about the segment.

To disable the discovery of a token-ring SNMP proxy agent:

1. Enter `smit cml` to start SMIT.
2. Select **Configure -> Configure SNMP token-ring capability**.
3. Select the type of proxy agent that you want to disable.
4. Enter the IP address of the agent.
5. In the **Manage this agent** field, select **No** and click on **OK**.
6. Do one of the following:
   - Stop and restart the lnmtrmon daemon by entering the following commands:

     ```
     /usr/CML/bin/cmlstop lnmtrmon
     /usr/CML/bin/cmlstart lnmtrmon
     ```

   - Delete and then rediscover the agent by entering the commands:

     ```
     cml_agent_delete <agent_IP_address>
     cml_agent_add <agent_IP_address>
     ```

For more information, see the section “Configuring SNMP Agents that Manage Token-Ring Segments” in the online book **Managing SNMP Token-Ring Resources and SNMP Bridges**.

Merging Example: SNMP Bridge and Segment

In your network, an SNMP bridge might be connected to segment 005, which is monitored by a token-ring SNMP proxy agent. Before merging takes place, the bridge

and the segment are both represented in the LAN Network Submap by different icons. If you navigate to the LAN submap or the Bridge submap for the bridge, segment 005 is shown to be connected to the bridge, but the bridge cannot provide detailed information about the segment or its stations.

When performing management functions, Nways Manager-LAN matches the MAC address of one of the bridge's adapters with the MAC address of an active station reported on segment 005. Once this match is identified, Nways Manager-LAN merges the submaps that pertain to the bridge and segment 005. To accurately show the topology, Nways Manager-LAN moves the segment submap to the Bridge submap.

Now when you navigate to the LAN Subnet submap or Bridge submap, you can display the stations on segment 005 by double-clicking on the segment icon. Management functions for the bridge and segment are available from the same submap.

Merging Example: Two Agents, Same Segment

In this example, there might be two SNMP agents that are connected to segment 040 in your network. One is a token-ring SNMP surrogate agent residing in an IBM 8229 Bridge that is connected to the segment, and the other agent is a token-ring SNMP RMON agent that is running on a workstation connected to the segment. Both agents are providing Nways Manager-LAN with information about the segment and the stations of which they are aware. Before merging takes place, Nways Manager-LAN displays a subnet icon for each agent on the LAN Network submap. The LAN submaps show different views of the same segment, according to the management information supplied by each agent.

While correlating the list of MAC addresses in the network, Nways Manager-LAN matches the MAC addresses of stations reported by the token-ring surrogate agent with the MAC addresses of stations reported by the RMON agent. If there are less than 6 stations on a segment, Nways Manager-LAN matches all (100%) of those stations with stations on the other segment before initiating merging. If there are 6 or more stations on both segments, Nways Manager-LAN matches at least half (50%) of the stations before merging. After the matching conditions are met, Nways Manager-LAN merges the submaps that are related to the two agents by eliminating the icon that represents the RMON agent.

For the purpose of merging, Nways Manager-LAN always gives management priority to a token-ring surrogate agent, instead of an RMON agent, when both agents are present on the same segment. Segment 040 is now presented through a single icon, and the duplicate submaps are eliminated. In addition, only SNMP is managing the segment, eliminating duplicate traps and improving performance.

Unmerging LAN Submaps

Although the secondary agent on the segment has been merged with the primary agent, the secondary agent still operates as a backup. If the primary agent loses connectivity, Nways Manager-LAN indicates this by changing the agent's status to Unknown and initiating an age-out timer. After you delete the agent, or after the age-out timer expires, the secondary agent assumes management and updates the Nways Manager-LAN submaps with its own information.

For example, suppose you have a token-ring surrogate agent and an RMON agent reporting on the same segment. Merging has already occurred, so the RMON agent's icon has been removed and merged with the token-ring surrogate's icon. If Nways Manager-LAN loses communication with the token-ring surrogate, and you delete the surrogate agent, a new Segment submap is created based on the RMON agent and its information about the stations on the segment.

To delete a token-ring surrogate agent, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Delete SNMP Agent**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Control -> Delete SNMP Agent**.

For more information, see the online book **Coupling and Autodiscovery**.

Customizing LAN Submaps

In Nways Manager-LAN, icons (symbols) representing LAN resources are automatically positioned on submaps if the automatic layout is set to `On`. As new resources are discovered (for example, by polling information), new icons are added and the group of icons on the submap is automatically repositioned.

Nways Manager-LAN allows you, however, to customize the icon positions on Subnet, Segment, and Bridge submaps that display point-to-point connections (for example, a bridge connected to a segment). To do so, you must select a background for the submap by choosing **Edit -> Select Background Picture** from the menu bar. Then follow these steps:

1. Make sure that the automatic symbol layout is turned off by selecting **View -> Automatic Layout -> For This Submap -> Off For This Submap** from the menu bar.
2. Drag the icons to their desired positions by pressing Ctrl and holding down the middle mouse button (MB2).

   Note: The Cut, Copy, and Paste functions in NetView for AIX are not supported.
3. Select **View -> Nways -> Save Symbols Positions**.

As new resources are discovered, their icons are placed in the New Object Holding area at the bottom of the submap. To position the new icons, use a mouse drag as described in Step 2 on page 55.

After changing icon positions on a submap, you can restore the last saved positions by selecting **View -> Nways -> Place Symbols Positions**.

To delete the last saved positions for a submap, select **View -> Nways -> Clear Symbol Position -> For This Submap**.

Part 3. Network Resources

Chapter 7. 8250, 8260, and 8265 Architectures

Hub Architectures

8250 Hubs and 8260 Hubs are used to connect end-stations, servers, and other shared devices to form local area networks (LANs). The hub may include management modules, media modules (concentrators, transceivers, and repeaters) terminal servers, bridges, routers, ATM Switches, and controllers. Controllers are the only mandatory module. Each hub must have at least one controller.

Bridge and Router modules can be used to connect segments within the same hub, to other LANs, and to wide area networks (WANs). The terminal server module can be used to connect several terminals to any network node, providing network connectivity for dumb terminals.

Several types of media (for example UTP, STP, and fiber) and connectors (for example RJ-45S, BNC, and fiber) are supported. Using the appropriate cabling, end stations can be connected to media modules. Some modules can also be used to extend the LAN between hubs.

All modules are hot swappable. Modules that support fault tolerance can have dual links and backup ports.

Depending on the type of module, there are three types of switching that can be used:

- Per-module switching (PMS) - All ports on the module are assigned to the same network at the same time.
- Per-port switching (PPS) - Each port on the module can be individually assigned to a segment.
- Per-connector switching (PCS) or per-bank switching (PBS) - All ports on a connector or bank are assigned to the same network at the same time. Each connector can be individually assigned to a segment.

8250 Hub Architecture

The architecture used by the 8250 Hub allows up to three Ethernet, four FDDI, or seven Token-Ring networks to run in a single hub. Modules operating under each of these protocols will operate simultaneously in the same hub.

Modules operating under each network provide exceptional flexibility for load balancing and network changes. Additionally, you can isolate a module from the backplane so that its ports can communicate without passing through the backplane. In the case of per-port switching (PPS) modules, you can select the ports you want to isolate without isolating every port on the module.

8260 Hub Architecture

The architecture used by the 8260 Hub supports ATM and allows up to eight Ethernet, four FDDI, or seventeen Token-Ring networks to run in a single hub. Modules operating under each of these protocols will operate simultaneously in the same hub.

Additionally, you can configure different isolated networks on the same module so that the ports assigned to these networks communicate without impacting the backplane and other isolated segments on the module.

The 8260 Hub also provides a cost-efficient management architecture that consolidates media management in a single card, the Distributed Management Module (DMM).

8265 ATM Switch Architecture

The 8265 ATM switch is a modular chassis that is based on the 8260 ATM architecture with increased (four times more) switching capacity. The 8265 architecture is designed to meet the requirements of the next generation of high-end ATM backbone networks by providing high aggregate throughput and high-speed port density.

Besides being used as a backbone switch, the 8265 can also be used as a building switch for native ATM/LAN switching. It allows you to interconnect ATM network protocols and is fully compatible with existing 8260- and 8285-based ATM networks.

The 8265 architecture combines the strengths of single stage switching, distributed buffer pools, and ATM traffic management. In addition to the support of all ATM Class of Services (CBR, VBR, ABR and UBR), the 8265 provides advanced traffic management functions, such as traffic shaping at VP level, statistics at connection level, traffic policing, and port mirroring. The 8265 supports a very rich set of ATM interfaces, signalling, and PNN1-1 features.

The 8265 provides:

- Integrated bridging and routing
- Integrated LAN emulation client server
- High call set-up rate
- Up to 16 000 bi-directional virtual connections
- PBX attachment via multiple T1/E1 interfaces
- Switched LAN ports for attached LAN servers
- WAN feeder ports (T1/E1, DS3/E3, OC-3, and STM-1)
- OC-12 ports (STS-12c or STM-4c) for inter-building connections
- OC-3 ports to attach floor switches and servers
- Support of ATM Forum interfaces and qualities of service
- Conformance to PNN-I standards, all UNI levels
- High availability and hot-plugging of components.
- High level ATM signalling performance and robustness

The 8265 supports 8260 ATM modules as well as 8265-specific ATM modules, including:

- Multiprotocol Switched Services (MSS) modules
- MPEG-2 Video Distribution module
- Circuit emulation modules
- ATM WAN modules (E3, DS3, E1, DS1, J1, and others)
- 1-port 622 Mbps modules
- 4-port 155 Mbps modules
- 12-port 25 Mbps modules
- 8271 ATM Ethernet LAN Switch modules
- 8272 ATM Token-Ring LAN Switch modules
- 8281 ATM LAN Bridge modules
- Modules developed under the ATM kit program

The 8265 brings a set of new enhanced ATM control and traffic management capability. These functions are fully distributed on each 8265 module as opposed to a centralized function residing on switching fabric. The distribution of functions is the key to network availability, scalability, and growth. It offers consistent performance whatever the number of the module or port. These functions are located in an ATM engine present on every ATM module and consisting of one VLSI module (for higher performance and port density) and two FPGA modules for openness to future extensions.

Accessing 8250 and 8260 Hubs and 8265 ATM Switches

There are four possible interfaces when remotely accessing 8250 and 8260 hubs and 8265 ATM switches over the network :

1. Out-of-band connection is provided by connecting an ASCII terminal (locally or remotely) to the RS-232 or RS-423 connector on the front of a Management module in the hub. This provides a text interface.

   Note: One connection is required for each agent to be controlled.
2. Inband connection is provided by connecting a TCP/IP station to a Management module in the hub. This connection can use Telnet and TFTP protocols and provides a text interface.

   Note: One connection is required for each agent to be controlled.
3. Inband connection is provided by connecting an SNMP Management Station or NetView for AIX station to a Management module in the hub. This connection can use SNMP protocol.

   Note: This provides a centralized focal point to access all the hubs and uses a graphical interface.
4. Inband connection is provided by connecting a TCP/IP station running NetView for AIX and Nways Manager-LAN to a Management module in the hub. This connection uses the SNMP protocol.

Note: This provides a centralized focal point to access all the hubs and uses a graphical interface.

Chapter 8. Agent Modules

8250, 8260, and 8265 management is performed by means of the Simple Network Management Protocol (SNMP). Modules with firmware that implements SNMP support SNMP management. In Nways Manager-LAN documentation, these modules are called *agents*.

8250, 8260, and 8265 Device Manager recognizes the following agents:

- 8250 Hub agents:
  - Token-Ring Management modules (TRMM)
  - Ethernet Management modules (EMM)
  - FDDI Management modules (FMM)
  - Terminal Server modules
  - Ethernet and Token-Ring Bridge modules
  - Router modules
  - 8235 Token-Ring/Ethernet modules
  - Ethernet RMON Multiprobe modules.
- 8260 Hub agents:
  - Any 8250 Hub agent
  - Distributed Management Modules (DMM) with a network monitor card (NMC) that can be one of the following:
    - Ethernet medium access card (E-MAC)
    - High-End Ethernet medium access card (HE-EMAC)
    - Token-Ring medium access card (T-MAC)
    - High-End Token-Ring medium access card (H-TMAC)
  - ATM Control Point and Switch (CPSW) modules
  - Ethernet Bridge modules
  - Router modules
  - Multiprotocol Switched Services (MSS) Server modules
  - 8281 ATM LAN Bridge modules
  - Switching Module Series that function as bridges allowing devices of various media types to communicate
  - LAN Switch modules
  - ATM/LAN Switch modules
- 8265 Switch agents:
  - ATM Control Point and Switch (A-CPSW) modules that contain a subset of the DMM MIB and provide full management of an 8265 ATM switch
  - Multiprotocol Switched Services (MSS) Server modules
  - 8281 ATM LAN Bridge modules
  - Switching Module Series that function as bridges allowing devices of various media types to communicate

– ATM/LAN Switch modules

8250 Management Modules

Management modules are the basis of 8250 network management. They provide a management interface that can be accessed locally through a terminal connected to the serial port (out-of-band) or inband through the network. 8250 Management modules are available for Ethernet (EMM), Token-Ring (TRMM), and FDDI (FMM) protocols. Refer to the Installation and Operating Guides shipped with your Management modules for a complete description of specific features supported by the software version of your module.

Functions common to all supported 8250 Management modules include:

- Compliance with industry standards such as IEEE 802.x, TCP/IP, Telnet (except EMM V2.0), SNMP, and TFTP (except EMM basic and FMM V1.01).
- Supporting Telnet to allow remote login to a Management module on the network and manage it from a remote Management module or a workstation with Telnet support.
- Monitoring and controlling the configuration of the hub, modules, and ports.
- Monitoring activity in the hub.
- Monitoring port and module status.
- Continuous monitoring and reporting of key network fault statistics to give a snapshot of the network and real-time information about hardware failures.
- Inband and out-of-band network management such as download features.
- Automatic detection of faults and failures including responding as an agent to SNMP requests and generating SNMP traps.
- Security control.
- TriChannel** Architecture support and fault tolerance capabilities.

The Management modules control the configuration of all the modules in a hub. Whenever a Management module is present and operating in a hub, the software management settings for individual media modules determine the configuration. The DIP switch settings are ignored.

An 8250 Management module can manage only one network at a time. If you need to simultaneously monitor traffic on two or more networks, you must add additional Management modules. If you need simultaneous management of multiple networks, you should dedicate a Management module to each network. When the hub includes more than one Management module, one of these modules becomes the master and handles all control and configuration functions. The Master Management module is chosen on the basis of an assigned mastership priority. If multiple Management modules have the same priority, an arbitrary selection is automatically made.

For box management, any type of Management module can be used to control modules for any network supported by the 8250 Hubs. For MAC-specific processing, such as gathering statistics, a dedicated Management module of the same LAN type is needed.

In other words, an EMM cannot gather statistics for a Token-Ring module. Likewise, a TRMM or FMM cannot gather statistics for an Ethernet module.

8260 Distributed Management Modules

Distributed Management Modules (DMMs) are the basis of 8260 network management. They provide a management interface for the same functions as for 8250 Management modules, plus the following:

- Storing configuration information that can be used to automatically configure a new module that is replacing a module of the same type.
- Providing complete inventory of the hub's contents, including fans and power supplies.
- Managing low power situations.
- Monitoring network status.

The 8260 Distributed Management Module (DMM) is a Management module designed to work in 8260 Hubs. The DMM enables you to fully manage and control your hub down to port level. In addition, the DMM contains monitoring and control capabilities (when used with IBM Network Monitor Cards) which allow you to configure and check the status of all Token-Ring and Ethernet modules in an 8260 Hub.

The main features of the DMM include all the features available for 8250 Management modules. Also, the DMM:

- Provides a cost-efficient management architecture that consolidates media management in a single card, while distributing network monitoring across a series of Network Monitor Cards (NMCs) which can be Ethernet medium access control (E-MAC), High-End Ethernet medium access control (HE-EMAC), Token-Ring medium access control (T-MAC), or High-End Token-Ring medium access card (H-TMAC) cards.

  E-MAC and HE-EMAC cards can be physically attached to any 8260 media module or Ethernet Distributed Management module installed in the hub. T-MAC and H-TMAC cards attach to any 8260 Token-Ring media module. These protocol-specific cards monitor all activity on a network, gathering statistics and reporting them to the protocol-independent Management module.
- Works with the controller to protect network integrity using power management. The DMM also has a command to implement fault tolerant power which allows the hub to reserve some of its power capacity to protect against a power supply failure.

You can install all 8250 modules, except for Controller modules, in an 8260 Hub by using an adapter kit.

8260 ATM Control Point and Switch Module

The 8260 ATM Control Point and Switch (A-CPSW) module Version 2.3 or higher allows you to manage all ATM resources in an 8260 hub using Nways Manager-LAN. The A-CPSW module manages all ATM modules by means of a subset of the DMM MIB installed in the module and is called the ATM Management Module (AMM).

An A-CPSW module Version 2.3 or later can be the master management module in an 8260 hub **only** if no DMM or Advanced Controller module is installed.

8265 ATM Control Point and Switch Module

The 8265 Control Point and Switch (CPSW) module operates like the 8260 ATM Control Point and Switch (A-CPSW) module. This means that the 8265 CPSW acts as the master management module and manages all ATM modules by means of a subset of the DMM MIB. This allows 8265 ATM switches to be managed by Nways Manager-LAN.

Chapter 9. Configuring Network Resources

This chapter describes how to configure your network resources. To perform most of these tasks, you use panels to enter the necessary information. For some functions, such as monitoring hub resources, creating logical LANs, and assigning resources to networks, you can use a drag and drop.

The following objects can be configured using a drag and drop or by selecting the Configuration menu option:

- Networks
- Hubs
- Modules
- Daughter cards: security and Medium Access Control (MAC) cards
- Ports
- RS-232 and RS-423 connectors (TTY)
- Trunks
- Power supplies
- Fan
- Temperature
- Power distribution boards (PDBs)

Configuration information is obtained by polling the Master Management module for the hub and the relevant agents, when required. If you think that the information displayed is not current, click on the **Refresh** button in the panel. This forces polling of the management module to display current data.

Configuring Networks

To configure an 8260 Token Ring network, do one of the following:

- Select a line shown in the Token-Ring Network Information List (see “Listing Ethernet and Token-Ring Networks” on page 92) and click on the **Configure** pushbutton.
- Double-click MB1 on a hub icon in the IBM Hubs Topology. On the right of the Hub Level view in the Network box, click MB1 on the TR 8260 icon. In the list of 8260 Token Ring networks, click MB3 on one of the network icons and select **Configuration** from the context menu.

  Note: You can only configure the 8260 Token Ring backplane networks using this method.

A configuration panel is displayed.

You can change the following for the selected network:

- Speed

- Mismatch Resolution
- Beacon Recovery.

Configuring Hubs

The color of the hub in the IBM Hubs Topology is an aggregate of the status for each module, power supply, fan, temperature, and power distribution board (PDB) in the hub. By default, the compound status of each hub is calculated by treating the status of each resource equally:

- If all resources are red, the compound hub status is red.
- If all resources are green, the compound hub status is green.
- Otherwise, the compound hub status is yellow.

If you use the Resource Monitor to change the default setting, a hub's compound status is calculated as described in "Monitoring Hub Resources" on page 84. The Resource Monitor allows you to fine tune the way in which the status of individual resources affect the compound hub status.

Hubs can be configured by:

- Selecting **HubManager -> Configuration** from the menu bar in the Root window.
- Selecting **Hub -> Configuration** from the menu bar in a Hub Level view.

Using the Hub Configuration panel, you can set a hub's label and the location and contact for the Master agent.

Note: The Master Agent Location and Master Agent Contact fields accept up to 127 alphanumeric characters.

This is the only way you can modify the hub label to give the hub a more suitable identifier. The default hub label is the host name of the Management module that was master when the hub was discovered.

When you change the hub label in the Hub Configuration panel, the hub label in the IBM Hubs Topology is automatically updated. The title of the Hub Level view, the Module Level view, and the Hub Configuration panel are also updated.

When you remove a hub from the topology database or clear the database, the hub label reverts to the default.

Note: Before changing the hub label in a Hub Configuration panel, do a search on the new label name you want to use to ensure that the name has not already been assigned.

Configuring Modules

In a Hub Level view, the color of a module icon represents the module's current status. A module's status is calculated by taking:

- The compound status of each port, trunk, bank, and daughter card (the module's children)
- The value of the module's ModStatus MIB variable as shown in Table 3.

To display information about the current value of the ModStatus MIB variable, click on the module's icon. Information on the ModStatus MIB variable is displayed in the information area at the bottom of the Hub level view.

Table 3. Module Status

ModStatus	**Color**
OK (1)	Green
FatalError (10)	Red
Booting (20)	Yellow
PartialFailure (21)	Yellow
UnknownStatus (26)	Blue
NotInserted (30)	Yellow
SpeedMismatch (31)	Yellow
TransientError (37)	Yellow

If Nways Manager-LAN is not coupled with Nways Manager-ATM, the status of each ATM module and port is **unknown** (blue) in a Hub Level view.

If Nways Manager-LAN is coupled with Nways Manager-ATM, Nways Manager-ATM reports only the status of ATM ports and Nways Manager-LAN reports the status of ATM modules as **unknown**. Because the status of ATM modules is **unknown**, the compound status of each ATM module is calculated by taking into account the status of each ATM port on the module. If an ATM module has no port, the status of the module is displayed as **unknown** (blue).

The status of a module is displayed in the following ways:

- By the color of the module's icon in a Hub Level view
- In the information area at the bottom of a Hub Level view when you select the module's icon.

Important: The compound status of a module is not affected by the settings you configure for children (ports, trunks, banks) in the module using the Resource Monitor. This function is described in "Monitoring Hub Resources" on page 84.

To configure a module, click on the module icon in a Hub Level view and select **Configuration** from the context menu. The Module Configuration panel is displayed. The module's slot number and the hub label is displayed in the title bar.

Notes:

1. For modules that are per-module switching, you can also change the network assignment by dragging and dropping the module icon on a network icon in a Hub Level view. See "Assigning a Resource to a Network" on page 82 for more information.
2. To change the way in which all children (ports, trunks, banks) in the module are configured for resource monitoring, drag and drop the module icon on a Resource Monitor icon in a Hub Level view. See "Configuring How Resources Are Monitored" on page 85 for more information.

Managing New Modules

The functions which are available for a particular module depend on how the master management module sees the module. There are two special settings for new modules: *unrecognized* and *generically managed*. (*Generically managed* is sometimes called *Unknown* on an ASCII terminal.)

In a Hub Level view, unmanaged modules are displayed with the icon for Unrecognized Module (as shown on the Legend panel).Modules are unmanaged when:

1. A new module is inserted in the hub but the existing agent does not recognize it.
2. A new agent and a new module are inserted in the hub but neither are known by the 8250, 8260, and 8265 Device Manager program that is currently running. To manage these modules, use the Hub Manager Telnet function on the Master Management module.

In a Hub Level view, partially managed modules are displayed with the icon for Generic Support (as shown on the Legend panel). You can perform the following actions from the context menu of a partially managed module by clicking on the module's icon:

- Reset and re-assign the module using the Master Management module.
- Display the slot index, version, vendor, module class, and whether or not this module has been configured.
- Configure general parameters for ports and trunks.
- Display the module's status.
- Display the Module Configuration panel and configure ports and trunks by clicking on the **Port Form** and **Trunk Form** pushbuttons.

Managing 8260 Ethernet Carrier DMM Modules

Because the 8260 Ethernet Carrier DMM module functions as part of a standalone DMM and a standalone Ethernet Carrier module, it is managed by Nways Manager-LAN in a specific way.

To display the tasks available for managing an 8260 Ethernet Carrier DMM module, display the module's context menu by clicking on the module's icon in a Hub Level view.

Managing 8260 Advanced DMM Modules

The IBM 8260 Advanced DMM module is installed in subslot 2 on an Advanced Controller module.

To perform management tasks on an Advanced DMM module, display the module's context menu by clicking on the daughter card in subslot 2 of an Advanced Controller module in a Hub Level view.

Managing Multiprotocol Switched Services Modules

To fully manage Multiprotocol Switched Services (MSS) modules, you must use the Device Management application for the 8210 Multiprotocol Switched Services (MSS) Server.

To start the Device Management application, select **Device Management** from the context menu of an MSS module in a Hub Level view.

Managing 8271 and 8272 Switch Modules

Nways Manager-LAN allows you to manage the following types of 8271 Ethernet and 8272 Token-Ring Switch modules:

- 8271 Ethernet LAN Switch module

  The 8271 Ethernet LAN Switch module is the integrated version of the standalone IBM 8271 Nways LAN Switch. By using Ethernet MAC addresses to forward Ethernet frames between ports, the 8271 module can accommodate any type of LAN segment to provide a high-performance switching solution. No direct ATM backbone connection is provided.
- 8271 ATM/Ethernet LAN Switch module

  The 8271 ATM/Ethernet LAN Switch module includes all the functions of the 8271 Ethernet LAN Switch module and also provides direct ATM backbone connectivity. This allows users connected to an Ethernet segment to interconnect to other Ethernet segments by means of LAN switching or high-speed ATM switching.
- 8272 Token-Ring LAN Switch module

  The 8272 Token-Ring LAN Switch module is the integrated version of the standalone IBM 8272 Nways LAN Switch. By using Token-Ring MAC addresses and source route descriptors to forward Token-Ring frames between ports, the 8272 module provides a high-performance switching solution. No direct ATM backbone connection is provided.
- 8272 ATM/Token-Ring LAN Switch module

  The 8272 ATM/Token-Ring LAN Switch module includes all the functions of the 8272 Token-Ring LAN Switch module and also provides direct ATM backbone connectivity.

This allows users connected to a Token-Ring segment to interconnect to other Token-Ring segments by means of LAN switching or high-speed ATM switching.

8271 and 8272 modules can be used in either two-slot or three-slot versions. In a Hub Level view, both the two-slot and the three-slot versions of 8271 and 8272 modules are displayed as occupying two slots.

To attach additional LAN segments, you must install Universal Feature Cards (UFCs): up to four UFCs in three-slot versions and up to two UFCs in two-slot versions.

Managing 8271 and 8272 ATM LAN Switch Modules

To display the management tasks available for an 8271 or 8272 ATM LAN module, display the context menu by clicking on the module's icon.

To display the status of the ports and the UFCs installed in a module, click on the port or UFC icon on the faceplate of the module.

The additional UFCs and ports are then displayed.

In order to fully manage an 8271 or 8272 ATM LAN Switch module, you must carry out these steps:

1. Install the Product Specific Module (for example, the 8271 or 8272 PSM) as described in the *IBM Nways Manager Installation Instructions (4304036)*.
2. Start the PSM by selecting **Device Management** from the module's context menu.

Managing 8271 Ethernet and 8272 Token-Ring LAN Switch Modules

8271 Ethernet and 8272 Token-Ring LAN Switch modules that do not have ATM backplane connections are displayed without ports in Hub Level views.

In order to manage these modules, you must configure the module's IP address. To do so, select **Configuration** from the module's context menu and enter the IP address in the Module Configuration panel.

Then you must carry out these additional steps:

1. Install the Product Specific Module (for example, the 8271 or 8272 PSM) as described in the *IBM Nways Manager Installation Instructions (4304036)*.
2. Start the PSM by selecting **Device Management** from the module's context menu.

Configuring Virtual Bridges Using Switching Modules Manager

A *virtual bridge* is a user-defined group of ports in the 8260 Switching Modules Series that supports IEEE 802.1D bridging functions. A virtual bridge allows you to create workgroups of network devices that are attached to multiple modules in the Switching Modules Series and that use different types interfaces (Ethernet, FDDI, or ATM). A

virtual bridge can contain ports on more than one module; a port on a module in the Switching Modules Series, however, can belong to only one virtual bridge.

To configure the Switching Modules Series to create virtual bridges, you use the Nways Switching Modules Manager (NSMM). To start Switching Modules Manager, do one of the following:

- From the NetView for AIX Root submap, choose **Hub Manager -> Nways Switching Module Manager -> Start Switching Module Mgmt**.
- From a Hub Level view, choose **Control -> NSMM** from the menu bar or from the context menu of a port on a module in the Switching Modules Series.

For information on how to use Nways Switching Modules Manager to create and use virtual bridges, see the *IBM Nways Switching Modules Manager User's Guide* shipped with modules in the 8260 Switching Modules Series.

Configuring Daughter Cards

To configure a daughter card, click on its icon in a Hub Level or a Module Level view and select **Configuration** from the context menu. A Daughter Card Configuration panel is displayed. The module's slot number and the hub label is displayed in the title bar.

Notes:

1. The NMC may be a Media Access Control (MAC) card or a security card.
2. To change the network assignment of a daughter card, you can also drag and drop the card's icon onto a network icon in a Hub Level view. See "Assigning a Resource to a Network" on page 82 for more information.

Configuring Ports

Nways Manager-LAN supports a variety of port types such as BNC, AUI (male and female), fiber, DB-9, RJ-45, and so on. Each connector type can have devices attached and can be assigned to a network.

The color of a port indicates its status and is based on a generic PortStatus MIB variable. The rules shown in Table 4 apply.

Table 4. Port/Trunk Status

Port/Trunk Status	Color
Okay_Standby	Green
Backup_Line	Green
Off (22)	Grey
local/remote linkFailure (4/2)	Red
fatalError (10)	Red
Partition (11)	Red

Table 4. Port/Trunk Status (continued)

Port/Trunk Status	Color
Beacon (27)	Red
WireFault (28)	Red
speedMismatch (31)	Red
invalid_impedance	Red
beacon_wrapped	Red
Okay-standby/backup-link (18/24)	Specific icon. (See Note 1.)
unknownStatus (26)	Blue
attach3174toxxx (33/34/35)	Blue
forwarding	Green
blocked	Green
listening	Yellow
learning	Yellow
All the rest	Yellow

Notes:

1. A redundant backup port is indicated in a Hub Level view with a small triangle displayed over its port connector. By clicking on the connector of a backup port, you display the slot and port number of the primary port in the Information area at the bottom of the panel.
2. On per-port switching modules, you can also change the network assignment of ports by dragging and dropping the port icon onto a network icon in a Hub Level view. See “Assigning a Resource to a Network” on page 82 for more information.
3. On 8260 FDDI Switching Series modules, port status is represented logically; that is, the color of the port represents the compound status of the two connectors (Media Access Units) in the port. You can configure each FDDI connector separately by choosing options from the port’s context menu. Also, you can configure each FDDI logical port as a critical resource by following the procedure in “Assigning a Resource to a Network” on page 82.

To configure a port, double-click on its icon or click once on the icon in a Hub Level or a Module Level view and select **Configuration** from the context menu. A Port Configuration panel is displayed. The port’s number, the module’s slot number and the hub label are displayed in the title bar.

Because hidden (backplane or virtual) ports do not have an icon, follow these steps to open a Port Configuration panel:

1. Open the Module Configuration panel for the module on which the hidden ports are located.
2. Click on **Port Form**.
3. Use the **<< Port >>** buttons to navigate through Port Configuration panels until you find the currently configured parameters for each hidden port.

The value displayed in the Monitoring field is the way that the port is configured for resource monitoring. To change this value, do one of the following:

- Select another value from the list box in the Monitoring field.
- Drag and drop the port icon onto a Resource Monitor icon in the corresponding Hub Level view. See “Configuring How Resources Are Monitored” on page 85 for more information.

If the value in the Monitoring field is *Critical*, the port is protected from undesired user action. You are automatically prompted to confirm any changes you make to the port parameters.

If Nways Manager-ATM is not installed and coupled with Nways Manager-LAN, the status of ATM ports is always *Unknown*. If Nways Manager-ATM is installed, the status of ATM ports is reported by Nways Manager-ATM.

Table 5 shows how the status of LAN ports displayed on the Port Configuration panel in Nways Manager-LAN corresponds to the operational state of ATM interfaces displayed in the ATM Interface Configuration panel in Nways Manager-ATM.

Table 5. Status of LAN Ports and Operational State of ATM Interfaces

Status of LAN Ports (Nways Manager-LAN)	**Operational State of ATM Interfaces (Nways Manager-ATM)**
unknownStatus	unknown
off	disabled-nosignal
off	disabled-idle
noPhantom	nosignal
noPhantom	idle
fatalError	idle
okay	in-service
okay	pvcOnly
fatalError	failing
fatalError	misConfigured
fatalError	wrong-network-prefix
fatalError	wrong-node-number

Configuring Redundancy for Ethernet Ports

Using the Port Configuration panel, you can configure redundancy for pairs of Ethernet ports. Each pair of redundant ports consists of a primary and a backup port. The configuration of a backup port ensures Ethernet data transmission if the primary port is inoperational.

To configure redundancy for a pair of Ethernet ports:

- Configure the primary port by selecting **Redundant_primary** in the Port Mode field. Then enter the slot and port number of the backup port in the Buddy Port field .

- Configure the backup port by selecting **Redundant_backup** in the Port Mode field of the configuration panel of the backup port. Then enter the slot and port number of the primary port in the Buddy Port field.

Important: When configuring redundant pairs of Ethernet ports, make sure that you configure only one port as the *Redundant_primary* and only one port as the *Redundant_backup*. If you configure more than one redundant backup port, unpredictable results can occur in your Ethernet network.

You can use critical resource settings to secure read-write access to pairs of Ethernet ports (backup and primary) in a redundant link. For example, if you configure a port as a *critical* resource, a message is displayed before port configuration parameters are changed to warn users that the port is a critical resource.

Configuring Serial Ports

The serial ports on 8250 and 8260 Management modules allow you to connect a terminal and directly manage the module. There are two types of serial ports:

- RS-232 (Console Port) - Used by the 8250 EMM, TRMM, FMM, and other agents.

  Serial ports cannot be assigned to networks. They are only used to connect ASCII terminals either locally or remotely via a modem.
- RS-423 (Auxiliary Port) - Used by the 8260 DMM.

  Used to connect the DMM to a terminal or modem so that you can enter management commands and download software.

To display ASCII terminal interface configuration (TTY) information, click on the RS-232 connector icon on a Management module in a Hub Level view and choose **Configuration** or double-click MB1 on a TTY port.

The Terminal Interface panel is displayed.

Configuring Trunks

The color of a trunk indicates its status and is based on a generic trunkStatus MIB variable. The rules shown in Table 4 on page 75 apply.

To configure a trunk, double-click on its icon or click once on the icon in a Hub Level view and select **Configuration** from the context menu. A Trunk Configuration panel is displayed.

Notes:

1. To change the network assignment of a trunk in a PPS module, you can also drag and drop the trunk icon onto a network icon in a Hub Level view. See “Assigning a Resource to a Network” on page 82 for more information.

2. To change the way in which a trunk is configured for resource monitoring, drag and drop the trunk icon on a Resource Monitor icon in a Hub Level view. See “Configuring How Resources Are Monitored” on page 85 for more information.

Configuring Power Supplies

To configure a power supply, double-click on its icon or click once on the icon in a Hub Level view and select **Configuration** from the context menu. A Power Status panel displayed.

The Power Status panel displays information about the overall status of the power supplies in the selected hub and allows you to set the PS Mode of the selected power supply.

The value displayed in the Monitoring field is the way that the power supply is configured for resource monitoring. To change this value, do one of the following:

- Select another value from the list box in the Monitoring field.
- Drag and drop the power supply icon onto a Resource Monitor icon in the corresponding Hub Level view. See “Configuring How Resources Are Monitored” on page 85 for more information.

If the value in the Monitoring field is *Critical*, the power supply is protected from undesired user action. You are automatically prompted to confirm any changes you make to the power supply parameters.

Configuring Fans

To check the status of fans in a hub and to configure a fan for resource monitoring, open the Hub Level view and do one of the following:

- Select **Configuration** from the context menu of a fan icon.
- Double-click MB1 on a fan icon.

The Fan Status panel is displayed.

The Fan Status field displays the overall status of fans in the selected hub. This value is calculated by taking the individual status of each fan. If one fan is faulty or inoperational, the overall fan status is *faulty*. The overall fan status is *OK* only if no fan reports a problem.

The value displayed in the Monitoring field is the way that the fan is configured for resource monitoring. To change this value, do one of the following:

- Select another value from the list box in the Monitoring field.

- Drag and drop the fan icon onto a Resource Monitor icon in the corresponding Hub Level view. See “Configuring How Resources Are Monitored” on page 85 for more information.

If the value in the Monitoring field is *Critical*, the fan is protected from undesired user action. You are automatically prompted to confirm any changes you make to the fan parameters.

Configuring Hub Temperature

To check the temperature in a hub and to configure it for resource monitoring, open the Hub Level view and do one of the following:

- Select **Configuration** from the context menu of a temperature icon.
- Double-click MB1 on a temperature icon.

The Temperature Status panel is displayed. This panel displays the overall status of all temperature probes in the hub.

The value displayed in the Monitoring field is the way that the temperature is configured for resource monitoring. To change this value, do one of the following:

- Select another value from the list box in the Monitoring field.
- Drag and drop the temperature icon onto a Resource Monitor icon in the corresponding Hub Level view. See “Configuring How Resources Are Monitored” on page 85 for more information.

  If the value in the Monitoring field is *Critical*, the temperature is protected from undesired user action. You are automatically prompted to confirm any changes you make to the temperature parameters.

Configuring Power Distribution Boards

To check the status of a power distribution board (PDB) and to configure it for resource monitoring, open the Hub Level view and do one of the following:

- Select **Configuration** from the context menu of a power distribution board.
- Double-click MB1 on the icon of a power distribution board.

The value displayed in the Monitoring field is the way that the PDB is configured for resource monitoring. To change this value, do one of the following:

- Select another value from the list box in the Monitoring field.
- Drag and drop the PDB icon onto a Resource Monitor icon in the corresponding Hub Level view. See “Configuring How Resources Are Monitored” on page 85 for more information.

If the value in the Monitoring field is *Critical*, the PDB is protected from undesired user action. You are automatically prompted to confirm any changes you make to the PDB parameters.

Grouping Ports

To perform a management action on more than one port at a time, you can configure a group of ports belonging to different slots under the same logical name.

Port grouping is only supported for the following modules:

- TRMM Advanced modules V2.1 or higher
- DMM V2.0 and higher.

To group ports, select **Hub -> Control -> Port Grouping** from the menu bar of a Hub Level view. A panel is displayed.

You can perform the following actions on the ports in a selected group:

- Add or delete ports from the group.
- Enable or disable all ports in the group.
- Clear all ports from the group.
- Graphically display ports within a group.

To select a group of ports, open the list box in the Group ID field and click on a group name. The ports currently assigned to the group are displayed at the bottom of the panel according to the slot number.

Notes:

1. Some port numbers may be displayed in parentheses. This means that in the current hub configuration, the ports either do not exist or are no longer valid. This condition occurs when the module containing the port is removed from the hub or inserted in a different slot. To remove the invalid ports from the group, select **Non-existing Ports** from the list box in the Slot field and then click on **Delete from group**.
2. If you select **All** from the Group ID list box, only the Delete operation is available. If you select **Delete**, you can only delete the following ports:
   - All non-existing ports
   - All ports from all slots.

   By deleting all non-existing ports, you ensure that the list of ports displayed on the panel contains only valid ports. By deleting all ports from all slots, you remove the group name from the Group ID list.
3. An asterisk (*) next to a port means that the port is protected.
4. Backplane ports are not listed in the Port Selection area.

When the selected group is displayed in the list box area, you can do the following:

- Enable all ports in the group.
- Disable all ports in the group.
- Show a graphical view of the group. This highlights all the ports in the group in the Hub Level view.

  To disable the resulting display in the Hub Level view either:

  – Exit from the Port Grouping panel.

  – Select **All** from the parameter list associated with the Group ID field and click on the **Show** pushbutton.

If the group assignment no longer corresponds to your logical view of the group, you can assign ports to the group or delete ports from the group as follows:

- Assign to Group - Select a valid slot number from the pull-down menu associated with the Slot field and select either **All Ports** or a specific port that is to be added to the group. Then press the **Assign to group** pushbutton. The assignment is automatically registered in the master agent in the network and the list box is refreshed with the new assignment for this group.
- Delete from Group - Select either a valid slot number from the pull-down menu associated with the Slot field or **All Ports of All Slots**. Select either a specific port number or **All Ports of this Slot**. Then press the **Delete from group** pushbutton. The contents of the list box area are refreshed with the new assignment for this group.

Note: To see the result on the Hub Level view press the **Show** pushbutton.

Assigning a Resource to a Network

Besides using a Configuration panel, you can also use a drag and drop to assign the following resources to a network:

- Modules
- Daughter cards
- Ports
- Trunks.

To assign a resource to a network, follow these steps:

1. Open the Hub Level view in which the resource is located.
2. Display the list of network types by clicking on the Network button on the right side of the view.
3. Click on the icon of a network type. You can reassign the resource to any of the networks on this list.

   To display a list of isolated networks, you must first click on the icon of the module to which the resource you are reassigning belongs and then click on a network type.
4. Drag the resource and drop it onto a network icon.

   The Information Area displays a confirmation message if the network reassignment is successful. If the operation is not successful, an error message is displayed.

Defining a Logical LAN

Nways Manager-LAN allows you to define a logical LAN to manage a group of users that share the same network across different segments and several hubs connected by trunks. You do this by assigning the same logical name to the network segments to which the user devices are attached.

The same logical name can be assigned to the network segments in two or more 8250, 8260 and 8265 devices. A logical name, however, must be unique for the network segments in the same hub.

You can use logical names with the Search function to quickly locate groups of users and display their IP and MAC addresses. The Search function uses logical names as part of its search criteria. See “Using the Search Function” on page 95 for more information.

By assigning a logical name to a network segment, you can more easily identify the group of users to which it refers. For example, instead of using the name, *Slot 10 Isolated 2*, you could rename the segment *Sales Dept*.

Also, in order to manage the network devices used by the Sales Department on a Token-Ring network across two hubs connected by a physical trunk, you could assign the logical name *Sales* to each network segment. The logical name you define appears instead of the physical name (for example, *Token Ring 3*) in the Network Area of the Hub Level view for each hub.

To assign a logical name to a network segment attached to a hub, follow these steps:

1. Open the Hub Level view of the hub to which the network segment is attached.
2. Click **Network** on the right side of the view to display the types of networks.
3. Click on the icon of a network type to display the segments attached to the hub.
4. Click on the icon of a network segment and select **Logical Name** from the context menu.
5. In the Logical Name panel, type in the name of a logical LAN (up to 30 alphanumeric characters without blanks) and a short description of what it means. Click **OK** to confirm.

   Note: The logical name must be unique for all network segments attached to the same hub. You can, however, use the same logical name for segments in other hubs.

   The logical name appears next to the network segment in the Network Area of the Hub Level view.

To delete a network name, take the following steps:

1. Open the Hub Level view in which the network name is displayed.
2. Select **Clear Logical Name** from the context menu of the network icon.

The network name is removed from the Network Area.

Monitoring Hub Resources

Securing Access to a Network Resource

You can use critical resource settings to secure read-write access to network resources; for example, pairs of Ethernet ports (backup and primary) in a redundant link. If you configure a resource as *critical*, a message is displayed before its configuration parameters are changed to warn users that the configuration of a critical resource is about to be modified.

Customizing How the Compound Hub Status is Calculated

The color of a hub in the IBM Hubs Topology indicates its operating status:

- Normal operation (green)
- Unmanaged (brown)
- Marginal (yellow)
- Critical (red)
- Unknown (blue)
- IP connectivity without SNMP (default color defined by NetView for AIX)

By default, this status is calculated by an algorithm that takes the status of all modules in the hub and the statuses of the following resources in each module:

- Ports
- Trunks
- Fans
- Temperature
- Power supplies
- Power distribution boards

The status of each of these resources is treated equally in the calculation of the overall hub status. The overall hub status is displayed as follows:

- If all resources are red, the compound hub status is red.
- If all resources are green, the compound hub status is green.
- Otherwise, the compound hub status is yellow.

Nways Manager-LAN, however, allows you to specify the relative importance of your hub resources (for example, a trunk or a power supply). The values you set for individual hub resources determine how the compound hub status is calculated. For example, if you configure only one hub resource as *critical* and if the status of this resource changes to red, the compound hub status shown in the IBM Hubs Topology reflects this change and also becomes red.

After you configure how individual resources are to be monitored, you can use the IBM Hubs Topology to see at a glance the color-coded status of each hub. A hub's color then reflects the logical status customized according to the needs of the network operator.

You can monitor a hub resource by using any of the following values:

- Critical
- Normal
- None

When a resource is defined as *Critical*, any change in its status is given greater weight in the calculation of the compound hub status displayed in the IBM Hubs Topology.

Normal means that the status of each resource that is defined as *Normal* is given equal weight when the hub's status is calculated. This is the default value for resource monitoring.

None means that the resource's status is not taken into account when the hub's status is calculated.

Note: Using SMIT, you can change the default value used in resource monitoring from *Normal* to *None*. For more information, see "Customizing Resource Monitoring" on page 87.

Configuring How Resources Are Monitored

To configure how ports, trunks, fans, temperature, power supplies, and power distribution boards are monitored, follow these steps:

1. Open the Hub Level view in which the resource is located.
2. Display the icons for the Resource Monitor by clicking on the Resource Monitor button on the right side of the view.
3. Drag a resource and drop it onto one of the icons (Critical, Normal, or None).

   To configure all the ports and trunks associated with a module you can use a single drag and drop to drop the module icon onto one of the icons. This technique is especially useful when you need to configure backplane ports that are not visible in a Hub Level view.

   The Information Area displays a confirmation message if the resource monitoring assignment is successful. If the operation is not successful, an error message is displayed.

Notes:

1. To configure resource monitoring, you can also select **Configuration** from the context menu of a hub resource and enter a value in the Monitoring field.
2. A Warning message is displayed when a network administrator changes the configuration parameters for a resource that has been configured for *critical*

resource monitoring. For example, a warning is displayed if you change the network assignment of a *critical* port with a drag and drop, change the port grouping, or use the Set Port All option.

3. By default, the threshold for a *critical state* is set to red. However, you can customize the default setting according to your network needs by using SMIT to change the **Threshold for Critical State** parameter. For more information, see "Changing the Threshold for Critical State" on page 88.

Displaying How Resources Are Monitored

To display the resources that have been configured using the Resource Monitor:

1. Open the Hub Level view.
2. Click on the Resource Monitor button to the right of the view.
3. Click on the icon (Critical, Normal, or None) for a type of resource monitoring.

All ports, trunks, fans, temperature, power supplies, and power distribution boards that have been configured for this type of monitoring are highlighted. Module icons are also highlighted if any port or trunk associated with the module has been configured for this type of monitoring.

To display all resource monitoring assignments for a hub, click on the **Show All** pushbutton.

Displaying Critical Resources that Have Failed

When a resource that is monitored as *Critical* reaches the threshold for the critical state as defined by the **Threshold for Critical State** parameter:

- In the IBM Hubs Topology, the compound status of the hub turns red.
- The following icon is displayed at the bottom of the Hub Level view:

If you click on the icon and select **Show** from its context menu, all resources configured as *Critical* that are in a critical state (as defined by the **Threshold for Critical State** parameter) are highlighted. Network operators can use this method as a fast way for locating an important resource that has failed.

For information on how to modify the **Threshold for Critical State** parameter, see "Customizing Resource Monitoring" on page 87.

Handling Traps for Critical Resources

Critical resources are detected as failing or recovering in the following ways:

- When a polling is performed.
- When the following traps are received from the agent: Slot Down, Environment, Trunk Down, Trunk Up, Port Down, and Port Up.
- When the configuration parameters of a resource are changed using panels on the user interface.

You can customize trap generation so that traps are automatically generated when critical resources fail and recover from failure. This allows you to automate an action to be taken when the traps are received; for example, sending a message to a beeper to indicate that a critical resource has failed.

To enable the automatic generation of traps for critical resources, you must use SMIT as described in “Trap Generation for Critical Resources” on page 89. Then the following traps are reported:

- When a critical resource fails, trap 6.40 (`Critical resources that failed`) is generated with a list of the critical resources that failed since the last polling.
- When a critical resource recovers from failure, trap 6.41 (`Failed critical resources that recovered`) is generated with a list of the critical resources that recovered since the last polling.

For more information, see “Customizing Traps and Events Using NetView for AIX V4 or V5” on page 158.

To see if any 6.40 and 6.41 traps have been generated for your critical resources, follow these steps:

1. Open the Hub Level view.
2. Click on the Resource Monitor button to the right of the view.
3. Click on the Critical icon and select **Fault** from its context menu.

Customizing Resource Monitoring

Using SMIT, you can customize some of the parameters used for resource monitoring. After you modify the current values, the compound status of all hubs is re-calculated to take into account the new values you define. All open Hub Level views are automatically refreshed with the new information and any icon that represents a failed critical resource is re-evaluated according to the new values.

To modify resource monitoring parameters:

- Start from the Root submap or the IBM Hubs Topology.
- From the menu bar, select **Administer -> Campus Manager SMIT -> Configure -> CML Hub Manager capability configuration -> Change the resource monitoring configuration**.

The current values for the following parameters are displayed:

- Default Resource Monitoring Policy (*Normal* or *None*)
- Threshold for Critical State (*Marginal* or *Critical*)
- Trap generated when a critical resource fails or recovers from failure (*Generated* or *Not Generated*)

Changing the Default Resource Monitoring Policy

Each time Nways Manager-LAN discovers a resource, the resource is monitored, by default, according to the current value of the **Default Resource Monitoring Policy** parameter. You can change the default value for resource monitoring from *Normal* to *None* by selecting the menu options described in “Customizing Resource Monitoring” on page 87.

When you change this default value:

- All resources configured by a network operator (as described in “Configuring How Resources Are Monitored” on page 85) with a specific monitoring value are **not** changed.
- All resources that took the SMIT default value (because they were not reconfigured using the Resource Monitor) are changed according to the new value you specify.

Changing the Threshold for Critical State

By default, the threshold that determines when a resource is considered as *failed* is set to *critical* (red) by the current value of the **Threshold for Critical State** parameter. However, you can change this setting to *marginal* (yellow) by selecting the menu options described in “Customizing Resource Monitoring” on page 87.

If you set this parameter to *marginal*, all resources that reach *marginal state* and that are monitored as *Critical* are considered as *failed*. The compound hub status then turns red to show that it contains at least one failed critical resource.

Example: Customizing Hub Monitoring

You may sometimes want to configure your resource monitoring so that Hub Level views display hubs only in normal (green) or critical state (red). No hubs are displayed in an intermediate state (yellow). This type of configuration can be useful for monitoring and troubleshooting hubs with failing resources.

To set up this type of resource monitoring, follow these steps:

1. Start from a Nways Manager-LAN configuration that has not yet been customized using the Resource Monitor. No new data is in the Resource Monitoring database.
2. From the menu bar, select **Administer -> Campus Manager SMIT -> Configure -> CML Hub Manager capability configuration -> Change the resource monitoring configuration**.
3. Change the Default Resource Monitoring Policy parameter to *None*.

   This means that no resource will be taken into account when the compound status for each hub is calculated. Each hub will appear in normal state (green) in the IBM Hubs Topology.
4. Configure only the resources that you consider to be the most important resources as *Critical* by following the steps in “Configuring How Resources Are Monitored” on page 85. As a result, the IBM Hubs Topology will display only green (normal) or red (critical) hubs, according to the compound status of the hub resources.

Trap Generation for Critical Resources

In order to generate the traps 6.40 and 6.41 (as described in “Handling Traps for Critical Resources” on page 86) for critical resources that fail and that recover from failure, use SMIT as follows:

1. Start from the Root submap or the IBM Hubs Topology.
2. From the menu bar, select **Administer -> Campus Manager SMIT -> Configure -> CML Hub Manager capability configuration -> Change the resource monitoring configuration**.
3. Change the Trap Generated parameter to *Generated*.

Displaying Configuration Information

You can display configuration information for the following NetView for AIX objects:

- Devices
- Fans
- Temperature
- Power Distribution Boards (PDBs)
- PS/2
- Networks

Displaying a Hub Configuration Listing

The Show Modules option displays a summary of the hub configuration, including the type of module in each slot and the network assignment. This function is only available for 8260 hubs.

To display the Show Modules panel, select **Hub -> Show -> Show Modules** from a Hub Level view.

In the Modules List section, the following information is retrieved for the modules in a selected hub:

- Slot - The slot number of the module.
- Description - A textual description of the module.
- Version - The version of the software in the module.
- Network - The network that this module is connected to.
- IP Address - The IP Address of this module.
- Enabled Ports/Trunks - The number of ports/trunks currently enabled.

Note: For an HE-EMAC module, the information displayed in the Enabled Ports/Trunks column is not relevant.

To display the Configuration panel for a module in the list, select the module and click on the **Configuration** pushbutton.

Saving a Hub Configuration

To save the information about a module displayed in the Show Modules panel, select **File -> Save** from the menu bar. Load:ehp2. from menu bar. A panel is displayed with the following read-only and read-write fields:

- File List - A read-only list box that displays the file names of all the files previously saved using this function.
- Filename - A read-write field where you can specify the name of a file to either display information from or save information to.

The Save option saves the information displayed for the selected module in two files:

- A *·dat* file that is used to redisplay information about the module in the Show Modules panel.
- A *·prt* file that you can print out and edit.

Loading a Hub Configuration

To display information about a module that is stored in a *·dat* file, select **File -> Load**.

Printing a Hub Configuration

To print out information on a module that is stored in a *·prt* file, select **File -> Print**. Then enter the name of the file to print.

You can open the Configuration panel by selecting a module and clicking MB1 on the **Configuration** pushbutton.

Displaying an Inventory

The Show Inventory option is only available for 8260 hubs. Use this option to display information about the hardware installed in a selected hub.

To display the hardware inventory for a hub:

1. Open the Hub Level view.
2. From the menu bar, select **Hub -> Show Inventory**. The Show Inventory panel is displayed.

In the Inventory List section, the following information is displayed about modules installed in the hub:

Slot	Slot number of the module
Model Number	Model of the module
Serial Number	Serial number of the module (8260 hubs only)
Hardware Version	Version of the module (8260 hubs only)
Software Version	Version of the software in the module (8260 hubs only)

Boot Software Version	Version of the boot software in the module's flash chips (8260 hubs only)
Manufacturing Date	Date that the module was manufactured (8260 hubs only)

Saving a Hub Inventory

To save the hardware information about a hub that is displayed in the Show Inventory panel, select **File -> Save** from the menu bar. A panel is displayed with the following read-only and read-write fields:

- File List - A read-only list box that displays the file names of all the files previously saved using this function.
- Filename - A read-write field where you can specify the name of a file to either display information from or save information to.

The Save option saves the hardware information for a selected hub in two files:

- A *·dat* file that is used to redisplay hardware information in the Show Inventory panel.
- A *·prt* file that you can print out and edit.

Loading a Hub Inventory

To display hardware information about a hub that is stored in a *·dat* file, select **File -> Load**.

Printing a Hub Inventory

To print out hardware information about a hub that is stored in a *·prt* file, select **File -> Print**. Then enter the name of the file to print.

Displaying Device Status

The Device Configuration panel displays information on IP devices.

To display information on a network device, open the Module Level view and select **Configuration** from the context menu of the device.

Note: If you double-click MB1 on a device, you invoke protocol switching.

Displaying PS/2 Status

To check the status of a PS/2 that is integrated in an 8250 6PS hub with load sharing, open the Hub Level view and do one of the following:

- Select **Configuration** from the context menu of the PS/2 icon.
- Double-click MB1 on the icon of the PS/2.

The PS/2 Status panel is displayed.

Displaying Network Information

Listing Ethernet and Token-Ring Networks

To display information about an Ethernet or 8260 Token-Ring network, follow these steps:

1. Open the Hub Level view of the hub to which the network segment is attached.
2. Click **Network** on the right side of the view to display the types of networks.
3. Click MB1 on the **Ethernet** or **TR 8260** icon and select **Information List** from the context menu.

A panel with information on the network segments is displayed.

To configure a network segment in the Information List panel, select the line in the panel and click on the **Configure** pushbutton.

Note: You can only configure Token-Ring networks from the Information List panel. There is no **Configure** pushbutton in the panel for Ethernet networks.

Graphical Network Maps

Use the **Show** option to display information about the resources connected to a network. You can select this option from the context menu of the following objects in a Hub Level view:

- Ports
- Network icons on the right side of the Hub Level View if at least one resource is assigned to the network.

All modules, ports, trunks and banks assigned to the selected network are shown in full color (as for the Hub Level View) and all modules that are not assigned to the network are shown in reduced highlight (dark gray). The name of the selected network is displayed at the top of the view.

For port-switching modules:

- A port icon is displayed in color if the port is assigned to the network.
- For TELCO, if at least one port in a bank is assigned to the selected network, the bank is displayed in color. If no ports are assigned to the selected network, the bank is shown in reduced highlight.

  RS-232 ports are not shown as being part of the network.

Displaying Ring Station Information

You select the **Ring Station Information** option from the 8250 Token-Ring icon in the Network area on the right of all Hub Level views if at least one resource is assigned on the ring. A panel displays information about the selected 8250 ring.

Chapter 10. Locating a Network Resource

This chapter describes different ways in which you can locate a network resource:

- You can use the Search function to locate the network device associated with a specific user in order to diagnose and solve network communication problems.
- You can use the Locate function to find a specific network device that is managed by an Nways application, such as Nways Manager-LAN, Nways Manager-ATM, or a Product Specific Module (PSM). The device is displayed in the IP Internet graphical view.

Using the Locate Function

The Locate function allows you to find a specific network device by displaying the device in the IP Internet submap. From the IP Internet submap, you can then use the Nways Protocols function (as described in the online book **User Interface**) to switch to different graphical network views according to the protocols running in the device.

The Locate function is a fast way to find a device discovered by one of the Nways Manager applications that you have installed.

The Nways Locate function is similiar to the NetView for AIX Locate function and allows you to perform additional tasks:

- Search for groups of devices using the wildcard (*) character.
- Display the status of devices managed by Nways applications in a single window.
- Display information about a selected device, such as a description of the device type.
- Sort the devices listed in the Locate results according to their status, IP address, name, and location.

To use the Locate function, follow these steps:

1. Start from the Root submap, the IBM Hubs Topology, or an ATM Campus or Device submap and select **NwaysCampus -> Locate** from the menu bar. .
2. In the Nways Device Inventory window, you must first list the device you want to locate in the Results box. To do so, select **IP Address** or **Host Name** for the type of list criteria you want to use. (Host name is the logical name associated with the IP address.)

   Then enter the text string to be used in uppercase or lowercase letters, including wildcard characters (*). The text field is not case sensitive. You can enter the search text in the following ways:

   - Type it in the field.
   - Cut and paste the string using the mouse.
   - Use a drag and drop. For example, you can drag the box label from a Hub Configuration panel and drop it in the text field.
3. Click on **Go**.

All devices that meet the search criteria are displayed in the Results box. You can sort the devices in the list by clicking on one of the column headings (Status, IP Address, Name, or Location).

4. Select the device you want to locate and click on **Locate**.

   The IP Internet submap is displayed. The device is highlighted in the IP submap and in all other submaps that are already open.

   To switch to another graphical view of the device, select **Nways Protocols** from the device's context menu or **View -> Nways -> Nways Protocols** from the menu bar.

Search Scenarios

This section describes a scenario in which the Search function is used in an environment consisting of an IBM 8260 Nways Multiprotocol hub that supports two token-ring LAN segments. Both segments are connected by token-ring to token-ring bridges to another segment where the company's servers and printer servers are located.

The system administrator has already used Nways Manager-LAN to assign each user to a station. Network polling gathers information on the hub port used by each station to communicate over the network. This information is then stored in the Search database.

This scenario shows how to look up a user to find the station he is currently using and where the station is located.

Problem Reported

Ted Jones is developing a presentation for an important management meeting tomorrow. He has called the Help Desk in a panic because he keeps losing his connection to the LAN. The Help Desk responder says he will open a severity one problem report and have someone address it by noon today.

Problem Analysis

1. Mary Shaw is the help desk responder who opens the trouble report on Ted's problem. Mary recognizes her first challenge is to determine the network location of Ted's workstation and its connection path to the LAN. Mary knows the network servers are isolated on a separate token-ring segment and that several user LANs are bridged to this segment.
2. Mary uses the Search function in Nways Manager-LAN to find and identify Ted's MAC address and the location of his station:
   - For LAN stations, the location is displayed in the format: *hub_label slot_number port_number*
   - For ATM stations, the location is displayed in the format: *ATM_device_label interface_index*
3. In the search results, Mary selects the line that identifies Ted's station and clicks on the **Show** pushbutton to display the graphical view in which his station appears:

- For LAN stations, a Hub Level view is displayed and the port to which the station is connected is highlighted.
- For ATM stations, an ATM view is displayed and the ATM interface in the ATM node to which the station is connected is highlighted.

4. From the Hub Level or ATM view, Mary clicks on the highlighted port or interface to display a context menu.

   The menu contains options that allow you to carry out various management operations to resolve the problem. For example, to check the current port configuration, you select **Configuration**; to gather statistical information about the port, you select **Statistics**.

Using the Search Function

The Search function allows you to locate a user or workstation connected to a network using a variety of search criteria. You can then use the search results to diagnose and solve problems in network communication.

For example, when there are network problems associated with TCP/IP devices, you can use the Search function to display the IP addresses of the devices, the corresponding MAC addresses, and the ports on the hub to which the devices are attached (or to which the devices were attached, if the devices were moved to other ports). From the Search panel, you can open the Hub Level view and troubleshoot the problem using the Configuration and Statistics functions.

To use the Search function, follow these steps:

1. Do one of the following:
   - To search without using a specific search criterion, start from the Root submap or the IBM Hubs Topology and select **NwaysCampus -> Search** from the menu bar.
   - To search for the users or workstations associated with a specific hub, start from the IBM Hubs Topology and select the hub. Then select **HubManager -> Search** from the menu bar.
   - To search for the users or workstations associated with the same logical LAN (LLAN) across different network segments and different hubs, start from a Hub Level view and click on **Network**. Then click on a network type to display the icon for the segment that has the logical name you want to use in the search. Click on the icon and select **Search by Logical Name** from the context menu.

     Note: Before you perform a search using a logical name, the logical name must already be defined as described in “Defining a Logical LAN” on page 83.

   The Search panel is displayed.

2. Select the type of search criteria by entering values in the Search For and By fields.

   To locate a user, select **User** and one of the following types of user information:
   - Name
   - First name

- Address
- Location (office number, building, and so on)
- Miscellaneous parameters that you enter as a text string

To locate a station, select **Station/Device** and one of the following of station parameters:

- Address - to search for LAN stations, enter a MAC address in the text field; to search for ATM stations, enter the 6-byte End System Identifier (ESI) of an ATM address; to search for LEC stations, enter the 6-byte End System Identifier (ESI) and the 1-byte Selector of an ATM address.
- Address type - to search for LAN stations, enter `MAC`; to search for ATM stations, enter `ESI`; to search for LEC stations, enter `LEC`; to search for ATM stations whose address is not known, enter `N/A`.
- MAC display inverted - lists all stations that have been configured with the Inverted Display Mode flag set to *Yes*. This flag toggles the display of the station's MAC address from canonical to non-canonical or from non-canonical to canonical format.
- IP address
- ATM address
- Host name (logical name associated with the IP address)
- Location (office number, building, and so on)
- Wiring information (where station is connected to the wiring closet)
- Group (name of workgroup that you define; for example, Development, Accounting, Sales)
- Function (for example, workstation, bridge LEC, LES, router)
- ELAN (for ATM stations, the logical name of an emulated LAN)
- When station was last polled (number of days)
- Miscellaneous parameters that you enter as a text string

To locate a LAN port or an ATM interface, select **Port/Interface** and one of the following parameters:

- Identifier

  For a LAN port, the format is: *hub_label slot_number port_number*.

  – The default value for *hub label* is the IP address of the Master Management Module.
  – The subslot for a daughter card is displayed *slot_number.subslot_number*.
  – A station external to the hub (such as a station attached to an IBM 8228 on a ring managed by the hub) is indicated by `EXT` in the place of *port_number*.

    You can use SMIT to specify whether or not external stations are to be shown.

  For an ATM interface, the format is: *ATM_device_label interface_index*
- Type of box (for example, 8260 hub, 8281 ATM LAN bridge, 8282 ATM workgroup concentrator)
- Physical segment (to which the port or interface is assigned)

- Logical segment (the logical name assigned to the physical segment)
- Delete flag YES - searches for ports and interfaces that have the Delete flag set to *Yes*. This happens when a hub is removed from the IBM Hubs Topology or when a module is removed from a hub.

  Information on the object is kept in the Search database until you manually delete it. This allows the information to be reported in search results. For information on how to delete a database object, see “Managing the Search Database” on page 99.
- Delete flag NO - searches for all ports and interfaces that are connected to the network.
- Freeze connection YES - searches for ports and interfaces that have the Freeze flag set to *Yes*. When this flag is set to *Yes*, the list of stations connected to the port is frozen and is not updated.

  This is useful when, for example, a bridge is connected to a port and reports all connected stations as also being physically connected to the port. To avoid having all connected stations appear in the search results and to have only the MAC address of the bridge:

  a. Select the line on which the port appears in the search results and click on **Port/Interface**.

  b. In the Freeze Connection field, select **Yes**.

  c. In the Connected Stations field, erase the MAC addresses of all stations connected to the bridge and leave only the MAC address of the bridge.

  d. Click on **Apply**.
- Freeze connection NO - searches for all ports and interfaces that have the Freeze flag set to *No*.
- Miscellaneous parameters that you enter as a text string

3. Enter the text string to be used in uppercase or lowercase letters, including wildcard characters (*). The text field is not case sensitive.

   You can enter the search text in the following ways:
   - Type it in the field.
   - Cut and paste the string using the mouse.
   - Use a drag and drop. For example, you can drag the box label from a Hub Configuration panel and drop it in the text field.
4. Click on **Search**. All objects that meet the specified search criteria are displayed in the search results.

One of the following parameters appears to the left of each station address and represents the address type:

- `MAC` for the MAC address of LAN stations
- `ESI` for the ESI part of the ATM address of ATM stations
- `LEC` for the ESI.SELECTOR part of the ATM address of LEC stations
- `N/A` for ATM stations whose address is not known.

To refresh the search results, click on **Refresh**. If the same search results are displayed, this means that the hub has not been polled since the last time you performed a search. Wait until the next hub polling is done and try again.

When performing a search for LAN ports and stations, note that:

- No search results are reported if the network to which a bridge or router is connected is managed by a TRMM module that does not have write access in the Community Table for the management station running 8250, 8260, and 8265 Device Manager. See “Polling Hubs” on page 117 for more information.
- If an Ethernet station is moved from one port to another port, the original port position is kept in the Search database until you manually delete the information as described in “Deleting Interface Entries” on page 101. Both addresses are shown in the Search panel and in the Module Level view.

  To collect Ethernet information, the Search function uses the MIB variable:

  ```
  ·iso.org.dod.internet.private.enterprises.chipcom.mib02
  ·products.hub.enet.enetStatsPortTable.enetStatsPortEntry
  ·EnetStatsPortLastSrcAddr
  ```

  This variable is the source address of ports that was last recorded.
- If a Token-Ring station is moved from one port to another port, the original port position is kept in the Search database until you delete it as described in “Deleting Interface Entries” on page 101.
- In the search results, Token-Ring stations are displayed as external if the TRMM is separated from them by two or more external trunk connections, even when the stations are directly connected to modules in the hub. This incorrect mapping occurs only when two or more trunks are used on two or more modules; for example, if you use two repeater modules (whether in consecutive slots or not) with at least one trunk on each module.

  To avoid this problem, assign modules to networks by starting with the module in slot 1 and assign the other modules in consecutive order (slot 2, 3, 4, and so on). Use the SHOW NETWORK_MAP TOKEN_RING PHYSICAL command to display the order of trunk and backplane connections. Refer to *Token-Ring Management Module: Installation and Operation Guide* (SA33-0213) for more information.

Note: Network administrators can access the Search panel to perform searches and to update the Search database without having to start up the user interface of NetView for AIX. To do so, enter the following command from the command line of the management station: `/usr/CML/bin/iubsearch -standalone`

Using Search Results

The search results display information (reading from left to right) about ports (interfaces), stations (devices), and users.

Notes:

1. Information on token-ring trunks is not displayed in search results.

2. If you perform a search for an 8250, 8260, or 8265 agent according to its MAC address and if the agent has been configured with different IP addresses according to the network to which it is assigned, the search results may display an incorrect IP address.

You can perform the following operations on search results:

- To change the order in which search results are displayed, open the list box for the **Sort By** field and select the type of information to use.
- To display more information about one of the users or stations in the search results, select the line on which the user or station appears. Then click on **Port/Interface**, **Station/Device**, or **User**.

  To modify any of the information about a user or station in the Search database:

  1. Select the line in the search results.
  2. Click on **User** or **Station** to display the currently configured user or station parameters.
  3. Enter a new value in any of the read-write fields.
  4. Click on **Apply**.
- To open the Hub Level view in which a LAN port is displayed or the Exploded Node view in which an ATM interface is displayed, select the port (or interface) and click on **Show**.
- To open the Emulated LAN submap in which an ATM station is displayed, select the station and click on **Show ELAN**.
- To open a Telnet session and log on to a module, select the module and click on **Telnet**.
- To ping a module and open an Emulator window that shows the ping taking place, select the module and click on **Ping**.
- To save the results displayed in the Search panel, select **File -> Save** from the menu bar. To redisplay the search results, open the Search panel and select **File -> Load**.

Printing Search Results

To print the results of a search operation, follow these steps:

1. Open the Search panel.
2. Select **File -> Print Command** from the menu bar.
3. Enter the print command you want to use. Click on **OK** to confirm.
4. Select **File -> Print** from the menu bar.

Managing the Search Database

You can manage the objects in the Search database in the following ways:

- Create and delete user entries.
- Create and delete station entries.
- Delete interface entries.

- Update the database from a formatted file.
- Save the contents of the database to a formatted file.

Creating and Deleting User Entries

To create a new user in the Search database:

1. Open the Search panel.
2. Select **Administer -> Create new user** from the menu bar. The User Information panel is displayed.
3. Enter values in the fields using uppercase or lowercase. The text fields are not case sensitive. Do not leave blank spaces. To get help, click on a field to display information in the Description box.

   When entering a user name, be sure to enter a unique value. If necessary, enter the first initial of the first name to distinguish users. For example, to create entries for two users called *Bill Smith* and *Dick Smith*, you could enter *Smith_B* and *Smith_D*.
4. Click on **Apply**.
5. Click on **Yes** to confirm. This creates a new user in the Search database.

To delete a user from the Search database:

1. Open the Search panel.
2. In the search results, click on the user to want to delete. Click on **Select All** to select all users in the search results.
3. From the menu bar, select **Administer -> Delete selected users from database**.
4. Click on **Yes** to confirm.

Creating and Deleting Station Entries

To create a new station in the Search database:

1. Open the Search panel.
2. Select **Administer -> Create new station** from the menu bar. The Station Information panel is displayed.
3. Enter values in the fields using uppercase or lowercase. The text fields are not case sensitive. Do not leave blank spaces. To get help, click on a field to display information in the Description box.
4. Click on **Apply**.
5. Click on **Yes** to confirm. This creates a new station in the Search database.

To delete a station from the Search database:

1. Open the Search panel.
2. In the search results, click on the station you want to delete. Click on **Select All** to select all stations in the search results.
3. From the menu bar, select **Administer -> Delete selected stations from database**.
4. Click on **Yes** to confirm.

Deleting Interface Entries

To delete an interface from the Search database:

1. Open the Search panel.
2. In the search results, click on the interface you want to delete. Click on **Select All** to select all interfaces in the search results.
3. From the menu bar, select **Administer -> Delete selected interfaces from database**.
4. Click on **Yes** to confirm.

Updating the Search Database from a Formatted File

Sometimes you may want to update the Search database with data stored in a server file (such as `/etc/hosts`), a phone directory, or another database. To do so, you must translate the data into the syntax recognized by the Search database. You can then use the file containing the formatted data to update the Search database.

To prepare the formatted file, enter data about users, stations, and ports (interfaces) using the following rules:

- The maximum record length is 255 characters.
- Use the double-quote character (") only to mark the beginning and end of a parameter.
- Use a semi-colon (**;**) to mark the end of each parameter section (`USER`, `STATION`, and `IDENTIFIER`). This is mandatory.
- Do not enter values for the following `INTERFACE` parameters: `IDENTIFIER`, `TYPE`, and `MACLIST`. These values are automatically discovered when you update the Search database. You can, however, add or modify miscellaneous text information for `MISC`.
- You must enter values for the following parameters: `USER NAME`, `STATION MACADDRESS`, and `INTERFACE IDENTIFIER`. These entries are mandatory.

An example of the grammar to use in a formatted file is shown here:

```
USER
  NAME            "Durand"
  FIRSTNAME       "Pierre"
  TELEPHONE       "(01) 99.99.99.99"
  ADDRESS         "18 rue Rivoli Paris-France"
  LOCATION        "B1 1N23 PARIS"
  MISC            "Development Manager"
  MACLIST         "420202020202 "
  ;

STATION
  MACADDRESS      "420202020202"
  ATMADDRESS      "01020304050607080910111213141516171819202l"
  IPADDRESS       "9.100.108.97"
  HOSTNAME        "server1"
  WIRE            "C1 YZ234"
  LOCATION        "B1 1N23 PARIS"
```

```
  GROUP           "Development"
  FUNCTION        "Server"
  DOMAIN          "LAN3"
  MISC            "AIX Version 4.1.4"
  ;

INTERFACE
  IDENTIFIER      "9.100.107.10         S07   P01"
  TYPE            "8260"
  MACLIST         "002035E10CD1 "
  MISC            "Development hub"
  ;
```

To update the Search database from the formatted file:

1. Open the Search panel.
2. From the menu bar, select **Administer -> Update database from formatted file**.
3. In the Filter field, enter all or part of the pathname of the directory where the file is stored. Click on **Filter**.
4. In the Directories box, click on the directory.
5. In the Files box, click on the file name.
6. Click on **Update database from file**.

Backing Up the Search Database to a File

Sometimes you may want to back up the Search database or edit it by removing old data and making global changes to existing data. To do so, you copy the database to a file. Then if you want to modify any of the data in the database:

1. Edit the file as needed using a standard text editor.
2. Reload the database using the file as described in “Updating the Search Database from a Formatted File” on page 101.

To copy the Search database to a file:

1. From the Search panel, select **Administer -> Save database to formatted file**.
2. In the Filter field, enter all or part of the pathname of the file. Click on **Filter**.
3. In the Directories box, click on the directory.
4. Enter the name of the file in which you want to save the Search database.
5. Click on **Save database to file**.

You can edit the file and use it to update the Search database.

Chapter 11. Managing Network Resources

This chapter describes how to manage your network resources after they have been configured. To perform these tasks, you use panels to enter the necessary information.

Enabling and Disabling Traps for Agents

The Alert Table option is only available for agents and allows you to disable or enable the traps sent by the agent.

To select the Alert Table option, click MB3 on an agent module icon and select **Control -> Alert Table** from the context menu. A panel is displayed.

You can set the following alerts:

snmp-authentication	Standard SNMP authentication failure such as bad community name. Can be set to *enable* or *disable*.
hello	Can be set to *enable* or *disable*.
change	Can be set to *enable* or *disable*.
script	Can be set to *enable* or *disable*.
console-display	Controls the display of alerts at the console terminal. Can be set to *enable* or *disable*.
port-up-down	Can be set to *enable*, *disable* or *filter*. If set to *filter*, you can define the ports for which these traps are to be sent in the Port Configuration panel.

Resetting Mastership

To select the Reset Mastership option, do one of the following:

- From the IBM Hubs Topology, select **HubManager -> Control -> Reset Mastership**.
- From a Hub Level view, select **Hub -> Control -> Reset Mastership**.

This option initiates the election of a Master Management module based on the mastership priority allocated to each Management module. The module with the highest priority (in the range from 1 to 10 where 10 is maximum) is elected master and becomes responsible for box management of the Hub. If two or more management modules have the same priority, mastership election is arbitrary.

Nways Manager-LAN detects that a mastership reelection has occurred and that a new agent is now master in a hub when:

- There is any SNMP communication between **iubd** and the managed hub.
- The agent sends a trap to report that the master agent has changed.

One side effect of this change is that the object representing the hub in the generic topology database that was merged with the object representing the master agent is split and merged with the new master agent.

Accessing Workstations Remotely

Some modules can be accessed remotely from a workstation that supports the Telnet protocol. When you remotely log on to a module, a text interface is used. This interface is similar to the interface of the out-of-band ASCII console connected to the RS-232 or RS-423 serial port on the module.

You can select the Telnet option in the following ways:

- From the IBM Hubs Topology, select a hub and then select **HubManager -> Control -> Telnet**.

  A panel is displayed containing a list of all modules in the hub that support Telnet. To start a Telnet session, select one of the lines in the list and click on the **Telnet** pushbutton.

  Note: The Master Management module is preceded by an asterisk (*).
- From the context menu of a module in a Hub Level view, select **Control -> Telnet**.

If a selected module or device does not support Telnet, the **Telnet** option is displayed in reduced highlight and cannot be selected. Only modules or devices that support Telnet allow you to start a Telnet session.

If no modules support Telnet, this panel will be empty. To use the autodiscovery process to check if any modules have been connected since this panel was displayed, click on the **Refresh** pushbutton.

When you select one of the modules in the list, additional information is displayed in the System Table section.

To start a Telnet session, select a module and click on the **Telnet** pushbutton.

Remotely Accessing Bridges and Routers

To remotely access and manage bridges and routers, you use the Router and Bridge Manager component of Nways Manager-LAN. You start by performing one of the following tasks:

1. Display all bridges and routers connected to a hub and all Bridge and Router modules installed in the hub (that are supported by the currently installed version of Router and Bridge Manager) by selecting:
   - **HubManager -> Control -> RandB Man** from the menu bar in the IBM Hubs Topology or from the context menu of a hub icon.
   - **Hub -> Control -> RandB Man** from the menu bar of a Hub Level view.

2. Start Router and Bridge Manager in a Bridge or Router module in a Hub Level view by selecting **Control -> RandB Man** from the context menu.
3. Start Router and Bridge Manager in the router connected to the hub in a Module Level view by selecting **Control -> RandB Man** from the context menu.

The Router and Bridge Manager Function Panel is then displayed. The panel displays no information if:

- No routers or bridges are connected.
- The network to which a bridge or router is connected is managed by a TRMM for which the management station running Nways Manager-LAN does not have write access in the TRMM's Community table. See "Polling Hubs" on page 117 for details.

To use the autodiscovery process to check if any devices have been connected since this panel was displayed, click on the **Refresh** pushbutton.

When you select one of the modules listed, the additional information is displayed in the System Table section.

To start Router and Bridge Manager, select one of the routers in the list and click on the **RandB Man** pushbutton. To start a Telnet session, click on the **Telnet** pushbutton.

Downloading Microcode

A Download operation (inband download) sends software to hub modules that support TFTP. Microcode is downloaded with parameters that specify the modules that receive microcode and the characteristics of the file to be downloaded.

To download microcode, click MB3 on a module icon in a Hub Level view and select **Control -> Download** from the context menu. The Download panel is displayed.

The following read-write fields can be changed:

- Host Name/IP Address - The address of the file server.
- File Name - The name of the file containing the code.
- File Type - The type of code to be downloaded.
- Target Location - Where the code is to be downloaded to.
- Start download - Indicates that the download is to be performed when you click on the Apply pushbutton.

Note: For 8260 modules, the software download is performed using TFTP first to the DMM, and then from the DMM to the other modules in the hub. All 8260 modules support the download operation; only certain 8250 modules, however, support it.

When the download operation finishes, the results of the operation and the date and time of the last successful download are displayed.

Results of Download When There Are Two or More DMM Modules

When there are two or more DMM modules in a hub and you download software to the **master** DMM module, the results displayed in the Download panel do not reflect the results of the download operation. This is because the master DMM is reset after the microcode is downloaded and during the reset, the slave DMM becomes master. The results that are displayed are the results of the last microcode download performed to the **slave** DMM (that is now master).

- Select **Hub —> Control -> Reset Mastership** from the menu bar of the Hub Level view. This sets the master DMM module to **slave**.
- Download microcode to the slave DMM module (that was master).
- Reset mastership again by choosing **Hub -> Control -> Reset Mastership** so that the slave DMM module (that was master) becomes master.

Configuring AIX for TFTP Inband Download

If the Download function is not available, you can configure the AIX for TFTP inband download by following these steps:

1. Check the **/etc/inetd.conf** file in AIX and make sure that the TFTP line is not commented out.
2. Start the TFTP subserver using the following commands:
   a. smit
   b. Processes & Subsystems
   c. Subservers
   d. Start a Subserver

      Select TFTP from the list. The command is: `startsrc -t'tftp'`. You must be a root user to able to do this.

Using BootP

BootP is a protocol that allows a client to discover its IP address and the location of a file to execute on startup. The BootP protocol is only used by Token-Ring Management modules (TRMM V3.0).

To configure BootP parameters, click MB3 on a Token-Ring Management module icon in a Hub Level view and select **BootP** from the context menu. The BootP Panel is displayed.

From the BootP panel, you can change the following settings:

- BootP Server IP Address or Hostname - Shows the IP address or host name of the BootP server. If you enter the BootP Server name or IP address, the Token-Ring Management module sends its initial BootP request to this server rather than to a broadcast address. If you enter 0.0.0.0, the TRMM will broadcast the BootP request.
- Perform BootP request on each Power Up - Specifies whether or not the module will send a BootP request each time that it powers up.

- Perform BootP Request On Apply - Specifies that the BootP request is to be sent to the server when you click on the **Apply** pushbutton. After the request is sent, this field is reset to *No*.

The result of the last BootP operation is displayed in the Last BootP Result field.

Modifying FDDI Station Management Information

The FDDI_SMT function allows you to view and modify FDDI management station information and to customize your FDDI network. The FDDI Station Management panel is only accessible from the context menu of an FDDI Management module.

Modifying FDDI MAC Timer Information

The FDDI_MAC_Timers function allows you to view or modify FDDI MAC-related timer information. The FDDI MAC Timer panel is only accessible from the context menu of an FDDI Management module.

Taking a Snapshot of the Hub Configuration

The Snapshot option saves a backup of the current hub configuration, including all customizable MIB variables for a given Hub Level view.

To save the configuration parameters for a hub, open the Hub Level view and select **Hub -> Control -> Snapshot**. The Snapshot panel is displayed.

The following information from the snapshot is saved in the file and directory specified in the Snapshot panel and can be printed:

- Number of modules
- Module Index
- Module Network
- Module Status
- Module Contents for:
  - Ports
  - Trunks
  - Banks
  - TTY
- With the following information, where applicable, for each:
  - Index
  - Displayed
  - Status
  - Network
  - Backup

– Connector type

Configuring Token-Ring and 8250 Ethernet Security

You can build secure Ethernet and Token-Ring LANs by giving access only to authorized LAN stations. Nways Manager-LAN provides intrusion protection by controlling access to the LAN through a MAC access list that is maintained on a port basis.

Intrusion protection is available for the following modules:

- IBM 8250 Token-Ring Media module when the Master Management module is a TRMM 3.0 or higher.
- IBM 8260 Token-Ring Media module when the Distributed Management module is a DMM 3.0 or higher.
- IBM 8250 Ethernet Media module when the Master Management module is an EMM 4.0A or higher.
- IBM 8250 Ethernet 10BASE-T Security module when the Master Management module is a TRMM 3.0 or an EMM 4.0.

The Intrusion function allows you to define a list of authorized MAC Addresses for a given port. You configure a port so that when a security violation occurs, the port is disabled and a trap is sent.

Notes:

1. A trap is sent if at least one agent (master or slave) is managing the segment.
2. The port is disabled only if the master is assigned to this segment or if it is an Ethernet 10BASE-T Security Module.

To configure Intrusion protection for a port, open a Hub Level or Module Level view and click MB3 on the port icon. Then select **Intrusion** from the context menu. The Port Intrusion panel is displayed.

Configuring 8260 Ethernet Security

Nways Manager-LAN allows you to configure security for 8260 Ethernet modules which are assigned to Ethernet and isolated networks. This is necessary because in a standard Ethernet network, packets transmitted from one node to another node are also transmitted to all nodes in the network. Each node examines the packet to see if its destination address matches the physical MAC address of the node. If the addresses do not match, the packet is discarded.

Without security protection, the following situations can occur:

- Intruders can transmit information to any port in the network.
- Unwanted users can eavesdrop on data transmitted between network nodes.

By configuring Ethernet security, you can prevent eavesdropping and intrusion in the network.

You can configure Ethernet security so that:

- Node B (eavesdropper) cannot examine the contents of each packet transmitted between nodes A, C, and D.
- Node C (intruder) cannot transmit packets to nodes A, B, and D.

In order to secure an Ethernet or isolated network, you must use one Ethernet Security Card (ESC) for each network segment in an 8260 hub. The ESC card is a daughter card that you install on an 8260 Ethernet module or Distributed Management Module (DMM). The module in which you install the ESC card is called the *securing module* for the network.

Each ESC card manages the ports in a hub that are assigned to the same Ethernet or isolated network segment. This means that if you have four Ethernet segments in an 8260 hub and want to secure each segment, you must install four ESC cards (one for each network segment).

To secure an Ethernet or isolated network, follow these steps:

1. For each Ethernet port that belongs to the network, configure the allowable MAC addresses of network nodes to which packets can be sent and received. This procedure is described in “Configuring Security for an Ethernet Port” on page 113.

   When configuring MAC addresses, you may want to define groups of MAC addresses that correspond to groups of users. This procedure is described in “Defining Security Groups” on page 113.

   Note: The 8260 Ethernet security function uses an address table that contains the MAC addresses and associated ports of nodes in a secure network. Although there is no limit to the number of allowable MAC addresses that you can configure for each port, the maximum number of *MAC address — port* entries that can be made in the table is 1000. Once this limit is reached, older entries are automatically deleted.

   To see how many entries have already been made in the security address table, follow these steps:

   a. Telnet to the Distributed Management Module where the network’s ESC card is installed.
   b. Enter the command: `SHOW SECURITY_ADVANCED ADDRESS_TABLE ALL`

   For more information on using the security address table, refer to the *IBM Ethernet Security Card User’s Guide* (SA33-0262).
2. If necessary, modify the security settings for each Ethernet port. To do so, you may use the default settings at the port level (as described in “Using Default Settings for Port Security” on page 110) and at the network level (as described in “Using Default Settings for Port Security” on page 110).

Using Default Settings for Port Security

When configuring Ethernet security, be sure to check the default settings that exist at port level. These defaults refer to Ethernet ports on all 8260 hubs in the IBM Hubs Topology. It may be easier to load the default settings and modify the ones you want to change rather than to manually enter each value.

To display the default security settings for 8260 Ethernet ports, follow these steps:

1. Open a Hub Level view.
2. From the menu bar, select **Hub -> Control -> 8260 Ethernet Security -> Port Security Defaults**. The Configuration panel for default port security is displayed.

The default settings (*enable* or *disable*) for the following parameters are contained on the panel:

Jamming

Enables and disables eavesdropping and intruder protection at port level in a secure network.

Eavesdropping protection means that packet transmission is jammed on all ports, except when a packet's destination address matches one of a port's allowable MAC addresses. To enable eavesdropping in a secure network, you must also enable the **Eavesdrop Protection** parameter at the network level.

Intruder protection means that a packet's source address is checked against the list of allowable MAC addresses for the port. If the source address does not match an allowable MAC address, the packet is treated as an intruder and is jammed. To enable intruder protection in a secure network, you must also enable the **Intruder Jamming** parameter at the network level.

Intruder check

Checks a packet's source address with the list of valid MAC addresses configured for the port. If no match is found, the packet is treated as an intruder. To enable intruder checking in a secure network, you must also enable the **Source Address Checking** parameter at the network level.

Fail safe

Allows you to jam all packets in a secure network when there is a failure in the security function.

All modules in the network are set to receive a security message with each packet. The message contains information about whether or not to jam the packet. If there is a failure in the security function and if the Fail Safe and Jamming parameters are enabled, all outgoing packets are jammed at port level.

Autolearn
: Automatically records the MAC address and associated port number of each node in the network in the security address table. To enable autolearning in a secure network, you must also enable the **Autolearning** parameter at the network level.

To change any of the default settings for port security, follow these steps:

1. Click on the list box of the parameter you want to change and select *enable* or *disable*.
2. Click on **OK**. This configures your selections as the new default values for Ethernet ports in 8260 hubs in the IBM Hubs Topology.

Using Default Settings for Network Security

When configuring Ethernet security at the network level, remember that:

- Network parameters are used to turn on and off port security parameters. For example, in order to enable autolearning for all network ports, you must enable the Autolearn parameter at port level and then enable the Autolearn parameter at network level.
- The default security parameters at network level refer to all Ethernet and isolated networks on 8260 hubs in the IBM Hubs Topology.
- The Mode parameter is used as a master parameter to turn on and off all network and port security functions.

To display the default security settings for Ethernet and isolated networks, follow these steps:

1. Open the Hub Level view for a hub that contains an Ethernet or isolated network segment.
2. From the menu bar, select **Hub -> Control -> 8260 Ethernet Security -> Network Security Defaults**. The Configuration panel for default network security is displayed.

The default settings (*enable* or *disable*) for the following parameters are contained on the panel:

Security Mode
: Enables and disables the security function in a secure network.

  When enabled, be sure to set all other network security parameters in the panel before you save your selections by clicking on **OK**.

Autolearning
: Enables or disables autolearning of node MAC addresses and Ethernet port numbers in a secure network.

  If you enable autolearning at the network level, you must also enable the **Autolearn** parameter at port level.

Eavesdrop Protection
: Enables or disables eavesdropping protection on ports that have the **Jamming**

parameter enabled. When network eavesdropping is enabled, a packet is transmitted only if its destination address matches one of the allowable MAC address configured for the port.

Intruder Jamming
Enables or disables intruder protection on ports that have the **Jamming** parameter enabled. When network jamming is enabled, intruder packets are jammed on all network ports. This prevents network nodes from receiving intruder packets.

In order for intruder packets to be detected, you must also enable the **Source Address Checking** or **Source Port Checking** parameter at network level.

Source Address Checking
Checks the source address of each packet transmitted on a secure network with the list of valid MAC addresses configured for each port. If the source address is not an allowable MAC address, the packet is treated as an intruder.

If you enable source address checking, source addresses of transmitted packets are checked only for ports that have the **Intruder Check** parameter enabled.

Source Port Checking
Checks the port number from which each packet on a secure network is transmitted with the list of valid port numbers configured for each port. If the source port number of a packet does not match an allowable port number, the packet is treated as an intruder.

If you enable intruder port checking, the source port number of transmitted packets is checked only for ports that have the **Intruder Check** parameter enabled.

Note: Intruder port checking is an optional parameter. If you enable both intruder address and intruder port checking, both the MAC address and port number of a transmitted packet are checked in the list of allowable MAC addresses. If either one (or both) does not match an entry in the table, the packet is treated as an intruder.

Intruder Reporting
Tracks intrusion attempts on a secure network. All intrusions are reported by modules and stored by the Distributed Management Module in the intruder table. In order for intruders to be reported, you must enable either the **Source Address Checking** or **Source Port Checking** parameter at the network level.

Note: Only 100 intrusion entries can be stored in the intruder table. Once this limit is reached, older entries are erased.

Intruder Port Disabling
Automatically disables ports that transmit intruder packets and have jamming enabled.

In order for intruder packets to be detected, you must enable the **Source Address Checking** parameter at the network level.

To change any of the default settings for network security, follow these steps:

1. Click on the list box and select *enable* or *disable* for the parameters you want to change.
2. Click on **OK**. This configures your selections as the new default values for the network in all 8260 hubs in the IBM Hubs Topology.

Defining Security Groups

To configure Ethernet security, you must specify the valid MAC addresses of the network stations that are allowed to transmit data through each port. A quick way to do this is by defining groups of allowable MAC addresses. You can then enter the number of a security group instead of manually entering one MAC address at a time.

When defining a security group, remember the following guidelines:

- You can define up to 254 security groups for the secure networks in an 8260 hub.
- You can assign a security group to more than one port on the same network. This is useful in order to create a redundant link to a node.
- You cannot assign a MAC address to more than one security group. When you assign a MAC address to a second group, it is erased from the first group.

To define a security group, follow these steps:

1. Open the Hub Level view for the hub that contains the network you want to secure.
2. From the menu bar, select **Hub -> Control -> 8260 Ethernet Security -> Security Groups**. The Security Group panel is displayed.
3. In the Security Group field, type a number to identify the group. Valid values: 1 - 254.
4. In the New MAC Address field, type the MAC address of each network node in the group. You can also drag and drop a MAC address in the field and modify it as necessary. Click on **Add** to save the MAC address under the group name.

To display the list of MAC addresses assigned to a security group, enter the group's number in the Security Group field and click on **List**. You can modify the list of MAC addresses in the following ways:

- To delete a MAC address from the group, click on the address to select it and then click on **Delete**.
- To delete all MAC addresses from the group, click on **Delete All**.
- To add a MAC address to a group, type in the address in the New MAC Address field and click on **Add**.

Configuring Security for an Ethernet Port

Before configuring security for ports in an Ethernet or isolated network, be sure to:

1. Assign the ESC card to the network you want to secure by following the procedure in "Configuring Daughter Cards" on page 75.

2. Assign the port to the network you want to secure by following the procedures in "Configuring Ports" on page 75 and "Assigning a Resource to a Network" on page 82.
3. Check the default settings for port security as described in "Using Default Settings for Port Security" on page 110. You can load the default settings and then modify individual parameters to customize port security.
4. Create a security group if you need to configure the same group of MAC addresses for more than one port. See "Defining Security Groups" on page 113 for more information.

To configure security for Ethernet ports, you must specify *allowable MAC addresses*. These are used to check the source and destination addresses in packets to determine the nodes from which a port can receive packets and to which it can send packets.

For example, if you want to prevent a port from receiving intruder packets, you must configure the MAC addresses for the *source* nodes from which the port can receive packets. Similarly, if you want to prevent unwanted eavesdropping, you must configure the MAC addresses for the *destination* nodes to which the port can send packets.

To set the security for an Ethernet port, follow these steps:

1. From the Hub Level view, click MB1 on the port icon and select **Control -> 8260 Ethernet Security** from the context menu. The Allowable MAC Address panel is displayed.
2. In the New MAC Address field, enter a MAC address and click on **Add**. The address is added to the list in the Allowed MAC address box.

   To delete an address from the list, click MB1 to select it and click on **Delete**. To delete all addresses from the list, click on **Delete All**.

   To add the MAC addresses contained in a security group, enter the group's number in the First Group or Second Group field.

   To display the contents of a security group, click on **MAC Addresses**. The Security Group panel is displayed. To add or delete the MAC addresses assigned to the group, follow the procedure in "Defining Security Groups" on page 113.
3. If you want to change the current security settings for the port, click on **Port Security Parameters** next to the Port field..

   The Port Security Parameters panel is displayed with the current security settings. If necessary, modify these parameters according to the procedure in "Using Default Settings for Port Security" on page 110.

   To reset port security to the default parameters, select **Defaults -> Load Defaults** from the menu bar.
4. Click on **OK**. This configures the port with the allowable MAC addresses and security parameters at port and network levels.

   To configure security for other Ethernet ports in the hub, click on **<< Port >>**.

Because port security is not activated unless the corresponding network security parameters are enabled, you may need to set or modify some of these parameters. To do so, follow the procedure in “Configuring Security for Ethernet and Isolated Networks”.

Configuring Security for Ethernet and Isolated Networks

To set the security settings for an Ethernet or isolated network, follow these steps:

1. Open the Hub Level view in which ports assigned to the network are displayed.
2. Display the list of network types by clicking on the Network button on the right side of the view.
3. To display a list of Ethernet networks, click on the Ethernet icon.

   To display a list of isolated networks, first click on the icon of the module that contains ports connected to network devices. Then click on the icon for Isolated networks.
4. From the list of network segments, click MB1 on the icon of a network and select **Control -> 8260 Ethernet Security** from the context menu. The Configuration panel for network security is displayed.

   If no ESC card has been assigned to the network, an error message is displayed: `No securing module has been assigned to current network`. To configure a ESC card, follow the procedure in “Configuring Daughter Cards” on page 75.
5. Select *enable* or *disable* for the security parameters (Autolearning, Eavesdrop Protection, and so on). For information on each parameter, see “Using Default Settings for Network Security” on page 111.

   To reset network security to the default parameters, select **Defaults -> Load Defaults** from the menu bar.
6. Click on **OK** to save the network security settings.

   To save the security settings in the panel as the new default values for network security, select **Defaults -> Save Defaults** from the menu bar.

Setting Fault Tolerant Power

The Power Management panel is only available for IBM 8260 hubs. It lets you specify whether or not the Hub Power Management Mode is fault tolerant. When this mode is enabled, one power supply is held in reserve and will be used during failure of one of the other power supplies in the hub.

To display the Power Management panel from a Hub Level View, select **Hub -> Control -> Power Management**.

Modules that have a higher power class receive power first. 10 is the highest power class; 1 is the lowest.

Note: The modules which are powered off are identified by a Power Off icon overlayed on top of an empty module icon that has no icon above it. This indicates that there is a module plugged into the slot but that there is insufficient power in the hub.

You must calculate the power requirements of all the modules in the selected hub to ensure that sufficient power supplies are available. An extra power supply, above that needed for normal operation, is required if you want to set fault tolerant mode on.

Important: The Power Admin State cannot be set on the Master Management module.

A question mark (?) in the operating status column in the Module Power Management list box means that a refresh is needed to know the value set by the agent. Click on the **Refresh** pushbutton to display the new value set by the agent in the Operating Status column.

Managing All Ports on a Module

The Set Port All function enables you to use one panel to manage all ports of a selected module by setting the following parameters on a per-port basis:

- Port Mode - You can set the Admin State of the port to enabled or disabled.
- Alert Mode - You can set the alert filter of each port if the master module supports this functionality.
- Network Assign - If the module is per-port switchable (PPS), you can assign each port to a network.

To manage all ports from the context menu of a module, select **Control -> Set Port All**. The Set Port All panel is displayed.

When using the Set Port All panel, you must perform the actions in the following order:

1. Select the operation that you want to perform by selecting one of the choices from the list box of the Operation field.

   The current values of all ports on the module for the selected operation are displayed in the Port List area.
2. Open the list box of the Possible Values field and select one of the available values for the selected operation.
3. Prepare the action to be performed on each port as follows:
   - Select the port that you want to configure by clicking on one of the lines in the Port List area and then click on the **Set** pushbutton. This displays valid values *Value to Set* column.

     To choose more than one port, click on the **Set** pushbutton and then select the line for each individual port.
   - To remove the value displayed in the *Value to Set* column, click on a lines and then click on the **Unset** pushbutton. Note that you can also select more than one line before you click on **Unset**.

- To configure all the ports on a module at the same time, click on the **Set All** or **Unset All** pushbuttons.

  Note: You cannot select a parameter from the *Value to Set* column if it is the currently set value. For example, you cannot select *enable* for a port that is currently enabled.

4. Click on the **Apply** pushbutton to send the values displayed in the Port List area to the agent. The results of the operation for each port are displayed in the *Current value* field.

Notes:

1. For the Network Assign operation, some values may not be authorized depending on the current configuration of the network. This produces poor results when you apply the changes.
2. An asterisk precedes protected ports.

Resetting a Device

To reset a hub and the modules in the hub, do one of the following:

- From the IBM Hubs Topology, select **HubManager -> Control -> Reset**.
- From a Hub Level view, select **Hub -> Control -> Reset**.

A dialog box is displayed for you to confirm that you want to reset the selected device. Press **Yes** to continue and reset the device; press **No** to cancel the operation.

Resetting a hub or a module is the same as rebooting the device. Make sure that you are aware of what is attached to the selected hub or module. Resetting a Controller or a Master Management module effectively resets the entire hub.

Hubs and modules displayed in red cannot be reset using the Reset function because there is no IP connectivity to the hub or module.

Polling Hubs

Nways Manager-LAN monitors hubs by means of polling and trap handling. Polling is performed when:

- A timer expires.
- You request a poll.
- A Hub Level view is opened.
- Certain traps are received.
- The polling policy is changed from On Request to Regular.

The polling of each hub consists of the following steps:

1. The Master Management module is polled for configuration parameters of the modules in the hub.

2. The Master Management module is polled for information on the hub environment (status of power supplies, fans, and so on).
3. Each Management module is polled for station information.

   The Search function uses station information to build a Module Level view. To receive accurate station information for a specific hub segment:

   - An IBM 8250 or IBM 8260 agent must manage the segment (that is, have an interface assigned to it).
   - For Token-Ring segments, Nways Manager-LAN must have read-write community name access to this management module.
   - The hub has been successfully polled at least once.

   Note: Bridges may hide the MAC Addresses of attached stations.

The information returned by the poll is held in memory and reflects the information gathered for the hub during the previous poll.

There are two types of polling: normal polling and forced polling.

Normal Polling

Normal polling (the default value that is shown in the SMIT installation panel) uses polling steps 1 and 2 with step 3 executed on every 10th cycle. Normal polling occurs when:

- A timer expires
- A particular trap is received
- The polling policy is changed from On Request to Regular.

Forced Polling

Forced polling uses polling steps 1, 2, and 3. Forced polling occurs when:

- A poll is requested
- A Hub Level view is opened.

Polling Single Hubs

Nways Manager-LAN monitors the status of discovered hubs by polling the hubs in either of the following ways:

- Regular polling that is done periodically
- Polling on request (see “Requesting a Hub Poll” on page 123).

The **Polling Policy** option lets you set the interval for periodically polling single or multiple hubs.

You can display the Single Hub Polling Interval Panel in any of the following ways:

- From the IBM Hubs Topology, select **HubManager -> Monitor: Polling Policy -> Single Hub**.
- From a Hub Level view by selecting **Hub -> Monitor -> Polling Policy**.

The information on polling policy and polling interval in the panel is also displayed at the bottom of the Hub Level view for each hub.

If the Polling Policy field is set to *On Request*, you cannot change the polling interval.

If the Polling Policy field is set to *Regular*, you can specify the interval between polls using the scrollable hours and minutes fields. Note that it is useful to set a higher polling rate for sensitive devices and reduce the frequency of polls for devices that have less effect on the network if they go off-line.

Note: Changing the Polling Policy from **On Request** to **Regular** triggers normal polling (see "Polling Hubs" on page 117 for details.)

The minimum polling interval is one minute; the maximum polling interval is 23 hours and 59 minutes. The default polling parameters are:

Polling Policy	On Request
Interval	Five minutes

These default values can be changed through SMIT.

Any values changed in the Polling Policy panel are saved when you click on **Apply** or **OK**.

Note: SNMP recovery performs a hub poll independently of the polling policy and hub status (`Managed` or `Unmanaged`) configured in NetView for AIX.

To cancel the hub poll started by the SNMP recovery, select the hub in the IBM Hubs Topology or the master agent in the IP Internet submap and select **Options -> Unmanage Objects** from the menu bar.

Polling Multiple Hubs

To set the same polling policy for two or more hubs, follow these steps:

1. In the IBM Hubs Topology, select the hubs by holding down MB1 and clicking on the icon for each hub.
2. From the menu bar, select **HubManager -> Monitor: Polling Policy -> Multiple Hubs**. The Multiple Hubs Polling Policy panel is displayed.

   Note: When all the hubs in the group have the same values, this panel displays the common values. Otherwise, it shows the default values which can be set by selecting **SMIT -> HubManager -> Configure -> Change the Default Polling Policy**.

Nways Manager-LAN uses two types of polling policy:

- Regular polling that is done periodically
- Polling on request (see “Requesting a Hub Poll” on page 123).

If the Polling Policy field is set to **On Request**, you cannot change the polling interval. If the Polling Policy field is set to **Regular**, you can specify the interval between polls.

The minimum polling interval is one minute; the maximum polling interval is 23 hours and 59 minutes. The default polling parameters are:

Polling Policy	On Request
Interval	Five minutes

Any values changed in the Polling Policy panel are saved when you click on **Apply** or **OK** and apply to all hubs selected in the IBM Hubs Topology.

Note: SNMP recovery performs a hub poll independently of the polling policy and hub status (`Managed` or `Unmanaged`) configured in NetView for AIX.

To cancel the hub poll started by the SNMP recovery, select the hub in the IBM Hubs Topology or the master agent in the IP Internet submap and select **Options -> Unmanage Objects** from the menu bar.

Setting Threshold Values

The Threshold function is available with master or slave TRMM agents V2.1 Advanced or higher. It lets you monitor activity (statistics) and to specify threshold values for selected resources.

TRMM agents provide thresholding capability for the network, station, port, and pre-defined MIB object identifier (provided that it has a type of counter or integer). Once you have set the threshold parameters, the TRMM monitors the associated counters at selected (user-defined) intervals. When the counter value exceeds the threshold value you have specified, an SNMP trap is sent to Nways Manager-LAN.

The TRMM sends additional traps each time the value drops below and then again exceeds the threshold value. No additional traps are sent if the value is consistently above the threshold.

If you specify a threshold value of 100 for an interval of 60 seconds, the TRMM will send a trap if the value of a specified counter reaches 101 during a 60-second period. Even if the counter value temporarily exceeds 100 during the next 60-second interval, the TRMM will not send a second trap. This is because the TRMM does not register that the threshold has been exceeded a second time until the counter value remains equal to or falls below the threshold for at least one 60-second interval.

To configure thresholds for a network, port, or station, you need the following information:

- Index allows unique identification for each threshold configuration. There is a limit to the number of thresholds that you can set depending on the agent. For example, you can configure up to 10 threshold configurations for a TRMM agent.
- Mode (enabled/disabled)
- Category (network, port, station, or other) for which you want to establish a threshold
- Type (broadcast frames, frames, bytes, or others).
- Network assignment for a particular threshold (optional only when the category is port)
- Threshold limit value
- Threshold sampling interval
- Threshold current value
- Threshold status.

A Threshold Control panel is displayed showing the status of all the current thresholds.

You can add new thresholds, enable or disable a threshold after selecting it in the list box, and modify or delete an existing threshold. You can also enable, disable, or clear all listed thresholds. When you select to add or modify a threshold, a panel is displayed corresponding to the threshold index selected and a complete description of the threshold's parameters is provided for information or modification.

Note: Modifications made in the Statistics Attributes Panel will be shown in the Statistics Control Panel when you click on the **Refresh** pushbutton.

Depending on the threshold category, other parameters must be entered.
Non-applicable parameters are shown in reduced highlight depending on your selection.

- Category - Specifies the category of statistics (network, port, station, or other) that you want to collect.
- Type - The contents of this menu vary depending on the option you have selected from the Category field. The full list of counters is summarized in Table 6.

Table 6. Summary of Threshold Counters

Type	Description
frames	Blocks of characters in the standard frame panel used by the Token-Ring protocol.
bytes	8-bit strings of data
broadcast frames	Frames sent to the broadcast address and received by all stations.
multicast frames	Frames sent to the multicast address.
hard errors	Fatal errors that require beacon recovery.
soft errors	Errors that are recoverable by the MAC layer protocol. These include line errors, burst errors, lost frame errors, ARI/FCI set errors, frame copy errors, receive congestion errors, and token errors.

- Network - This field is applicable when network or station has been selected from the Category field.
- MAC Address - This field allows you to specify the MAC address for the station you want to monitor. This field is applicable when the Station option has been selected in the Category field.
- Slot/Port - Note that these fields are applicable only when Port level statistics are specified in the Category field.
- MIB Variable - Applicable when the variable for Type is *other*. It must be a complete MIB object identifier, including indexes if any.
- Threshold Limit Value - Use this field to define the value which, when exceeded, causes the TRMM to generate an SNMP trap. Nways Manager-LAN determines whether a trap should be generated by comparing the threshold limit for a counter with the counter value at the end of an interval minus the counter value at the beginning of the interval.
- Threshold Current Value - The current value of the variable you chose to monitor.
- Threshold Status - The state of the threshold. This should be valid if everything is configured correctly.

  Note: If the MIB variable has not yet been specified, Threshold Status is *no-statistic-specified*. If the first interval has not yet completed, **threshStatus** will be not-yet-available.

  If the object referenced by the MIB variable is not accessible, Threshold Status is *not-accessible*. Otherwise, Threshold Status is *valid*.
- Interval - Use the scales to select an interval that defines the period between threshold sampling.
- Description - This field can contain up to 40 characters of text to describe the threshold configuration you have created. The TRMM will use this information to send an SNMP trap if the threshold value has been exceeded.

Testing Hubs

The Test option is available from all level views and the context menu in the Hub Level view. This option allows you to perform problem determination by executing specific tests.

When you select **Hub -> Test** in a Hub Level view, the following options are displayed:

- Request Hub Poll
- Ping
- Echo

When you press MB3 on a module icon in a Hub Level view, the following options are displayed on the context menu:

- Ping
- Echo

Requesting a Hub Poll

The Request Hub Poll option allows you to poll a specified hub to check its status. Polling on request allows you monitor critical resources more often.

To poll a hub on request, follow these steps:

1. From the IBM Hubs Topology, click on the hub you want to select.
2. From the menu bar, select **HubManager -> Test -> Request Hub Poll**. The results of the poll are displayed in the Poll Results section of the Request Hub panel.

Notes:

1. The Request Hub Poll panel is the only panel which is selectable even if the hub has not been polled before. All other options are shown in reduced highlight.
2. The Request Hub Poll panel shows the information returned when the Master Management module is requested for module configuration and station information.

The **Restart** pushbutton allows the poll to be reissued.

Notes:

1. The Demand Poll function retrieves standard MIB variables while the Request Hub Poll option retrieves hub-specific parameters.
2. Requesting a poll triggers forced polling. See “Polling Hubs” on page 117 for details.

Pinging Agents in a Hub

The Ping option can be selected:

- From the Root View by selecting **IP Network -> Hub -> Device**.
- From a Hub Level view by doing one of the following:
  - By pressing MB3 on an agent icon and selecting **Test -> Ping** from the context menu. An emulator window is displayed showing the Ping taking place.
  - By selecting **Hub -> Test -> Ping**. from the menu bar in the Hub Level view.

    A panel is displayed showing a list of all the agents in the hub that can be pinged.

    Note: An asterisk (*) next to a slot number means that the Master Management module is installed in the slot.

    When you click on an agent in the list box, information from the NetView for AIX Object Database and the Nways Manager-LAN database is displayed in the System Table section on the Ping panel.

    When you select an agent and click on the **Ping** pushbutton, an emulator window is displayed showing the ping taking place.

If the selected module is not an agent, the Ping option is shown in reduced highlight in the context menu.

The Ping option performs a standard echo test on a Management module by sending one ICMP packet to the module and waiting for a reply. A message is displayed in a

terminal emulator window indicating the result of the test. A successful test means that the agent in the selected hub is operating correctly and Nways Manager-LAN has IP connectivity to them.

Starting and Stopping a Remote Echo Test

The Echo function can be selected only from the context menu of a module. It cannot be selected from the menu bar and is available only for 8250 agents and 8260 Master DMMs.

The Echo option performs a remote echo test of any other IP node that supports the Internet Control Message Protocol (ICMP) Echo protocol. A panel is displayed to allow you to change the settings for the echo test.

You can change the following parameters:

To IP Address	IP address to test
Pattern	Pattern of bits to be sent during the test. To change the default pattern, click on the menu button and select an option from the list that is displayed.
Packet Size	Size of the test packets. Packets can be from 64 to 1500 bytes long. When testing equipment and lines that show problems under a heavy load, increase the packet size.
Number of packets	Number of packets to be sent during the test. Between 1 and 255 packets can be used. When testing for intermittent faults, increase the number of packets used.

Click on the **Start** pushbutton to start the echo test. Click on the **Stop** pushbutton to stop the echo test and display the results. If the test was successful, the number of packets successfully received is shown in the Packets Received field.

While the echo test is running, all the pushbuttons at the bottom of the screen are shown in reduced highlight and cannot be selected. To stop the test, click on the **Stop** pushbutton.

If the test failed, repeat the test with different parameters and use the Statistics utility to record the errors for analysis.

Chapter 12. Listing Unauthorized Users

Use the **Show Intruders** option to display information about unauthorized users that try to access the network through a port.

To display unauthorized user calls, open a Hub Level view and do one of the following:

- From the menu bar, select **Hub -> Show -> Show Intruders**.
- Display the context menu for a port and select **Show Intruders**.

The Show Intruders panel is displayed.

- For 8250 Hubs, the panel displays the action taken on the port that received the unauthorized call. The action can be *Disable* or *No Action*.
- For 8260 Hubs, the panel displays the network on which the unauthorized call was received.

In the List of Intruders field, each unauthorized attempt to access the network through ports on an 8260 Hub is shown with one attempt per line. The **Clear All** pushbutton removes all the entries in the field.

Chapter 13. Displaying Fault Information

To view error information about an object in an NetView for AIX submap (such as a hub, module, port and so on), do one of the following:

- From the IBM Hubs Topology, select a hub and then select **HubManager -> Fault** from the menu bar.
- From a Hub Level view, select **Hub -> Fault** from the menu bar or display the context menu for an object and select **Fault**.

The error information is displayed in the All Events Browser panel. The events are logged for further analysis.

Note: When you activate the **Fault** menu on an object, two windows are displayed:

- One for all general events (if a window does not already exist).
- One with filtering done on the selected object.

You can open several event lists at the same time. By selecting **File -> Close** from the menu bar, you close all the event lists that are currently open.

For more information about how faults are handled, refer to “Chapter 16. Working With Traps” on page 151.

Chapter 14. Displaying Statistics

You can work with two different types of statistics:

- RMon (Remote Monitor)
- Private (8250, 8260, and 8265 Device Manager component of Nways Manager-LAN)

Statistical Information for Remote Monitor

If you have installed Remote Monitor, you can start it any of the following ways:

- From a Hub Level view, select **Hub -> Statistics... -> RMon**. (This displays a Summary panel for 8250, 8260, and 8265 Device Manager instead of for Remote Monitor. See “Displaying the Hub Level RMON Statistics Summary” on page 131 for more information.)
- From a Hub Level view, display the context menu for a module, port, or network and select **Statistics -> RMon**.
- From a Module Level view, display the context menu for a port and select **Statistics -> RMon**.

Different RMon statistics are displayed depending on:

- The type of module, port, or network you selected
- Whether the RMON probe is currently monitoring the corresponding network
- Whether the Remote Monitor application is installed.

The following RMon statistics options are available according to the version of Remote Monitor you have installed:

- **Summary** - Starts the Remote Monitor Summary window.
- **Alarm** - Invokes the Alarm application to trace specific events on the network.
- **Host** - Invokes the Host Table application which displays statistics about hosts on a network. If a port is selected and there is an associated MAC Address, it will display the statistics for that MAC Address.
- **Host TopN** - Invokes the Host Table application which displays statistics about the TopN host talkers on a segment.
- **Matrix** - Invokes the Matrix application which identifies the network devices that are communicating and the type of traffic flowing between them. If a port is selected and there is an associated MAC Address, it will display the traffic flowing to and from this MAC Address.
- **Statistics** - Invokes the Statistics application which allows you to view network statistics on any combination of packets, bytes, errors, size distributions, multicasts, and so on.
- **History** - Invokes the History application which specifies a sample period and spots trends over the period.

- **Capture** - Invokes the Capture application which captures packets according to specific alarm conditions, filters out only those packets you want to see, and stores the results for analysis.
- **Ring Station** - Invokes the Ring Station application which allows you to analyze the subtle relationships between seemingly separate events on a Token-Ring network.
- **Ring Station Order** - Displays the Ring Station Map. If a port is selected and there is an associated MAC Address, the ring display will start with that MAC Address.

For more information on these Remote Monitor applications, refer to *IBM Nways Remote Monitor: Installation and User's Guide* (SA33-0367). A dialog window is displayed allowing you to set parameters such as polling, category, and so on. To bypass this panel, you can add these parameters to the shell script **/usr/CML/bin/iub.lm.interface**. The command syntax is described in the *IBM Nways Remote Monitor: Installation and User's Guide* (SA33-0367).

Note: RMON statistics are displayed in the same format each time. To display statistics in a different format, you must open the shell script and specify different values for the parameters.

Table 7 and Table 8 display the types of statistics available for different versions of Ethernet and Token-Ring probes.

Table 7. Ethernet Probes Required for 8250 and 8260 Hubs

Type of Statistics	**E-MAC**	**HE-MAC**	**E-Probe**
Alarm	V2.00	V1.00	V1.00
Host	V2.00	V1.00	V1.00
Host TopN	V2.00	V1.00	V1.00
Matrix	V2.00	V1.00	V1.00
Statistics	V2.00	V1.00	V1.00
History	V2.00	V1.00	V1.00
Capture	–	V1.00	V1.00
Event	V2.00	V1.00	V1.00
Filter	–	V1.00	V1.00
DLM-ECAM	–	V1.00	V1.00
Note: The version numbers are the minimum version required for each Ethernet probe.			

Table 8. Token-Ring Probes Required for 8250 and 8260 Hubs

Type of Statistics	**T-MAC**	**H-TMAC**	**TRMM**
Alarm	V2.00 + DMM V2.2	V2.00 + DMM V2.2	V4.00
Host	V2.00	V1.01	V4.00
Host TopN	–	V1.01	V3.1A[1]
Matrix	–	V1.01	V4.00
TR MAC Statistics	V2.00	V1.01	V3.10

Table 8. Token-Ring Probes Required for 8250 and 8260 Hubs (continued)

Type of Statistics	T-MAC	H-TMAC	TRMM
TR Promi Statistics	V2.00	V1.01	V3.10
TR MAC History	–	V1.01	V3.10
TR Promi History	–	V1.01	V3.10
Capture	–	V1.01	–
Ring Station	V2.00	V1.01	V4.00
Ring Station Order	V2.00	V1.01	V4.00
Ring Station Configuration	V2.00	V1.01	V4.00
Source Routing	V2.00	V1.01	V4.00
Event	V2.00	V1.01	V4.00
Filter	–	V1.01	–
DLM-ECAM	–	V1.01	–

Note:

1. TRMM V4.00 implements the Host TopN. TRMM V3.1A, however, implements the Host TopN group in a private way.
2. The version numbers in the table are the minimum version required for each Token-Ring probe.

Displaying the Hub Level RMON Statistics Summary

The hub level RMON statistics summary panel allows you to select which probe and interface to use when collecting statistics for a network.

Select one of the entries shown and click on the **IBM RMON** pushbutton. The Remote Monitor Summary window is displayed for the selected interface.

Displaying 8250, 8260, and 8265 Device Manager Statistical Information

The 8250, 8260, and 8265 Device Manager Statistics function can be started:

- From NetView for AIX (for 8260 Hubs only):
  - From the menu bar of the IBM Hubs Topology by selecting **HubManager -> Statistics...**.
  - From the context menu displayed by clicking MB3 on a hub in the IBM Hubs Topology by selecting **HubManager -> Statistics...**.
- From 8250, 8260, and 8265 Device Manager:
  - From the Hub menu (for 8260 Hubs). Select **Hub -> Statistics... -> Private**.
  - From the Hub Level View using the context menu (8250 Hub and 8260 Hubs) for a selected module or port. Select **Statistics... -> Private**.
  - From the Module Level View using the context menu (8250 Hub and 8260 Hubs) for a selected station or port. Select **Statistics... -> Private**.

Note: From the module context menu, you can access network and module statistics. From the port context menu, you can access network and port statistics.

Selecting the Statistics to Display

The Statistics Selection panel is displayed.

The Statistics Selection panel displays one of the following resource names:

- Hub label for power budget.
- Port number plus slot number plus hub label for a port resource.
- Slot number plus hub label for a module resource.
- Network ID plus hub label for a network resource.

In the panel, you can:

- Select one of the lines shown in the Category section.
- Select one or more of the counters available for that category in the Counters field. By default, all available counters are selected; to deselect a counter, click on its name in the list. There are two exceptions to this rule:
  - For the TopN category, only one counter at a time can be selected.
  - For the Power Budget category, all counters are selected and cannot be deselected. That is, all counters must be run together.
- Change the polling interval.
- Specify the directory and filename of the log file.
- Specify whether to log the results in a file.

  If this field is set to *Off*, the results are not saved and are shown only on the screen.

After you enter parameters in the Statistics Selection panel, click on **Apply** to display the Statistics Display panel.

Note: One of the following messages may be displayed:

- No Category defined - A statistics category has not been defined for this resource (which can be a hub, module, port, or a network resource which is accessible through a port or a module). This may happen in the case of new modules.
- No Category available - Statistics categories are defined for the resource but are not available. This means that there is no Management module for this module or port, or that the associated Management module does not support statistics.

In both cases, click on **OK** to remove the message box. Then click on **Close** in the Statistics Selection Panel.

Using TopN statistics, you can display more information about the stations in the Search panel (see “Using the Search Function” on page 95). Double-click MB1 on a MAC

Address and use MB2 to put it into the **Search for** field in the Search Panel. This allows you to do a search on the MAC Address and, if it is known, to highlight it on the graphical view using the **Show** pushbutton.

On the left of the Statistics Display panel (at the bottom of the Power Budget panel), the value for each statistic is displayed.

At the bottom of the Statistics Display panel (on the left of the Power Budget panel), you can perform these actions:

- Select the following types of values to be displayed in the list of statistics:

  Current Current values

  Marker Values pointed to by the marker (available if the display is a plot display)

  Peak Peak values since the beginning of the polling or from the last reset

  Reset Resets the peak values.

  Note: The marker is shown in the graphic area, only for specific categories, when there is a plot display. It is a red vertical line that you can move by clicking the mouse at the position where you want the marker to appear. If the marker is outside of the plotted area, the values are filled by
- Select the type of display:
  - Plot (only available for some categories)
  - Bar
  - Pie

  Note: If you select the Pie display type but all values are equal to zero, the graphic area on the right remains empty.
- Invert the display for plot or bar display.
- Print the panel.
- Call the Control panel.

On the right of the Statistics Selection panel, a plot, bar, or pie graph is displayed. The terms used on the vertical axis have the following meanings:

Units The real values of the MIB variables.

Units/PollInt The difference in the values of the MIB variables between two polls.

Units/s The difference in the values of the MIB variables between two polls, divided by the polling interval value.

% The percentage of use according to media capacity, or for Power Budget, according to power availability.

At the same time, the Statistics Control panel is displayed. This panel gives you a list of all the statistics that you have already started. When you have selected a statistics entry, you can use the:

- **Stop** pushbutton to stop the polling of the selected statistic. The Statistics Display panel is frozen.
- **Restart** pushbutton to continue polling the selected statistic. The contents of the Statistics Display panel are cleared and new values are displayed.
- **Front** pushbutton to bring the associated Statistics Display panel to the foreground.
- **Modify** pushbutton to modify the parameters for the selected statistic. The Statistics Attribute panel is displayed.
- **Delete** pushbutton to delete the associated Statistics Display panel.

When you click the **Exit** pushbutton at the bottom of the panel, a confirmation dialog box is displayed before all the statistics panels are deleted.

Multiple requests for statistics can be started on different resources and will display separate display panels for each resource.

Note: Multiple requests for the same resource and category will result in any existing panel being brought to the front.

Specifying Statistics Attributes

The Statistics Attribute panel is displayed when you click on the **Modify** pushbutton in the Statistics Control panel. You can modify the following parameters in this panel:

- Polling Interval
- File Logging:
  - You can enter a new directory or file
  - You can specify whether or not to activate file logging.

Printing Statistics Information

To print the statistics presented in graphical format in the Statistics Display panel, click on **Print**.

The Statistics Print panel is displayed. Enter the following print information in the Destination box:

- In the Printer field, enter the name of the printer. For best printing results, it is recommended that you use a color printer. If you do not specify a printer, the default is used.
- In the Directory and File fields, enter the path and name of the file you want to print.

Replaying Statistics Information

Any statistical information (except for Power Budget and TopN statistics) that you have collected and logged can be viewed at any time by replaying the data.

Replaying statistics is similar to real-time graphing except that:

- Only the plot display is available.

- The **Print** pushbutton is not available.

You can view multiple sets of recorded data in the same log file. You can use a Zoom function to expand a selected part of the displayed graph.

To replay statistics, do one of the following:

- From the command line, enter `/usr/CML/bin/iubStatReplay <filename>` where `<filename>` is the name of the file with the statistics you want to display.
- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Statistics -> Remove Statistics files**. Then enter the name of the file with the statistics you want to display and press Enter.
- From the menu bar, select **Administer -> Nways Campus Manager**. From the SMIT main menu, select **Statistics -> Replay**. Then enter the name of the file with the statistics you want to display and press Enter.

To stop statistics from replaying, click on **Close** in the Replay window.

Clearing Statistics

To erase the statistical information displayed in the Statistics panel, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Statistics -> Remove Statistics files**.
- From the menu bar, select **Administer -> Nways Campus Manager**. Then from the SMIT main menu, select **Statistics -> Remove Statistics files**.

Statistics Categories

This section contains a list of categories for each resource type and a list of MIB variables for each category.

Table 9. Statistics Categories: 8260 Hubs

Power_Budget for each voltage type (-12V -5V +2V +5V +12V)	
Voltage_level	Actual voltage level as sensed on the backplane. This voltage is supplied by all operational power supplies.
Power_capacity	Maximum watts of this voltage available from the currently installed power supplies.

Table 9. Statistics Categories: 8260 Hubs (continued)

Power_available	Watts of this voltage available for new modules. If power fault-tolerant mode is enabled (when it was previously disabled), this value is decreased by the amount of power reserved for this voltage. If power fault-tolerant mode is disabled (when it was previously enabled), this value is increased by the amount of power that is returned to the available power budget for the given voltage type.
Power_consumed	Watts consumed by all hub modules. For a given voltage, this value is the sum total of the power consumed by the hub itself, two Controller modules, all installed hub modules, and all power-enabled slots containing IBM 8260 modules. If power fault-tolerant mode is enabled (when it was previously disabled), this value is increased by the amount of power reserved for the given voltage. If power fault-tolerant mode is disabled (when it was previously enabled), this value is decreased by the amount of power that is returned to the available power budget for the given voltage.
Power_unmanaged	Amount of power consumed by modules not controlled through power management.

Note: All counters are selected. You cannot deselect a counter.

Table 10. Statistics Categories: Token-Ring

Network_Traffic	
Frames_received	Throughput rate, in number of frames on the network per second.
Mac_Frames_received	Throughput rate, in number of MAC frames on the network per second. MAC frames are made up of packets specific to the token ring protocol.
Broadcast_Frames_received	Throughput rate, in number of non-MAC frames transmitted to a broadcast address per second.
Multicast_Frames_received	Throughput rate, in number of non-MAC frames transmitted to a multicast address per second.
Network_Utilization	
Data_bandwidth	Percentage of ring capacity being used by non-MAC frames.
MAC_bandwidth	Percentage of ring capacity being used by MAC frames.
Network_Distribution	
18-63_octet_frames	Number of non MAC-frames with a size between 16 and 63 bytes.

Table 10. Statistics Categories: Token-Ring (continued)

64-127_octet_frames	Number of non MAC-frames with a size between 64 and 127 bytes.
128-255_octet_frames	Number of non MAC-frames with a size between 128 and 255 bytes.
256-511_octet_frames	Number of non MAC-frames with a size between 256 and 511 bytes.
512-1023_octet_frames	Number of non MAC-frames with a size between 512 and 1023 bytes.
1024-2047_octet_frames	Number of non MAC-frames with a size between 1024 and 2047 bytes.
2048-4095_octet_frames	Number of non MAC-frames with a size between 2048 and 4095 bytes.
4096-8191_octet_frames	Number of non MAC-frames with a size between 4096 and 8191 bytes.
8192-18000_octet_frames	Number of non MAC-frames with a size between 8192 to 18000 bytes.
>18000_octet_frames	Number of non MAC-frames with a size greater than 18000 bytes.
Network_Errors	
Line_errors	Incremented when a frame or token is copied or repeated by a station. The E bit is zero in the frame or token, and one of the following conditions exists: 1. There is a non-data bit (J or K bit) between the SD and the ED of the frame or token. 2. There is an FCS error in the frame (incorrect checksum).
Burst_errors	Incremented when a station detects the absence of transitions for five half-bit timers (burst-five error).
Address_copied_errors	Incremented when a station receives an AMP or SMP frame in which A=C=0, and then receives another SMP frame with A=C=0 without first receiving an AMP frame. Identifies a station that cannot set the AC bits properly.
Lost_Frames	Incremented when a station is transmitting and its TRR timer expires. Indicates a condition where a transmitting station in strip mode does not receive the trailer of the frame before the TRR timer expires.
Congestion	Congestion occurs when too many packets are present on the network and performance degrades. This counter increments when a station recognizes a frame addressed to itself, but has no available buffer space.

Table 10. Statistics Categories: Token-Ring (continued)

Frame_copied_errors	Incremented when a station recognizes a frame addressed to itself and detects that the FS field A bits are set to 1, indicating a possible line hit or duplicate address.
Token_errors	Incremented when a station acting as the active monitor recognizes an error condition that requires it to transmit a token.
Duplicate_address	The number of times this station experienced a duplicate address error.
Beacon_events	Number of times that the ring entered the beaconing state. (A station transmits a beacon frame when it notices that either of its neighbors appears to be dead).
Drop_events	Total number of times one or more frames are dropped because of heavy traffic. Note that this number is not necessarily the number of frames dropped; it is just the number of times this condition has been detected.
Token_Rotation_Time	
Rotation_Time	Estimated time, in microseconds, a token requires to complete a single rotation on the ring.
TopN (See Warning)	
In_Frames	The activity of the 8 highest stations is displayed, according to the number of frames transmitted to these stations during the last TopN data collection period. The MAC Addresses of these stations are displayed.
Out_Frames	The activity of the 8 highest stations is displayed, according to the number of frames transmitted by these stations during the last TopN data collection period. The MAC Addresses of these stations are given.
In_Octets	The activity of the 8 highest stations is displayed, according to the number of bytes transmitted to these stations during the last TopN data collection period. The MAC Addresses of these stations are given.
Out_Octets	The activity of the 8 highest stations is displayed, according to the number of bytes transmitted by these stations during the last TopN data collection period. The MAC Addresses of these stations are given.

Table 10. Statistics Categories: Token-Ring (continued)

Out_Errors	The activity of the 8 highest stations is displayed, according to the number of errors transmitted by these stations during the last TopN data collection period. The MAC Addresses of these stations are given. Only isolating errors (LineErrors, BurstErrors, ACErrors, InternalErrors, and AbortErrors) and CongestionErrors are counted.
Out_BroadcastFrames	The activity of the 8 highest stations is displayed, according to the number of frames transmitted by these stations that were directed to a broadcast address during the last TopN data collection period. The MAC Address of these stations are given.
Out_MulticastFrames	The activity of the 8 highest stations is displayed, according to the number of frames transmitted by these stations that were directed to a multicast address during the last TopN data collection period. The MAC Addresses of these stations are given.

Notes:

1. You can only select one counter at a time.
2. When you start a TopN statistic, the polling time in the agent is set with Polling Interval value (this polling time is common for all TopN statistics on the agent):
   - If the setting failed only because of a write protection problem, a message such as `The MIB variable setting failed for xxx` is displayed. The Polling Interval is changed (or not if it is the same value) with the agent polling time and a message such as `polling time of 'xxx' has been changed to yy seconds` is displayed where `xxx` is the resource and category name.
   - If other TopN statistics have already been started on the same agent with a different polling interval, a message such as `polling time of 'xxx' has been changed to yy seconds` is displayed during the polling interval, where `xxx` is the resource and category name. The Polling Interval is set to the new value.

Table 11. Statistics Categories: Token Ring Networks

dot5	Only available with a TMAC V2.
Line_errors	Number of Line errors detected at the T-MAC station.
Burst_errors	Number of Burst errors detected at the T-MAC station.
AC_errors	Number of AC errors detected at the T-MAC station.
Abort_transmitted_errors	Number of Abort Transmitted errors detected at the T-MAC station.
Internal_errors	Number of Internal errors detected at the T-MAC station.

Table 11. Statistics Categories: Token Ring Networks (continued)

Lost_frame_errors	Number of Lost frame errors detected at the T-MAC station.
Receiver_congestion_errors	Number of Receiver congestion errors detected at the T-MAC station.
Frame_copied_errors	Number of Frame copied errors detected at the T-MAC station.
Token_errors	Number of Token errors detected at the T-MAC station.
Soft_errors	Number of Soft errors detected at the T-MAC station.
Hard_errors	Number of Hard errors detected at the T-MAC station.
Signal_losses	Number of Signal losses detected at the T-MAC station.
Transmit_beacons	Number of times the T-MAC station has transmitted a beacon frame.
Recoveries	Number of times the T-MAC station has been purged from the ring and then recovered.

Table 12. Statistic Categories: Token-Ring Ports

Port_Traffic	
In_frames	Throughput rate, in number of frames transmitted to this address per second.
Out_frames	Throughput rate, in number of frames transmitted by this address per second.
Out_errors	Throughput rate, in number of error frames transmitted by this address per second. Only isolating errors (LineErrors, BurstErrors, ACErrors, InternalErrors, and AbortErrors) and CongestionErrors are counted.
Broadcast_Frames	Throughput rate, in number of frames transmitted by this address directed to the broadcast address per second.
Multicast_Frames	Throughput rate, in number of frames transmitted by this address directed to a multicast address per second. This number does not include frames directed to the broadcast.
Port_Utilization	
In_Octets	Throughput rate, in number of bytes transmitted to this address per second.
Out_Octets	Throughput rate, in number of bytes transmitted by this address per second.
Port_Errors	

Table 12. Statistic Categories: Token-Ring Ports (continued)

Line_errors	Incremented when a frame or token is copied or repeated by a station. The E bit is zero in the frame or token, and one of the following conditions exists: 1. There is a non-data bit (J or K bit) between the SD and the ED of the frame or token. 2. There is an FCS error in the frame (incorrect checksum).
Burst_errors	Incremented when a station detects the absence of transitions for five half-bit timers (burst-five error).
Address_copied_errors	Incremented when a station receives an AMP or SMP frame in which A=C=0, and then receives another SMP frame with A=C=0 without first receiving an AMP frame. Identifies a station that cannot set the AC bits properly.
Lost_frames	Incremented when a station is transmitting and its TRR timer expires. Indicates a condition where a transmitting station in strip mode does not receive the trailer of the frame before the TRR timer expires.
Congestion	Congestion occurs when too many packets are present on the network, and performance degrades. This counter increments when a station recognizes a frame addressed to itself, but has no available buffer space.
Frame_copied_errors	Incremented when a station recognizes a frame addressed to itself and detects that the FS field A bits are set to 1, indicating a possible line hit or duplicate address.
Token_errors	Incremented when a station acting as the active monitor recognizes an error condition that requires it to transmit a token.
Duplicate_address	The number of times this station experienced a duplicate address error.

Table 13. Statistics Categories: Ethernet Networks

Network_Traffic	
Frames_received	Throughput rate, in number of valid frames successfully received by this network per second.
Multicast_Frames_received	Throughput rate, in number of valid multicast-address packets received by this network per second. Multicast is a technique that allows a single packet to be addressed to a selected subset of destinations.

Table 13. Statistics Categories: Ethernet Networks (continued)

Broadcast_Frames_received	Throughput rate, in number of valid broadcast-address packets received by this network per second. Broadcast is a form of multicast in which a packet is addressed to all possible destinations.
Network_Utilization	
Bandwidth	Percentage of media capacity: number of valid bits received per second, divided by 2**20 (theoretical maximum bandwidth) * 100.
Network_Errors	
Frame_too_long	Number of frames received that exceed the maximum permitted Ethernet frame size (1518 bytes).
Alignment_errors	Number of frames that did not pass the FCS check (Frame Check Sequence) and that are not an integral number of bytes. These frames are not counted in FCS Errors.
FCS_errors	Number of frames that did not pass the FCS check (Frame Check Sequence), that is, have incorrect checksums, and are an integral number of bytes.
Runts	Number of runt (less than 512 bits long) frames recorded over this network.
Local_collisions	Number of times that two or more ports within this concentrator have received traffic simultaneously.
Drop_events	Total number of events in which frames were dropped due to lack of resources. Note that this number is not necessarily the number of frames dropped; it is just the number of times this condition has been detected.
Short_events	This counter is the total of the values of the Short_events counters for all of the ports in the network (only available on 8260 hubs).
Collisions	This counter is the total of the values of the Collisions counters for all of the ports in the network (only available on 8260 hubs).
Late_events	This counter is the total of the values of the Late_events counters for all of the ports in the network (only available on 8260 hubs).
Very_long_events	This counter is the total of the values of the very_long_events counters for all of the ports in the network (only available on 8260 hubs).
Data_rate_mismatches	This counter is the total of the values of the Data_rate_mismatches counters for all of the ports in the network (only available on 8260 hubs).

Table 13. Statistics Categories: Ethernet Networks (continued)

Auto_partitions	This counter is the total of the values of the Auto_partitions counters for all of the ports in the network (only available on 8260 hubs).

Table 14. Statistics Categories: Ethernet Modules

Module_Traffic	
Frames_received	Throughput rate, in number of valid frames received per second by this module.
Multicast_Frames_received	Throughput rate, in number of valid multicast-address packets received by this module per second. Multicast is a technique that allows a single packet to be addressed to a selected subset of destinations.
Broadcast_Frames_received	Throughput rate, in number of valid broadcast-address packets received by this module per second. Broadcast is a form of multicast in which a packet is addressed to all possible destinations.
Module_Utilization	
Bandwidth	Percentage of media capacity: number of valid bits received by this module per second, divided by 2**20 (theoretical maximum bandwidth) * 100.
Module_Errors	
Frame_too_long	Number of frames received by this module that exceed the maximum permitted Ethernet frame size (1518 bytes).
Alignment_errors	Number of frames that did not pass the FCS check (Frame Check Sequence) and that are not an integral number of bytes. These frames are not counted in FCS Errors.
FCS_errors	Number of frames that did not pass the FCS check (Frame Check Sequence), that is, have incorrect checksums, and are an integral number of bytes.
Runts	Number of runt (less than 512 bits long) frames recorded over this module.

Attention: Accessible only on per-module switching module managed by an EMM (not a DMM).

Table 15. Statistics Categories: Ethernet Ports

Port_Traffic	
Frames_received	Throughput rate, in number of valid frames received on this port per second.

Table 15. Statistics Categories: Ethernet Ports (continued)

Multicast_Frames_received	Throughput rate, in number of valid multicast-address packets received on this port per second. Multicast is a technique that allows a single packet to be addressed to a selected subset of destinations.
Broadcast_Frames_received	Throughput rate, in number of valid broadcast-address packets received on this port per second. Broadcast is a form of multicast in which a packet is addressed to all possible destinations.
Port_Utilization	
Bandwidth	Percentage of media capacity: number of valid bits received per second, divided by 2**20 (theoretical maximum bandwidth) * 100.
Port_Errors	
Frame_too_long	Number of frames received on this port that exceed the maximum permitted Ethernet frame size (1518 bytes).
Alignment_errors	Number of frames that did not pass the FCS check (Frame Check Sequence) and that are not an integral number of bytes. These frames are not counted in FCS Errors.
FCS_errors	Number of frames that did not pass the FCS check (Frame Check Sequence), that is, have incorrect checksums, and are an integral number of bytes.
Runts	Number of runt (less than 512 bits long) frames recorded on this port.
Short_events	Packets received containing less than 80 bits (only available on 8260 hubs).
Collisions	Total number of collisions detected (only available on 8260 hubs)
Late_events	Collision detected after 512 bits were received from a port (only available on 8260 hubs).
Very_long_events	Port entered a jabber lockup state due to a timeout (only available on 8260 hubs).
Data_rate_mismatches	Number of FIFO overflow and underflow occurrences (only available on 8260 hubs).
Auto_partitions	Number of times the autopartition threshold has been passed (only available on 8260 hubs).

Table 16. Statistics Categories: FDDI Networks

Network_Traffic	
Frames_received	Frames count per second (refer to ANSI MAC 2.2.1).
Network_Errors	

Table 16. Statistics Categories: FDDI Networks (continued)

Ring_oper_count	Number of times the ring transitioned to operational.
Errors	Number of errors.
Lost_Frames	Number of lost frames.
Network_Error_Ratio	
Error_ratio	(delta LostFrames + delta Errors)/(delta LostFrames + delta Frames) x 2**16.

Table 17. Statistics Categories: FDDI Modules

Module_Errors	
Mgt_rcv_errors	Number of errors encountered while receiving data on the Management Channel.
Mgt_xmit_errors	Number of errors encountered while transmitting data on the Management Channel.
Back-plane_errors	Number of invalid FDDI symbols received from another FDDI module over the hub's backplane.
Phased_lock_loop_errors	Number of times the receive clock circuitry on the module failed to recognize a backplane clock and unlocked.

Table 18. Statistic Categories: FDDI Ports

Port_Errors	
LCT_failure	Link Confidence Test failures: number of successive link failures detected during the connection process (as detected by the Link Confidence Test) during connection management. Once the connection has been established, the count reverts to zero. (Refer to ANSI 9.4.1.)
LER_estimate	Link Error Rate estimate: long-term average link error rate based on the current LER error count. The error rate ranges from 15 (good: 10**-15) to 4 (poor: 10**-4). A 0 entry indicates an unconnected port.
LEM_rejects	Link Error Monitor rejects: number of times the link has reinitialized as a result of excessive link errors reported by the link error monitor.
LEM_errors	Link Error Monitor errors: number of invalid line state transitions as reported by the link error monitor. The link error monitor error count is set to zero only on station powerup. The long-term rate average of this variable is the LER Estimate.

Table 19. Statistics Categories: RMON Error Report View

Line_errors	The total number of line errors reported in error reporting packets detected by the probe.

Table 19. Statistics Categories: RMON Error Report View (continued)

Internal_errors	The total number of adapter internal errors reported in error reporting packets detected by the probe.
Burst_errors	The total number of burst errors reported in error reporting packets detected by the probe.
AC_errors	The total number of AC (Address Copied) errors reported in error reporting packets detected by the probe.
Abort_errors	The total number of abort delimiters reported in error reporting packets detected by the probe.
Lost_frame_errors	The total number of lost frame errors reported in error reporting packets detected by the probe.
Congestion_errors	The total number of receive congestion errors reported in error reporting packets detected by the probe.
Frame_copied_errors	The total number of frame copied errors reported in error reporting packets detected by the probe.
Frequency_errors	The total number of frequency errors reported in error reporting packets detected by the probe.
Token_errors	The total number of token errors reported in error reporting packets detected by the probe.
Soft_error_reports	The total number of soft error report frames detected by the probe.

Table 20. Statistics Categories: RMON Beacon View

Beacon_time	The total amount of time that the ring has been in the beaconing state.
Beacon_events	The total number of times that the ring enters a beaconing state (beaconFrameStreamingState, beaconBitStreamingState, beaconSetRecoveryModeState, or beaconRingSignalLossState) from a non-beaconing state. Note that a change of the source address of the beacon packet does not constitute a new beacon event.
Beacon_packets	The total number of beacon MAC packets detected by the probe.
Purge_packets	The total number of ring purge MAC packets detected by probe.
Purge_events	The total number of times that the ring enters the ring purge state from normal ring state. The ring purge state that comes in response to the claim token or beacon state is not counted.

Table 20. Statistics Categories: RMON Beacon View (continued)

Claim_token_events	The total number of times that the ring enters the claim token state from normal ring state or ring purge state. The claim token state that comes in response to a beacon state is not counted.
Claim_token_packets	The total number of claim token MAC packets detected by the probe.

Table 21. Statistics Categories: RMON Packet Distribution

18-63_Bytes	The total number of good non-MAC frames received that were between 18 and 63 bytes in length inclusive, excluding framing bits but including FCS bytes.
64-127_Bytes	The total number of good non-MAC frames received that were between 64 and 127 bytes in length inclusive, excluding framing bits but including FCS bytes.
128-255_Bytes	The total number of good non-MAC frames received that were between 128 and 255 bytes in length inclusive, excluding framing bits but including FCS bytes.
256-511_Bytes	The total number of good non-MAC frames received that were between 256 and 511 bytes in length inclusive, excluding framing bits but including FCS bytes.
512-1023_Bytes	The total number of good non-MAC frames received that were between 512 and 1023 bytes in length inclusive, excluding framing bits but including FCS bytes.
1024-2047_Bytes	The total number of good non-MAC frames received that were between 1024 and 2047 bytes in length inclusive, excluding framing bits but including FCS bytes.
2048-4095_Bytes	The total number of good non-MAC frames received that were between 2048 and 4095 bytes in length inclusive, excluding framing bits but including FCS bytes.
4096-8191_Bytes	The total number of good non-MAC frames received that were between 4096 and 8191 bytes in length inclusive, excluding framing bits but including FCS bytes.
8192-18000_Bytes	The total number of good non-MAC frames received that were between 8192 and 18000 bytes in length inclusive, excluding framing bits but including FCS bytes.
>18000_Bytes	The total number of good non-MAC frames received that were greater than 18000 bytes in length, excluding framing bits but including FCS bytes.

Table 22. Statistics Categories: RMON Packet View

Drop_events	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected. This value is the same as the corresponding tokenRingMLStatsDropEvents.
Data_packets	The total number of non-MAC packets in good frames received.
Data_broadcast_packets	The total number of good non-MAC frames received that were directed to an LLC broadcast address (0xFFFFFFFFFFFF or 0xC000FFFFFFFF).
Data_mulitcast_packets	The total number of good non-MAC frames received that were directed to a local or global multicast or functional address. Note that this number does not include packets directed to the broadcast address.

Table 23. Statistics Categories: RMON Host View

In_packets	The number of packets without errors transmitted to this address since it was added to the hostTable.
Out_packets	The number of packets including errors transmitted by this address since it was added to the hostTable.
In_bytes	The number of bytes transmitted to this address since it was added to the hostTable (excluding framing bits but including FCS bytes), except for those bytes in packets that contained errors.
Out_bytes	The number of bytes transmitted by this address since it was added to the hostTable (excluding framing bits but including FCS bytes), including those bytes in packets that contained errors.
Out_errors	The number of error packets transmitted by this address since this host was added to the hostTable.
Out_broadcast_packets	The number of good packets transmitted by this address that were directed to the broadcast address since this host was added to the hostTable.
Out_multicast_packets	The number of good packets transmitted by this address that were directed to a multicast address since this host was added to the hostTable. Note that this number does not include packets directed to the broadcast address.

Chapter 15. Managing the User Interface

Setting Forms to Their Default Size

The Default Size function resizes 8250, 8260, and 8265 Device Manager windows which have been maximized or had their size altered by clicking MB1 on an edge of the window and dragging the border to resize the window.

To redisplay a window at its default size from a Hub Level view or a Module Level view, select **View -> Default Size** from the menu bar.

Closing All Forms

The Close All Forms function allows you to quickly close all open panels associated with a hub or module. All panels that are displayed, minimized, or hidden behind other windows are closed.

To close all open panels associated with a hub or module in a Hub Level view or a Module Level view, select **View -> Close All Forms** from the menu bar.

Closing All Module Views

The Close All Module Views function allows you to quickly close all Module Level views for a selected Hub Level view. All Module Level views that are displayed, minimized or hidden behind other windows are closed.

To close all Module Level views that were opened from a Hub Level view, select **View -> Close All Module Views** from the menu bar of the Hub Level view.

Closing Views and Forms

Use the Exit function to close the current view and any lower level views and panels opened from the current view. Depending on the view from which you select this option, the following happens:

- If you select **View -> Exit** from the menu bar of a Hub Level view, the Hub Level view and any Module Level views opened from the Hub Level view are closed.
- If you select **View -> Exit** from the menu bar of a Module Level view, Module Level view is closed.

Closing Hub Level Views

The Close function allows you to quickly close all Hub Level views for hubs selected in the IBM Hubs Topology. All Hub Level views for selected hubs, whether minimized or hidden behind other windows, are closed.

To close all Hub Level views for selected hubs:

1. Select one or more hubs in the IBM Hubs Topology Submap by clicking MB1 on them.
2. Select **HubManager -> Close** from the menu bar.

Exiting from 8250, 8260, and 8265 Device Manager

When you exit from 8250, 8260, and 8265 Device Manager, all 8250, 8260, and 8265 Device Manager windows are closed and you also exit from NetView for AIX. You exit from either the Root window or the IBM Hubs Topology by selecting **File -> Exit** from the menu bar.

A dialog box is displayed and prompts you to confirm. Click **OK** to close all 8250, 8260, and 8265 Device Manager panels and exit from NetView for AIX. Click **Cancel** to return to the currently displayed panel.

Chapter 16. Working With Traps

This chapter describes how to work with and customize some of the traps, events, and filters provided by NetView for AIX and used by the 8250, 8260, and 8265 Device Manager component of Nways Manager-LAN.

event management in Nways Manager-LAN is fully integrated with the event management provided by NetView for AIX. However, its behavior differs depending on whether you are using IBM SystemView NetView/6000 V2 or IBM NetView for AIX V4 or V5. See the *NetView for AIX User's Guide* for detailed information.

"General Overview" gives a general overview that applies to both versions of NetView for AIX. "Using NetView for AIX V4 or V5" on page 155 gives specific information when using NetView for AIX V4 or V5.

If you are not familiar with the way NetView for AIX handles traps, events, and filters, read "General Overview" and when necessary, refer to the *NetView for AIX User's Guide*.

For more detailed information on how Nways Manager-LAN interacts with NetView for AIX, refer to the sections in this chapter that describe the level of NetView for AIX you are running.

General Overview

8250 and 8260 agent traps are received by the NetView for AIX **trapd** daemon. These traps are logged in ASCII format in the **/usr/OV/log/trapd.log** file and in binary format in the **/usr/OV/log/ovevent.log** file. They are forwarded to the **iubd** daemon which decodes and processes the traps before returning the interpreted trap to **trapd**. These interpreted traps are also logged in **trapd.log** and **ovevent.log** and are forwarded to **nvevents** for display if this application is running.

The **nvevents** and **nvela** facilities are used by the 8250, 8260, and 8265 Device Manager component to manage the traps received by NetView for AIX. The **nvevents** application allows you to access dynamic and static workspaces, while the **nvela** application provides access to the event log (static workspaces only). Refer to the*NetView for AIX User's Guide* for a complete description of these applications.

Starting nvevents

The **nvevents** application is also called the Event Display Application. To start **nvevents**,

Starting xnmevents

select **Monitor -> Events -> Current Events** from the menu bar of the IBM Hubs Topology. This application displays all the events which have been received and filtered for display during the current NetView for AIX session.

Dynamic Workspaces

Panels that contain dynamic workplaces display the list of events received for a given resource and dynamically update the display to show **new** traps coming from the resource.

Note: Events in the *Log Only* category do not appear in a dynamic workspace but are still logged in the **trapd.log** and**ovevent.log** files.

Static Workspaces

Panels that contain static workplaces display the list of events already received for a resource. Static resources do not dynamically update the display as new events are generated, such as the results of a Search operation from a dynamic workspace.

For example, to display all the events for a given hub (corresponding to master and slave management modules), open a static workspace by doing the following:

- Use **Operations -> Search -> String** or **Search -> By Criteria** (depending on the version of NetView for AIX) with a search string corresponding to the hub label from a dynamic workspace that has no active filter (that is, the dynamic workspace opened by default by NetView for AIX at startup time),
- Use **Operations -> Create -> Selected** or **Create -> Static Workspace** (depending on the version of NetView for AIX) to create a static workspace with all the hub's agents traps (slave(s) and master).

  The new events generated by these agents will not be dynamically displayed.

Starting nvela

The **nvela** facility is also called the Event History Application. You start it by selecting **Monitor -> Events -> Event History** from the menu bar of the IBM Hubs Topology.

This application displays all events which have been logged in the **/usr/OV/log/ovevent.log**. To display these events, select a filter criterion (optional) and then select **Query -> Display Events**.

Event History

All events are systematically logged into the NetView for AIX event log file **/usr/OV/log/ovevent_log** unless the size of this file is set to zero by selecting **Operations -> Set Log Size** from the **Event History** menu. The default size of the event history log is 128KB (user-defined up to a maximum of 2MB).

To access the event log file, select **Monitor -> Events -> Event History**.

Note: The default size of dynamic and static workspaces is 500 events. Both sizes are customizable in the **/usr/OV/app-defaults** directory by setting values in the **Nevla** and the **Nvevents** files. When this size is exceeded, the first events are overwritten and a warning is displayed.

The 8250, 8260, and 8265 Device Manager component of Nways Manager-LAN detects and reports all the faults taking place in the various hub networks. All related events are logged in the NetView for AIX event log and dynamic workspaces for further analysis. You can save these logs into different files using static workspaces or the Event History application.

As this function is based on the NetView for AIX log facility, you can use the following parameters:

- Search (by Filter or Criteria):
  - String
  - Filter
    - Time
    - Trap type
    - Enterprise
    - Severity
    - Hostname
  - Severity
    - Cleared
    - Intermediate
    - Warning
    - Minor
    - Critical
    - Major
  - Category
    - Threshold
    - Network Topology
    - Error
    - Status
    - Node configuration
    - Application alert
    - Log Only (will be logged into the event log file, event history, but will not appear in dynamic workspace).
  - Event Source
    - Agent
    - NetView/6000 daemons

You can also associate specific actions to the different hub events and traps using the NetView for AIX event configuration. To do so, select **Options -> Event Configuration -> Trap Customization: SNMP**.

- Mail - For these specific events, an email is sent to a predefined user.
- Beep - Generates an audible beep until the operator stops it (based on NetView for AIX **ovxbeep**).
- Ack - You must acknowledge the event (a pop-up window based on NetView for AIX **ovxecho**) or even use the built-in pop-up facility in NetView for AIX.
- User action with a shell script.

For details about Beep and Mail, see the Optional Command and Argument Format section of the NetView for AIX online help for **Options -> Event Configuration -> Trap Customization: SNMP** or the relevant sections in the *NetView for AIX User's Guide* for **ovxbeep** and **ovxecho**.

Ordering capability is also provided, based on the following criteria:

- Time
- Hostname
- Trap Type
- Enterprise
- Severity

Note: A sample filter definition for filtering *all* traps generated by an 8250 or 8260 hub is provided in the **/usr/OV/filters/iub.filters** file.

Working With Hub Events

The conventions described in Table 24 are used to identify slots, subslots, ports, trunks, threshold identifiers, and power supplies. All the traps formatted by Nways Manager-LAN use these conventions. When you perform a search, you can use these conventions as search criteria. Also, you can use the hub label when you search for a specific hub.

Table 24. Identifying Resources

S	Slot Level
s	Subslot Level
p	Port Level
t	Trunk Level
T	Threshold Identifier
P	Power Supply
crm	Critical Resource Monitoring

When working with hub-specific events, you may need to take different actions depending on which resource level you are working at and whether you are using IBM SystemView NetView/6000 V2 or IBM NetView for AIX V4 or V5.

Using NetView for AIX V4 or V5

Selecting Traps for Hubs

Select one or more hubs in the IBM Hubs Topology or open a Hub Level view. Filtering is based on the hub label(s) of the selected hub(s) when you select **HubManager -> Fault** from a hub's context menu or **Hub -> Fault** from the menu bar of the Hub Level view.

This means that one or more dynamic workspaces are opened for the hub label(s). Master and slave traps are shown in these workspaces as they come from the same hub label.

Creating Dynamic Workspaces

Dynamic workspaces are automatically opened with the filtering criteria that correspond to the selected resource. This can be:

- At hub level - All traps that come from the master and slave agents in the hub.
- At module level - All traps that come from the selected slot, its ports, and its trunks in the hub.
- At port level - All traps that come from a selected port in the hub.
- Power supplies and trunks are treated in the same way as ports.

Thresholds and subslots can be used as search criteria.

To create a dynamic workspace with automatic filtering for a resource (hub, module, port, trunk, or power supply), press MB3 on the resource icon and select **Fault** from the context menu.

To create a dynamic workspace with hub-level filtering for a resource, select **Hub -> Fault**.

For example, to start the filtering for a module, select **Fault** from the context menu displayed when you click MB3 on the module icon. Filtering is performed according to the hub label(s) and the slot number. A dynamic workspace is opened where all the traps matching the hub label and slot number are displayed.

Dynamic workspaces display the list of events received for the selected resources and dynamically update the display when new traps are received from the agent.

Note: Events in the *Log Only* category do not appear in a dynamic workspace but are still logged in the **trapd.log** file.

Creating Static Workspaces using NetView for AIX V4 or V5

To use a dynamic workspace as input to create a static workspace, select **Search ->By Criteria** and enter a criterion for the search. Then click on the **Create Workspace** radio button to create a new workspace for the **Search Results** field.

Note: Using this facility, all search criteria described in Table 24 on page 154 can also be done under NetView for AIX V4 or V5. However, it is easier to directly select a resource and create a dynamic workspace with filtering if you select **Fault** from the context menu of the resource.

Customizing Traps and Events

Nways Manager-LAN lets you customize the actions that are performed when traps are received from a hub. This includes specifying what action to take on a per-trap basis. The generic and specific traps are shown in Table 25.

Table 25. Generic and Specific Traps

Generic	Specific	Description	Program Action
0	0	coldStart	Normal Polling
1	0	warmStart	not applicable
2	0	linkDown	Polling
3	0	linkUp	Polling
4	0	authenticationFailure	not applicable
5	0	egpNeighborLoss	not applicable
6	1	Hello	Polling
6	2	Slot Down	Polling
6	3	Slot Up	Polling
6	4	Environment	Update memory
6	5	Hardware	Polling
6	6	Software	not applicable
6	7	Change	Update memory
6	8	Fatal	Polling
6	9	Trunk Down	Update memory
6	10	Trunk Up	Update memory
6	11	Port Down	Update memory
6	12	Port Up	Update memory
6	13	Ping	Forward to panel
6	14	aboveThreshold	Update memory
6	15	belowThreshold	Update memory
6	16	SubModuleDown	Polling
6	17	SubModuleUp	Polling
6	18	Security	Update memory
6	19	Bridge Port Down	Update memory
6	20	Bridge Port Up	Update memory
6	21	Bridge Port Mau Down	Update memory
6	22	Bridge Port Mau Up	Update memory

Table 25. Generic and Specific Traps (continued)

Generic	Specific	Description	Program Action
6	25	ChipOutOfInterfaces	not applicable
6	26	ChipFDDISMTPeer WrapCondition	not applicable
6	27	ChipFDDIMacFrame ErrorCondition	not applicable
6	28	ChipFddiMacFrameError ConditionCleared	not applicable
6	29	ChipFddiMACDuplicate AddressCondition	not applicable
6	30	ChipFddiMACNotCopied Condition	not applicable
6	31	ChipFddiMACNotCopied ConditionCleared	not applicable
6	32	ChipFddiMACNeighbor ChangeEvent	not applicable
6	33	ChipFDDIPortLer Condition	not applicable
6	34	ChipFddiPORTEBError Condition	not applicable
6	35	ChipFddiPORTUndesirable ConnectionEvent	not applicable
6	36	ChipInvalidConfiguration	
6	37	ChipDuplicateLESAddress	not applicable
6	38	ChipFDDITraceStatus	not applicable
6	39	ChipAtmIlmiFailure	not applicable
6	23	Port of SubModuleDown	Update memory
6	24	Port of SubModuleUp	Update memory
6	40	Critical Resource Failed	not applicable
6	41	Critical Resource Recovered	not applicable

Note: In order for the traps 6.40 and 6.41 to be generated each time a critical resource fails or recovers from failure, you must first enable trap generation by using SMIT. To do so, follow these steps:

1. Start from the Root submap or the IBM Hubs Topology.
2. From the menu bar, select **Administer -> Campus Manager SMIT**.
3. From the SMIT menu, select **Configure -> Configure HUB Manager capability -> Change the resource monitoring configuration**.
4. In the `Trap generated when critical resource fails or recovers` field, change the parameter to **Generated**.

For more information, see “Handling Traps for Critical Resources” on page 86.

When no Distributed Management Module (DMM) is installed in an 8260 hub, hub resources can still be managed from Nways Manager-LAN if an ATM Switch (A-CPSW) module Version 2.3 or higher is installed. This is because the A-CPSW module (Version 2.3 or higher) contains a subset of the DMM MIB. In this case, the A-CPSW module acts as the master Management module in the hub and reports the traps shown in Table 26.

Table 26. Generic and Specific Traps when A-CPSW Module Acts as Master Agent

Generic	Specific	Description	Program Action
6	102	Slot Down	Polling
6	103	Slot Up	Polling
6	104	Environment	Update memory
6	107	Change	Update memory

Table 26. Generic and Specific Traps when A-CPSW Module Acts as Master Agent (continued)

Generic	Specific	Description	Program Action
6	116	SubModuleDown	Polling
6	117	SubModuleUp	Polling

Customizing Traps and Events Using NetView for AIX V4 or V5

When you use Nways Manager-LAN with NetView for AIX V4 or V5, you can customize how you want traps to be handled and automate the action to be taken when they are received. This section summarizes the information on how to customize traps. For full details, refer to the *NetView for AIX User's Guide* and online help.

The following procedure is an example of how you may customize traps and events using NetView for AIX V4 or V5:

1. Select the trap you want to customize (for example, 6.8). From NetView for AIX, select **Options -> Event Configuration -> Trap Customization: SNMP**. This displays the Event Configuration panel.
2. Select the enterprise name *hmp6000*. This corresponds to the enterprise ID 1.3.6.1.4.1.2.6.40. 8250 and 8260 agent traps, received by the NetView for AIX **trapd** daemon and only logged, are formatted with the Enterprise ID 1.3.6.1.4.1.49 and should not be changed.

   Using these traps, Nways Manager-LAN reformats them with Enterprise ID 1.3.6.1.4.1.2.6.40 with default actions and meaningful textual information. You can customize these traps by specifying an Enterprise Name and ID, such as hmp6000 1.3.6.1.4.1.2.6.40. The generic and specific traps shown in Table 25 on page 156 are displayed in the panel. The following information is displayed:

   - Event Name
   - Event Identification
   - Severity
   - Status
   - Source
3. To customize a specific type of trap regardless of its source:
   a. Select the trap to be customized
   b. Click on the **Modify** pushbutton. The Modify Event dialog box is displayed. From the dialog box, you can:
      - Modify the event description.
      - Modify the severity of the event.
      - Add a pop-up window with text that will be displayed when the trap is received.
      - Add an automatic action to be done when the trap is received. For example, to add the trap description to a file called **/usr/OV/log/trapd.log.hublabel** (where **hublabel** is the label assigned to the hub), you would enter:

```
echo "trap from hub $1: content $2" >>
/usr/OV/log/trapd.log.$1
```

c. Click on the **OK** pushbutton. Then click on the **Apply** pushbutton to apply the change shown in the Event Configuration dialog box.

4. To customize a specific action if the trap is received from one or more pre-defined hubs, use the event source facility:
   a. Select the trap to be customized.
   b. Click on the **Copy** pushbutton. The **Copy Event** dialog box is displayed. From the dialog box, you can:
      - Modify the event name according to the criteria you will choose.
      - Modify the event description accordingly.
      - Add the IP Addresses, the host names, or the pathname either by typing in the field or selecting one or more hubs in the IBM Hubs Topology and clicking on the **Add from Submap** pushbutton. In this example, the IP address 9.100.108.80 is used.

        Note: Check that there is not an existing modified event that matches the IP Address you are adding.
      - Add a pop-up window.
      - Add a command. For example, enter the command that you want to be activated each time a trap with the specified number (6.8 in this example) is received. For example:

        ```
        echo "received from hub $1, from its agent
        IP address $A:$2 >>/usr/OV/log/hubs.log"
        ```

        where $1 and $2 are the label of the hub and the textual description of the trap respectively, and $A is the host name or IP address of the agent that sent the trap.
   c. Click on the **OK** pushbutton. A new line is created with the Sources field as you defined it.
   d. Click on the **Apply** pushbutton in the Event Configuration dialog box to refine it.

The next trap received with the specified number **and coming from one of the sources you selected in the map** will do the specified action. In this example, the file **hubs.log** will be filled with the message:

```
Received from hub PITUFO, from its agent IP address 9.100.108.80:
TRMM fatal error
```

Multiple EUIs with NetView for AIX V4 or V5

The flag **nvevents.executeCommands** in the **/usr/OV/app-defaults/Nvevents** file allows you to configure whether a command will be executed once by the **ovactiond** daemon or by **nvevents** in each end user interface (EUI) opened.

When this resource is set to *True*, your command is executed by a daemon in its own environment. This avoids setting some environment variables. For example, **ovxbeep**

and **ovxecho** will not run because the DISPLAY variable is not set. Also, your command will be run *only once* because only one daemon runs at a time. This feature can be useful for recovery actions that need to be done once only.

When this resource is set to *False* and **ovactiond** is not registered (refer to the *NetView for AIX User's Guide*), your command will be executed for all windows running the NetView for AIX end user interface. This feature can be useful for messages sent, using **ovxbeep** and **ovxecho**, to all NetView for AIX operators.

You can change the default behavior of **ovxbeep** by customizing **/usr/OV/app-defaults/XNm**. Also, you can customize **ovxbeep** and other defaults, in your HOME directory in the **.Xdefaults** file so that you have a personal environment.

Filtering Traps

When NetView for AIX is first started, the event application in the control desk has no filtering by default.

Customizing Filters

You can customize the standard NetView for AIX event application so that it receives only hub-related events by activating a special Nways Manager-LAN filter, Receive_from_8250_8260_Hubs, in the **/usr/OV/filters/iub.filters** file.

To select a filter and modify it:

1. IP addresses can filter the IP addresses that you want to see, or those that you do not want to see:
   - You can filter on the IP address by using your preferred editor in the **/usr/OV/filters** directory and adding the keywords for the IP address to the file. For example:

     ```
     (...) && (IP_ADDR=9.67.4.8) && (IP_ADDR=9.67.4.1)
     ```

     where IP_ADDR is the IP address of the agent in the hub.

     You can also receive all except the one specified by using the NOT operator. For example:

     ```
     && ! (IP.ADDR=9.100.50.40)
     ```
   - You can achieve the same result by using the user interface to create compound filters:
     – Select the hubs in the NetView for AIX view submaps (multiple selection).
     – Select **Tools -> Filter Editor**.
     – Select file **/usr/OV/filters/iub.filters** by using the **File List...** pushbutton.
     – Click on the **Add Simple...** pushbutton.
     – Select **From Objects Equal to List** in the Add Simple Filter Editor window and click on the **Add From Map** pushbutton.

- Choose a new name for the created filter (for example, *myhubs*).
- Click on the **OK** pushbutton. A new filter rule is created.
- Click on the **Add Compound** pushbutton to create a new rule that consists of two existing rules.
- Click on the **Get Filter** pushbutton.
- Select the **Receive_from_8250_8260_Hubs** rule.
- Click on the **AND** pushbutton.
- Click on the **Get Filter** pushbutton.
- Select another rule, for example, myhubs
- Click on the **OK** pushbutton.
- Rename the new compound and click on the **OK** pushbutton.

When activated, this filter displays all the traps that come from the selected hubs.

2. Time range and threshold - Displays only specific events during a specific period of time. See the *NetView for AIX User's Guide* for more details.

Using Filters to Retrieve Logged Hub-Related Events

The Receive_from_8250_8260_Hubs filter can be used on the Event Log to display events that have already been received from an 8250 or 8260 hub, as follows:

- Start the **Events History** application.
- Select **Operations -> Filter Control** or **Options -> Filter Control** depending on your version of NetView for AIX.
- Select file **/usr/OV/filters/iub.filters** using the **File List** pushbutton.
- Select **Receive_from_8250_8260_Hubs**. or a customized version
- Click on **Activate**.
- Click on **Query -> Display Events**.

Only events reported from an 8250 or 8260 hub are displayed.

Using Filters to Display Only Hub-Related Events

The Receive_from_8250_8260_Hubs filter can be used directly on the event display application to display events when they arrive as follows:

- Start the **Event Display** application.
- Select **Operations -> Filter Log Control** or **Options -> Filter Log Control** depending on your version of NetView for AIX.
- Select file **/usr/OV/filters/iub.filters** using the **File List** pushbutton.
- Select **Receive_from_8250_8260_Hubs** or a customized version.
- Click on **Activate**.
- Click on **Close**.

Only events reported from an 8250 or 8260 hub and which correspond to your filter will be displayed in the Event Display application.

Part 4. Troubleshooting

Chapter 17. 8250 and 8260 Hub Directories

This chapter describes Nways Manager-LAN directories that contain information used by 8250, 8260, and 8265 Device Manager. Some of the directories contain files with configuration information that you can modify; other directories contain information on 8250 and 8260 hubs that is useful for troubleshooting problems in hub management.

- **/usr/lpp/X11/lib/X11/app-defaults** - Definitions for application resources. These defaults can be modified.
- **/usr/CML/app-defaults** - Definitions for application default resources. **Do not modify these files**. If you want to modify application resource definitions, modify the files in **/usr/lpp/X11/lib/X11/app-defaults**.
- **/usr/CML/bin** - Processes and daemons used by Nways Manager-LAN.
- **/usr/CML/sockets** - Sockets used for communication.
- **/usr/CML/specs** - Contains the 8250 and 8260 MIBs used by 8250, 8260, and 8265 Device Manager, the other MIBs used, the supported versions of 8250 and 8260 agents, and the configuration files for the statistics application. **Do not modify these files**.
- **/usr/CML/specs/hdwmst** - Contains the description files for all supported 8250 and 8260 modules. **Do not modify these files**.
- **/usr/CML/specs/eui** - Contains the configuration files for the display of all supported hubs, modules, and other hub resources. **Do not modify these files**.
- **/usr/CML/gif** - Contains the GIF images for the display of all supported hubs, modules, and other hub resources; also contains the bitmaps for drag and drop icons. **Do not modify these files**.
- **/usr/CML/specs/pdf** - Contains files used by the graphical user interface to display panels. **Do not modify these files**.
- **/usr/CML/data** - Contains the default polling configuration file and data files for the Search function, critical resource monitoring, and user-saved information.
- **/usr/CML/conf** - Contains the registration files of 8250, 8260, and 8265 Device Manager daemons.
- **/usr/CML/fields/C** - Contains the 8250, 8260, and 8265 Device Manager field definitions that have been added to the NetView for AIX database.
- **/usr/CML/registration/C** - Contains the registration files for the 8250, 8260, and 8265 Device Manager menus that have been added to the NetView for AIX user interface.
- **/usr/CML/help/C/CML** - Contains the 8250, 8260, and 8265 Device Manager help files.
- **/usr/lpp/hmp6000** - Contains the files used in 8250, 8260, and 8265 Device Manager installation.
- **/usr/ebt** - Contains the DynaText browser and the collection of online books in the *Nways Nways Manager-LAN for AIX User's Guide*.
- **/usr/CML/samples** - Contains sample shell scripts.
- **/usr/CML/deinstall_log** - Contains the log files used in 8250, 8260, and 8265 Device Manager de-installation.

- **/usr/CML/install_log** - Contains the log files used in 8250, 8260, and 8265 Device Manager installation.
- **/usr/CML/migration** - Contains the files used for 8250, 8260, and 8265 Device Manager migration. **Do not modify these files**.
- **/usr/CML/misc** - Contains files with the supported versions of 8250 and 8260 agents and the files to append to the oid_to_sym file from NetView for AIX. **Do not modify these files**.
- **/usr/CML/nls** - Contains the nls catalog and nls files.
- **/usr/CML/bitmaps/C** - Contains the bitmap files for symbols in submaps.

Chapter 18. Processes and Daemons

Generic Processes and Daemons

nvot_server

The **nvot_server** daemon maintains the Nways Manager-LAN topology database.

cmld

The **cmld** daemon is common to both Nways Manager-LAN and Nways Manager-ATM. In Nways Manager-LAN, the **cmld** daemon makes the link between Nways Manager-LAN and the NetView for AIX background daemons. The **cmld** daemon is automatically started and stopped when the NetView for AIX daemons are started and stopped.

To start the **cmld** daemon, do one of the following:

- Enter the command `/usr/OV/bin/ovstart cmld`
- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Start cmld daemon**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Control -> Start cmld daemon**.

To stop the **cmld** daemon, do one of the following:

- Enter the command `/usr/OV/bin/ovstop cmld`
- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Stop cmld daemon**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Control -> Stop cmld daemon**.

To check the status of the **cmld** daemon, do one of the following:

- Enter the command `/usr/OV/bin/ovstatus cmld`
- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Diagnose -> Display Nways Campus Manager general status**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Diagnose -> Display Nways Campus Manager general status**.

cmldiscd

The **cmldiscd** process is common to Nways Manager-LAN and Nways Manager-ATM, and is the basic topology discovery mechanism. It provides the daemons with the LAN resources discovered by NetView for AIX. **cmldiscd** is started and stopped when **cmld** is started and stopped.

To start the **cmldisd** process, do one of the following:

- Enter the command `/usr/CML/bin/cmlstart cmldiscd`
- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Start a daemon controlled by cmld**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Control -> Start a daemon controlled by cmld**.

To stop the **cmldisd** process, do one of the following:

- Enter the command `/usr/CML/bin/cmlstop cmldiscd`
- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Start a daemon controlled by cmld**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Control -> Start a daemon controlled by cmld**.

iubd

The **iubd** daemon is the LAN topology discovery and maintenance daemon. It is automatically started and stopped by the **cmld** daemon.

To start the **iubd** daemon, do one of the following:

- Enter the command `/usr/CML/bin/cmlstart iubd`
- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Start a daemon controlled by cmld**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Control -> Start a daemon controlled by cmld**.

To stop the **iubd** daemon, do one of the following:

- Enter the command `/usr/CML/bin/cmlstop iubd`
- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Stop a daemon controlled by cmld**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Control -> Stop a daemon controlled by cmld**.

iubeui

The **iubeui** process is the process for displaying the Nways Manager-LAN user interface. **iubeui** is not automatically started when the NetView for AIX user interface is started; **iubeui** is, however, automatically stopped when NetView for AIX is stopped.

iubeui is automatically started when you double-click on a hub icon in the IBM Hubs Topology.

cmlsm

The **cmlsm** process is common to Nways Manager-LAN and Nways Manager-ATM and is the daemon that runs 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. When **cmlsm** starts, the copyright panels of Nways Manager-LAN and Nways Manager-ATM (if installed) are displayed.

iubsearchx

The **iubsearchx** process is common to Nways Manager-LAN and Nways Manager-ATM and is the process that provides the user interface with a repository of stations and devices found and managed by Nways Manager-LAN and Nways Manager-ATM. **iubsearchx** is automatically started and stopped when the NetView for AIX user interface is started and stopped.

nwsstatif/iubstat

The **nwstatif** and **iubstat** processes are common to Nways Manager-LAN and Nways Manager-ATM. They control the user interface of the Statistics application that provides graphical information on all counters and values of resources managed by Nways Manager-LAN and Nways Manager-ATM. They are automatically started and stopped when the NetView for AIX user interface is started and stopped.

To erase the statistical information displayed in the Statistics panel, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Statistics -> Remove Statistics files**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Statistics -> Remove Statistics files**.

Start and Stop Process

Important: If for any reason you need to stop NetView for AIX daemons, IBM strongly recommends that you enter the **/usr/CML/bin/cmlovstop** command instead of **ovstop**. The **cmlovstop** command stops NetView for AIX and Nways Manager-LAN daemons in a safe way so that the NetView for AIX topology database maintains consistent data in all network views.

If you have problems starting a daemon, refer to “Generic Processes and Daemons” on page 167.

Nways Manager-LAN is 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, then the **ovw** command. The **netnmrc** shell script starts all the daemons registered in the **ovsuf** file. Each entry in the **ovsuf** file 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 the daemons registered in the **ovsuf** file. Before you start Nways Manager-LAN, 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 must be a root user to start it.

- To check the status of the **cmld** daemon, enter the**ovstatus** command or use SMIT.
- To start and stop the **cmld** daemon, use the **ovstart** and **ovstop** commands or follow the procedures described in “cmld” on page 167.

To have the **cmld** daemon automatically start when you enter the **ovstart** command, add the daemon to the NetView for AIX **ovsuf** startup file.

- To add **cmld** to the **ovsuf** file, do one of the following:
  - From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Configure -> Nways Campus Manager general configuration -> Add cmld daemon to the ovsuf startup file**.
  - From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Add cmld daemon to the ovsuf startup file**.
- To delete **cmld** from the **ovsuf** file if you do not want to automatically start the **cmld** daemon, do one of the following:
  - From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Configure -> Nways Campus Manager general configuration -> Delete cmld daemon to the ovsuf startup file**.
  - From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Delete cmld daemon to the ovsuf startup file**.

The **cmld** daemon automatically starts the **cmldiscd** and **iubd** daemons. To check the status of these daemons, use the **cmlstatus** command.

The user interface of Nways Manager-LAN (configuration and fault panels, statistic displays, and so on) are started by clicking on NetView for AIX icons and by selecting menu items either in the menu bar or through context menus at object level. All the Nways Manager-LAN panels in the user interface are controlled by the **iubeui** process. The statistics graphing interface is controlled by the **nwsstatif** and **iubstat** processes. The Search function is controlled by the **iubsearchx** process. Because these processes are standalone, no information is provided through the **ovstatus** command.

Note: If the **nvot_server** daemon stops, ensure that the **/var** directory is not more than 70% full.

Chapter 19. Automatic Handling of Management Module Changes

When managing 8260 Hubs, you may sometimes perform management tasks that result in a loss of connection between the target hub and the management station. When this happens, 8250, 8260, and 8265 Device Manager uses a mechanism to automatically recover from the SNMP errors.

In order to work properly, the recovery mechanism requires you to configure your hubs and management station in a certain way. The required configurations are described in the next section, “Required Configurations for Automatic Recovery”.

Required Configurations for Automatic Recovery

The following prerequisites are required for automatic recovery and change handling:

- 8250 Management modules must be connected to the management station on each of the possible network assignments. This applies for master and slave Management modules.
- 8260 Management modules must have at least two network monitor cards configured so that the connectivity between the DMM and the management station is reliable.
- For the management station:
  - All Management modules (master and slave) must be discovered by NetView for AIX and must be present in the object database.
  - The NetView for AIX SNMP configuration must be able to detect changes in the IP configuration of Management modules and report these changes in the object database. For more details refer to the *NetView for AIX User’s Guide*.

Understanding the SNMP Recovery Process

In all cases, the panels involving the faulty Management module are invalidated prior to starting the recovery. On these panels, only the Close and Help pushbuttons are available. If a panel is open, a pop-up window displays the result of the SNMP recovery. When you click on the **OK** pushbutton all invalidated panels are revalidated.

Messages describing each SNMP recovery step are logged in the NetView for AIX log, **/usr/OV/log/nettl.LOG00**. To display the contents of this log, enter the command:

```
/usr/OV/bin/netfmt -f nettl.LOG00
```

If connection with the master agent is lost, the lost hub connection icon is displayed in the Hub Level view and the hub status changes to **red**.

A hub poll is started by the SNMP recovery process and is performed for all hubs regardless of what status (`managed` or `unmanaged`) and polling policy they have been configured with under NetView for AIX.

Recoverable Situations

Recoverable situations include:

- Mastership reelection
- Network assignment change
- Lost connection with the master agent.

Mastership reelection

Explanation: Occurs when a No Such Name SNMP error occurs on the hub master agent. You have requested the hub configuration from a slave agent that no longer implements the MIB variables.

System Action: All agents in the hub are requested to report their master status.

Network assignment change

Explanation: A Time-Out SNMP error has occurred on a hub agent. You are either trying to communicate with an agent that no longer uses the same IP address or that has been removed from the hub, or you are using an incorrect community name.

System Action: When the error occurs on a master agent, each master agent interface in the hub is tried. If this is unsuccessful, all agents in the hub are requested to report their master status.

When the error occurs on a slave agent, a hub poll is started.

Lost connection with the master agent

Explanation: Following a mastership reelection or a network assignment change, the connection with the master agent may be lost. If there is still connectivity with another agent in the same hub, recovery from the lost connection may be initiated.

System Action: Check that the prerequisites are met (see “Recovery of Lost Connection with Master”) and initiate the recovery according to the user customization of this function.

Recovery of Lost Connection with Master

After losing connection with the master agent, hub management capability can be recovered by means of the SNMP recovery mechanism, Lost-Connection-with-Master. The lost connection may be due to a network reassignment or a mastership reelection. If the loss of connection persists due to a network problem, the Lost-Connection-with-Master mechanism tries to recover the situation.

Prerequisites

The prerequisites for the Lost-Connection-with-Master SNMP recovery mechanism are as follows:

- There must be more than one Management module in the hub.
- Connectivity between the management station and the Management modules must be set up so that if a loss of connection occurs between one Management module and the management station, it is still possible to reach another Management module.
- No Management modules can be configured with the highest mastership priority (10). This value must be reserved.
- Community names should be configured so that the management station has write access to all Management modules.

Basic Principles

The Lost-Connection-with-Master SNMP recovery takes place after a traditional SNMP recovery failure in Lost-Connection-with-Master-Agent. It relies on the capability of the Management modules to set their own mastership priority and to trigger a mastership reelection for the hub, even if they are slaves.

The basic algorithm is as follows:

1. Check whether the prerequisites are met. If not, no recovery can be started and a Warning message is displayed.
2. Elect a slave agent candidate to become the new master.

   The candidate agent is chosen based on its current mastership priority. The agent with the highest priority is chosen. This simple algorithm allows priorities for back-up Master Management modules to be specified by specifying accurate mastership priorities to its Management modules.
3. Set the mastership priority to the highest value.
   a. If the change in mastership priority is successful, connectivity is established with the agent. Then trigger a mastership reelection through the agent.
   b. If the pdu is acknowledged by the agent, after waiting a few seconds to let the hardware complete its reelection process, trigger a traditional SNMP recovery.
   c. If the recovery is successful, the chosen agent is the new master.
   d. Set the new master agent mastership priority back to its original value, even if step c) was not successful.
4. If step 3) or b) have failed, repeat step 1) with the next eligible slave agent.

Note: If step b) failed, it is probably due to a severe hardware problem or system error which is not recoverable.

Configuration Parameters at Application Level using SMIT

Configuration Parameters at Application Level

To recover a lost connection with a Master agent, you use SMIT to configure certain application parameters. To configure these parameters, follow these steps:

1. Open the Root window or the IBM Hubs Topology.
2. From the menu bar, select **Administer -> Campus Manager SMIT -> Configure -> CML Hub Manager capability configuration -> Change the SNMP recovery configuration**.

In the panel that is displayed, configure the following parameters:

- Automation Level - `LOW` or `HIGH`. Default: `LOW`.
  - `LOW` - When a Lost-Connection-with-Master-Agent is detected, a message is displayed to explain the problem. You are prompted to start an automatic recovery. If you confirm (`YES`) or enter no response, the default action (`RECOVER`) is used and a recovery is triggered.
  - `HIGH` - The recovery is started automatically.

In both cases, messages are displayed to inform you of the recovery result.

- Default Action - RECOVER or NORECOVER. Default: NORECOVER.

  If you do not respond to the message in the pop-up window before the confirmation time expires, the application uses the default value.

  – RECOVER - Automatic recovery is triggered.
  – NORECOVER - No action.

  This parameter is ignored in HIGH automation level configuration.
- User Decision Time - A number of minutes. Default: 3 minutes.

  This value corresponds in LOW automation level mode to the time that the application waits for user confirmation.
- Next Polling Delay Factor - A number to be multiplied by the currently configured polling interval to determine when the next polling will be performed.

SNMP Recovery Pop-Up Messages

The general format of all pop-up messages is:

Pop-up Identifier
Result of the recovery
The SNMP error that was detected
Optionally, additional information

Pop-Up Identifier

The pop-up identifier consists of:

- Hub Label
- Master agent IP address at the time of the failure.

Result of the Recovery

The result of the recovery may be any one of the recovery messages described in “Recovery Messages” on page 175.

SNMP Error Detected

The SNMP error that was originally detected consists of four parts:

- First part:
  – No Such Name
  – Time Out
  – System Error
  – Other Error
- Second part:

  - during polling of the
  - following a user request to the
- Third part:
  - master
  - slave
- Fourth part:
  - agent nnn.nnn.nnn.nnn

Additional Information

The additional information included at the end of the pop-up message is related to the recovery of the lost connection with the master agent (see “Optional Information” on page 177).

Recovery Messages

Master agent changed: old master agent IP address nnn.nnn.nnn.nnn new master: nnn.nnn.nnn.nnn hub polling started.

Explanation: A No Such Name SNMP error has been detected on the master agent, or on a slave agent during polling. The new master agent has been found.

System Action: A hub poll is started.

Connectivity reestablished after a time out. New master agent IP address used: nnn.nnn.nnn.nnn Old IP address used: nnn.nnn.nnn.nnn hub polling started.

Explanation: A Time-Out SNMP error has been detected at the master agent, but a new IP address has been found. The master agent was probably assigned to a new network, but its IP address was up to date in the NetView for AIX database.

System Action: A hub poll is started.

Connectivity reestablished after a time out. Same master agent IP address nnn.nnn.nnn.nnn used.

Explanation: A Time-Out SNMP error was detected at the master agent, but connectivity was reestablished with the same IP address. This generally occurs when trying to write with an incorrect community name.

User Response: Check your SNMP configuration on both the agent side and the network management station side.

Probable configuration change: hub polling started.

Explanation: This message occurs in two situations:

- A No Such Name SNMP error has been detected from a panel on the master agent and the master is still master; for example, you have requested an action on a module that was removed and the 8250, 8260, and 8265 Device Manager was not aware of this change.
- A Time-Out SNMP error has been detected from a panel on a slave agent. You have requested an action involving a slave agent that is not reachable (for example, it is isolated), that has been assigned to a new network, or that has been removed. 8250, 8260, and 8265 Device Manager was not aware of this change.

System Action: A hub poll is started.

Lost connection with master agent due to system error: next polling in n minutes.

Explanation: A No Such Name SNMP error has been detected on the master agent, or on a slave during polling. Due to a system error, the master status of the agents in the hub was not retrieved.

System Action: A hub poll will start in n minutes, where n is the polling interval multiplied by 5.

User Response: This error could also be due to a problem with the SNMP NetView for AIX API, for example. Check the log to find the system error.

Non-recoverable loss of connection during the polling of the last agent known as master.

Explanation: A Time-Out SNMP error has been detected on the last agent known as master. This occurs if you poll a hub after a mastership reelection that was not successfully handled by 8250, 8260, and 8265 Device Manager. All agents are slaves, so 8250, 8260, and 8265 Device Manager polls the last agent known as master.

System Action: None

User Response: If you wish to force a mastership reelection in order to let a slave agent become master, request a manual hub poll and follow the instructions given for the Lost-Connection-with-Master recovery.

Attempt to retrieve a MIB variable unknown by the agent: next polling in n minutes.

Explanation: A No Such Name SNMP error has been detected on the master agent during polling, and the master is still master.

The agent's version is not fully supported by 8250, 8260, and 8265 Device Manager.

System Action: A hub poll is started in n minutes, where n is the polling interval multiplied by 5.

User Response: Use SMIT to change the default version for this agent to the lowest value supported.

Probable mismatch between the agent version and the MIB variable requested.

Explanation: A No Such Name SNMP error has been detected from a panel on a slave agent.

The agent's version is not fully supported by 8250, 8260, and 8265 Device Manager.

System Action: None.

User Response: Use SMIT to change the default version for this agent to the lowest value supported.

Mastership reelection in progress: SNMP recovery stopped. You might want to perform a manual request hub poll in a few seconds.

Explanation: A No Such Name SNMP error has been detected on the master agent (or on a slave during polling) and the agents are electing.

System Action: SNMP recovery is stopped.

User Response: Perform a manually requested poll in a few seconds.

Probable configuration change. Polling in progress. Please try again.

Explanation: An SNMP error has been detected from a panel.

System Action: A poll is taking place.

Probable configuration change. Recovery already in progress. Please try again.

Explanation: An SNMP error has been detected from a panel.

System Action: Recovery is already in progress for that hub for another IP address.

Agent IP address nnn.nnn.nnn.nnn is no longer accurate.

Explanation: An SNMP error has been detected from a panel involving an agent that is no longer in the hub.

System Action: None.

User Response: Close the panel.

Lost connection with master agent due to a non-recoverable SNMP error.

Explanation: SNMP recovery has been started for an error that is not No Such Name or Time-Out. A system error occurred during the polling.

System Action: None.

User Response: Check the log to find the error.

Last known master agent became slave and the connection was lost with the new master. The lost connection with master agent recovery forced agent nnn.nnn.nnn.nnn master again.

System Action: None.

User Response: None.

The connection with the master agent was lost. The following agents are candidates to become master: Type Priority IP address xMM x nnn.nnn.nnn.nnn xMM x nnn.nnn.nnn.nnn Do you want Hub Manager to attempt to force a mastership reelection?

Explanation: SNMP recovery has been started for an error that is not No Such Name or Time-Out. A system error occurred during the polling.

System Action: None

User Response: Check the log to find the error.

Lost connection with master agent or cannot find master agent in the hub: next polling in n minutes.

Explanation: A No Such Name SNMP error has been detected on the master agent (or on a slave during polling) and all agents are slaves. The lost connection with master SNMP recovery was not triggered. This arises if a new Management module has been plugged into the hub and is now master, but 8250, 8260, and 8265 Device Manager was not aware of this change.

This message could also be due to an SNMP error (such as a Time-Out) where the master status of the agents in the hub could not be retrieved.

System Action: A hub poll is started in n minutes, where n is the polling interval multiplied by 5.

Optional Information

The following optional information may appear at the end of the pop-up message.

The lost connection with master agent recovery can not be attempted because no slave agent was responding.

Explanation: The slave agents do not respond to SNMP requests.

System Action: None.

User Response: Check the connectivity between the management station and the agents and the customization of the community names.

The lost connection with master agent recovery can not be attempted because it was already attempted.

Explanation: The recovery of lost connection with master was attempted but did not succeed in letting one slave agent become the new master and so recovery is stopped.

System Action: None.

User Response: Check mastership priorities for this hub. The old master probably has a priority of ten.

The lost connection with master recovery was initiated but failed due to system error.

Explanation: The recovery of lost connection with master was attempted but did not succeed.

System Action: None.

User Response: None.

The lost connection with master recovery was not initiated

Explanation: The recovery of lost connection with master was not attempted either because the user has answered NO to the pop-up or the default action was NORECOVER.

System Action: None.

User Response: None.

The lost connection with master recovery was initiated but failed.

Explanation: The recovery of lost connection with master was attempted but failed.

System Action: None.

User Response: None.

Chapter 20. Troubleshooting

This chapter describes the problems that can occur associated with the management of 8250 and 8260 hubs and the steps to take to resolve each problem.

Problems Associated With NetView for AIX and the IP Internet Submap

Pink Hub Icons Appear Without a Shape Around Them

NetView Version 4 Release 1 PTF #U443133 introduces a bug in the **netmon** daemon that impacts Nways Manager-LAN in the following ways:

- In the IP Internet submap, the icon of the hub with the master agent is pink.
- In the IBM Hubs Topology, the shape around the hub to indicate that the hub is executable is not displayed. This means that you cannot open the Hub Level view by double-clicking on the hub icon. To display the Hub Level view, you must select the icon and then select **HubManager -> Open View**.

PTF #U447036 for NetView Version 4 Release 1 Server will fix this problem.

Fatal IP Submap Errors

If you receive the NetView for AIX error message, `Fatal IP Map Error`, this means that a severe problem has occurred and that some hub objects may be corrupted in **ovw**.

To recover the situation for a given hub object:

1. Remove the hub from IBM Hubs Topology using SMIT cml6000.
2. Delete the agent from all submaps using NetView for AIX.
3. Delete all other hub agents in the same hub from all submaps using NetView for AIX
4. Allow the deleted agents be rediscovered by NetView for AIX.

Slow Response Time For Discovering Network Devices

Nways Manager-LAN uses resolver subroutines to resolve host names into network addresses. When you perform network address translation, make sure that the file **/etc/resolv.conf** exists.

If the file exists, the resolve subroutines assume that the local network has an operational nameserver. If the nameserver in /etc/resolv.conf is invalid or not operational, the response time of NetView for AIX for discovering network devices and performing operations on network nodes is delayed.

Therefore, if you use a nameserver in your local network, make sure that the nameserver is functional. If you do not use a nameserver, the resolve subroutines use the file **/etc/hosts** for network address resolution.

Network Device Icons Are Not Automatically Updated From Database

When NetView for AIX discovers a network device and associates a symbol (icon) to it, the symbol type is not dynamically updated when the device's characteristics change.

In order to have the icons of network devices reflect the current status of the objects in the Nways Manager-LAN database, delete the devices from all submaps and allow them to be rediscovered.

Hub Agents With Incorrect Community Names

When a hub agent with an incorrect community name is first discovered by NetView for AIX, the hub icon of the agent is displayed with a box around it. If you then set the correct community name by selecting **Options -> SNMP Configuration** from the NetView for AIX menu bar and perform a Demand poll, the correct hub icon is displayed, but the hub is not executable.

To restore executable behavior for the hub icon, delete the hub from all submaps and allow the hub agent to be rediscovered.

Co-Existence with Bay Networks Optivity LAN 7.1

When using Bay Networks Optivity LAN 7.1, you may find that the IBM Hubs Topology or LNM Topology icons are not displayed in the NetView for AIX Root submap.

To resolve this problem, make sure that the current value of the AIX environment variable LIBPATH (LIBPATH=*pathname1*:*pathname2*: *pathname3*) does not contain the **/usr/lnms/lib** directory as its first pathname (*pathname1*).

To check the current LIBPATH setting, enter the command:

```
echo $LIBPATH
```

Problems Associated With the IBM Hubs Topology

A Hub Icon Is Not Displayed

When an 8250 or 8260 hub is not discovered by polling and does not appear in the IBM Hubs Topology, follow these steps to resolve the problem:

1. Check that the agent is in the NetView for AIX IP Internet Map.

   Select **Locate -> Objects** to find the agent in the NetView for AIX IP Internet Map. If you cannot locate the agent, this means that the agent has not yet been discovered by NetView for AIX.

2. Check IP connectivity with the agent:

   If the agent is in the NetView for AIX IP Internet Map, select it and then select **Test -> Ping**.

If the agent is not in the NetView for AIX IP Internet Map, use the Ping command from an AIX command window. If you have IP connectivity with the agent, check your NetView for AIX configuration (discovery switch enabled, seed file, and unmanaged networks) until **netmon** discovers the agent.

3. Check that you have SNMP communication with the agent.

   Select the agent in the NetView for AIX IP Internet Map and then select **Test -> Demand Poll**.

4. Check that the agent is a master agent:

   a. Select the agent in the NetView for AIX IP Internet Map.

   b. Select **Tools -> MIB Browser**.

   c. Request under the iso.dod.internet.private.enterprises.chipcom branch .mib02.products.hub.agents.agentsMySlot.

   d. Then request .mib02.products.hub.agents ·.agentsTable.agentsEntry.agentsMasterStatus.

      This table is indexed by slot enabling you to check the master status of the slot you retrieved in step c.

5. Check the Agent Filter file to make sure that the agent for the hub has not been excluded. Refer to the online book **Coupling and Autodiscovery** for more information.

6. Check the agent's fields in the NetView for AIX object database.

   Use the **/usr/OV/bin/ovobjprint** command and check that you have all the fields corresponding to a hub added to the NetView for AIX Generic Topology Database and discovered by Nways Manager-LAN (see **/usr/OV/fields/C/iub.fields** for a list of fields).

7. Check the log to find errors.

   Use the **/usr/OV/bin/netfmt** command to find the error messages logged by Nways Manager-LAN.

If everything has checked out successfully, stop and then restart **ovw**. Then from the IBM Hubs Topology, select **Options -> Unmanage** and then **Options -> Manage**.

8260 Hubs Concurrently Managed by ATM Control Point and DMM

Incorrect Icon Displayed for 8260 Hubs Managed by ATM Control Point and Switch

When an 8260 hub contains both a DMM and an ATM Control Point and Switch (A-CPSW) module, the DMM is always the master agent. If you remove the DMM, the A-CPSW module automatically becomes master. In the IP Internet submap, the DMM hub icon changes to red to indicate that the hub cannot be pinged. In the IBM Hubs Topology, the hub icon should change to indicate that the A-CPSW module is now the master management module in the hub. The icon for an 8260 hub managed by an A-CPSW module is shown in the online book **User Interface**.

If the hub icon in the IBM Hubs Topology does not change or if the shape around the hub icon disappears to indicate that it is no longer executable, follow these steps to resolve the problem:

1. Delete the hub symbol from all submaps by selecting the hub and then selecting either **Edit -> Delete Object -> From All Submaps** from the menu bar or **Edit -> Delete -> Object -> From All Submaps** from the context menu.
2. Rediscover the hub.

This allows the new hub icon to be displayed.

Hub Icon Not Displayed After Inserting DMM

If you remove and reinsert the DMM in the hub, the DMM may not be discovered in the IBM Hubs Topology, even though a new hub icon is displayed in the IP Internet submap in NetView for AIX.

If the hub is being regularly polled, the hub icon changes to red in the IBM Hubs Topology to indicate that it is still managed by the A-CPSW module. In order for the hub's new status to be correctly displayed, follow these steps:

1. From the menu bar, select **Administer -> Campus Manager SMIT**.
2. From SMIT, select **Control -> Find SNMP agent**.
3. Enter the IP address of the DMM and select **OK**.

The hub icon is added to the IBM Hubs Topology. The red hub icon disappears when the hub is next polled (or at the next polling of the hub that was seen as managed by the A-CPSW module).

Hub Icons Are Blue

When you start the Nways Manager-LAN, hub icons are blue (unknown) until the first poll is performed. As soon as the polling is finished, the color of the icon is updated to reflect the compound status of the hub.

If the message `The iubd process is not running` is displayed, enter the command:

```
cmlstart iubd
```

PSM-Managed Device Icons Are Blue

If the icons for PSM-managed Devices appear blue in the IP Internet submap and IBM Hubs Topology, follow these steps to restore the correct color-coded status:

1. Select the icon.
2. Choose **Options ->Unmanage** and then **Options ->Manage** from the menu bar.

Problems with Executable Symbols

Double-clicking on Symbol Icons

If an Error message is displayed when you double-click on the icon of an agent in the IP Internet window, the 8250, 8260, and 8265 Device Manager component of Nways Manager-LAN has been de-installed. In this case, you cannot execute an action on agent symbols in the IP Internet submap.

To restore executable behavior for a symbol, select its icon in the IP Internet submap and choose **Modify/Describe -> Symbol**.

Symbol Representing an Agent is not Executable

This can be caused by the following:

- SNMP communication was not possible at the time the agent was discovered by NetView for AIX.

  After SNMP communication has been reestablished, do one of the following:

  – Delete and then recreate the agent.

  – Stop and then restart **ovw**. Then select a hub and click on any hub menu item.

  – You stopped **iubd** while **ovw** was running, thereby stopping **iubeui**. A new agent was then discovered by NetView for AIX and its corresponding symbols added to the IP Internet Map, but Symbol Manager has not set them to executable.

    Restart **iubd**. Then restart **iubeui** by clicking on any hub menu item.

  – The agent is an 8260 ATM Switch. To see the information added by Nways Manager-ATM to the interface map for this object, select **HubManager -> Open View** from the menu bar.

For more information on the Symbols Manager, the Nways Manager-LAN process that manages executable devices, see the online book **User Interface**.

Problems Accessing and Working In a Hub Level View

Cannot Open Hub Level View

After restarting **iubd**, a red hub icon is displayed in the IBM Hubs Topology. When you double-click on the icon, an error message is displayed.

This may occur for the reasons shown in Table 27.

Table 27. Cannot Open View for Explode Hub -- Reasons and Actions

Possible Reason	Corrective Action
First polling is running.	Wait a few seconds and retry.

Table 27. Cannot Open View for Explode Hub -- Reasons and Actions (continued)

Possible Reason	Corrective Action
First polling in error.	Check the NetView for AIX log for Nways Manager-LAN messages. Ensure that preparation of Management modules has been done as specified in “Chapter 19. Automatic Handling of Management Module Changes” on page 171.
The hub is currently in the NetView for AIX unmanaged state.	Check that this is the desired state for that hub. If it is not, use the NetView for AIX Manage function to declare this hub as managed. Then try to double-click on the hub.
iubd has been stopped and then restarted. During this time, a Master Management module which was master before the stop, became a slave.	Check whether the old master agent is seen as a slave in the newly discovered hubs. If this is the case, use the NetView for AIX functions to delete the red hub icon from all submaps.

Cannot Open Hub View: Agent Not in a Known Hub

This error message occurs when the agent cannot be found in any hub managed by Nways Manager-LAN.

To resolve this problem, follow these steps:

1. In the Root submap, select the IBM Hubs Topology icon.
2. Select **Options -> Unmanage Objects**.
3. Select **Options -> Manage Objects**. This forces a polling of all the hubs managed by the Nways Manager-LAN.
4. Double-click on the agent again.
5. If you receive the same message, the Master Management module that manages this hub has not yet been discovered by NetView for AIX. Follow the procedure in “A Hub Icon Is Not Displayed” on page 180 or refer to the *NetView for AIX User's Guide* for information on discovering hubs.

Cannot Open Hub View: Unable to Know if Hub is Managed

This message means that an error occurred while retrieving the **iubHubIsManaged** field value for the hub. To resolve the problem, follow these steps:

1. Check the event log to find the error.
2. Use SMIT to delete and then recreate the hub.

Cannot Open Hub View: Cannot Retrieve Agent Hostname

This message means that an error occurred while retrieving the agent hostname. To resolve this problem, follow these steps:

1. Find the error in the event log.
2. With the object ID of the agent, use the **/opt/OV/bin/ovobjprint** command to check the object in the database.
3. Delete and then recreate the agent.

Cannot Open Hub View: Cannot Find IP Address Corresponding to Agent Hostname

This message means that an error occurred while retrieving the IP address corresponding to the agent hostname. To resolve this problem, follow these steps:

1. Check the event log to find the error.
2. Check that your name server is running, or that the agent hostname is defined in your **/etc/hosts** file.

Cannot Open Hub View: Hub with Master Agent Unknown

This message means that an internal error occurred. To resolve this problem, follow these steps:

1. Check the event log to find the error.
2. Stop and then restart **ovw**.

No Shadow Appears Around Management Modules

If no shadow appears around the cons of Master Management modules in a Hub Level view, close and reopen the view. The correct shadow is then displayed.

8260 LAN Modules Are Not Displayed

8260 modules installed in an 8260 hub that is managed by an 8250 Management module (for example, EMM, TRMM, or FMM) are not recognized and are not displayed in the Hub Level view. Only 8250 modules are displayed. The Controller module is always shown in slot 17. Although there can be up to four power supplies installed, only two power supplies can be displayed.

In order to display (and manage) 8260 modules, you must install an 8260 Management module in the hub and configure the module as master.

8260 ATM 155Mbps Modules Are Not Displayed

If 8260 ATM 2-port and 3-port 155Mbps (ATMflex) modules are not displayed in a Hub Level view, check if daughter cards are installed in all the daughter card slots on the module's motherboard. If one or more daughter card slots are empty, check which module is the master agent in the hub. Then do one of the following to resolve the problem:

- If the master agent is a Distributed Management Module (DMM) or an Advanced Distributed Management Module (ADMM), contact your IBM representative to upgrade the DMM or ADMM module to Version V4.14 or higher.
- If the master agent is an ATM Control Point and Switch (A-CPSW) module, contact your IBM representative to upgrade the A-CPSW module to Version V2.5.2 or V3.1.1.
- Install daughter cards in all daughter card slots that are empty.

8271 and 8272 Modules Are Displayed as Master Agent

In a Hub Level view, 8271 and 8272 ATM/LAN Switch modules are sometimes displayed as the master agent (master management module). To resolve the problem and redisplay the correct master management module:

1. Delete the icons of the 8271 or 8272 ATM/LAN Switches from all NetView for AIX submaps by selecting **Edit -> Delete object -> From All Submaps**.
2. Allow Nways Manager-LAN to rediscover the hub.

Another way to resolve the problem is by removing modules from the 8260 hub and re-inserting them in the following order:

1. Insert the Distributed Management Module (DMM).
2. Insert the ATM Control Point and Switch module.
3. Insert the 827x ATM/LAN Switch module(s).
4. Insert the other 8260 modules.

RMON Menu Options Are Greyed Out

If you have installed Nways Remote Monitor if the RMON-related menu items remain greyed out in the Hub Manager user interface (Hub Level views, Module Level views, and so on), run the following command from an AIX window:

```
/usr/CML/bin/cml.8250-60.ksh -setRmonApplicationStatus 1
```

To restore RMON-related menu options, you must then close and reopen all Hub Level views that are currently open.

PSM of MSS Module Does Not Start

You cannot start the PSM in the 8210 Multiprotocol Switched Services (MSS) by selecting **Device Management** from the module's context menu due to a hardware problem in the MSS module. This is a known problem and will be fixed in Version 1.1 of the 8210 MSS microcode.

LAN Modules Are Not Displayed or Are Unrecognized

In Hub Level views of 8260 hubs, you may find that:

- 8250 modules are not displayed.
- 8260 LAN modules are displayed with the Unrecognized Module icon (shown on the Legend panel in the online book **User Interface**).

This occurs when an 8260 hub is managed by an ATM Control Point and Switch (A-CPSW) module at Version 2.3.0 or higher. To manage and display all 8250 and 8260 modules in the hub, install and configure a Distributed Management Module (DMM).

Use the A-CPSW module Version 2.3.0 or higher as the master management module only to manage 8260 ATM modules.

Using Refresh Pushbutton Displays 'No Such Name' Warning

While performing hub management tasks in Nways Manager-LAN panels in Hub Level views, you may find that selecting the **Refresh** pushbutton results in the following warning message instead of updating the information in the panel:

```
SNMP error:
No such name
```

To resolve this problem, check to see if the hub is being managed by an ATM Control Point and Switch (A-CPSW) module. Then follow the steps suggested in one of the following situations:

- If the hub is managed by an A-CPSW module, the Refresh pushbutton is inoperative. The Refresh action is not accepted and the warning message is displayed. A hub polling is automatically performed to recover from the SNMP error. To display the refreshed information gathered from the polling, close and then re-open the panel.
- If the hub is not managed by an A-CPSW module, the hub is unreachable. Re-establish the connection to the hub by following the action suggested in the recovery message that is displayed. For a detailed description of each message, see "Chapter 19. Automatic Handling of Management Module Changes" on page 171.

User Interface Hangs When Modifying Threshold Values

If you repeatedly select the **Modify** pushbutton on the Thresholds panel, the Nways Manager-LAN user interface may hang. If this happens, do one of the following:

- Kill (SIGKILL) the iubeui process. The iubeui process restarts automatically as soon as you perform an action on a hub object from the NetView for AIX user interface.
- Close the NetView for AIX session by selecting **File -> Exit** from the menu bar. Then restart NetView for AIX.

Problems Assigning Ports and Modules to a Network Segment

If, while working in a Hub Level view, you receive an error message when assigning a module, port, or trunk to a network segment, this may be caused by insufficient data paths left on the backplane that are unable to successfully perform the operation.

For 8250 Hubs

Table 28 shows the combinations of the number of segments allowed.

Table 28. Segment Combination Table - 8250 Hubs

Ethernet	Token-Ring	FDDI
3	0	0
2	0	1
2	3	0
1	0	2
1	4	0

Table 28. Segment Combination Table - 8250 Hubs (continued)

Ethernet	Token-Ring	FDDI
1	3	1
0	7	0
0	6	1
0	3	2
0	1	3
0	0	4

For 8260 Hubs

Table 29 shows the combinations of the number of segments allowed.

Table 29. Segment Combination Table - 8260 Hubs

Ethernet	Token-Ring	FDDI
8	10	0
8	8	1
8	6	2
8	3	3
8	0	4

Refer to the *8250 Hub Planning and Site Preparation Guide* and to the *8260 Hub Planning and Site Preparation Guide* for further details and rules about maximizing the available network segments.

Problems Working in a Module Level View

No Station Is Displayed on the Module Level View

If stations in your network do not appear in a Module Level view, this may be due to one of the following causes:

- There is no agent on the segment.
- You do not have read-write access to the corresponding agent.
- The agent on the segment is not of the correct type to monitor this station. For example, an EMM cannot monitor TR MACs.

ATM Port Configuration Cannot Be Changed

If the coupling between Nways Nways Manager-LAN and Nways Nways Manager-ATM is stopped while the Module Level view of an ATM module is open, you cannot change the configuration settings of the ports on the module until you close and reopen the Module Level view.

Color-coded Status of Bridges Is Incorrect

When the 8250, 8260, and 8265 Device Manager and LAN Network Manager components of Nways Manager-LAN are running, the color-coded status of attached bridges in Module Level views may be incorrect.

Problems Working in LAN Submaps

Loss of Customized Symbol Positions

While customizing LAN submaps (as described in the online book **User Interface**), you may find that you lose symbol positions that you have saved. This happens for the following reasons:

- If the Automatic Layout parameter for LAN submaps is set to `On`, NetView for AIX continues to create and position symbols. When customizing LAN submaps, you must set automatic layout to `Off` by selecting **View -> Automatic layout -> For This Submap -> Off For This Submap**.
- If you have set no background graphics before starting to customize a LAN submap, NetView for AIX may adjust the position of each symbol that you move so that the symbol positions are different from what you expected. To be able to position symbols in the exact locations that you want, set background graphics before customizing a submap. To set background graphics, select **Edit -> Select Background Picture**.

Interprocess Communication Errors

If Interprocess Communication (IPC) errors (such as `Sorry I can't find the port number for iubsearch`) are logged and displayed in the NetView for AIX alarm card display, follow these steps:

1. Exit from NetView for AIX by selecting **Close** from the System menu pull-down on the window bar.
2. Restart NetView for AIX.

Performance Problems

Problems Due to Memory Consumption

To minimize CPU use and memory consumption by the iubd process (for example, when Nways Manager-LAN is handling many traps), close the Hub Level view in which the hub sending the traps is displayed.

Problems With Color Allocation

A problem of color allocation may occur if you start the end user interface of Nways Manager-LAN **after** starting color-consumming applications, such as Nways Traffic

Monitor, Nways Switching Modules Manager, and web browsers. The IBM Hubs Topology is not displayed and one of the following messages is displayed in the nv6000.log:

```
Cannot allocate color map for gray78. Using optional color white.
X Error of failed request:
BadAccess (attempt to access private resource denied)
Major opcode of failed request:  88 (X_FreeColors)
Serial number of failed request:  3046
Current serial number in output stream:  3048
```

```
X Error of failed request:
BadValue (integer parameter out of range for operation)
Major opcode of failed request:  91 (X_QueryColors)
Value 0xffff
```

To resolve this problem, open the 8250, 8260, and 8265 Device Manager user interface by double-clicking on the IBM Hub Topology icon in the Root submap **before** you start color-consuming applications.

Problems with the Application Transporter

You may have performance problems when running the Application Transporter (MAT) and Product Specific Modules (PSMs) with large numbers of users. This is due to resource limits in the Application Transporter. For example, you may find that the PSMs perform well when there are *n* network users, but that the PSMs stop working when the *n+1* user accesses the network.

If this problem occurs, follow these steps:

1. Find the number of Application Transporter sockets open when the PSM problem occurs by entering the command:

   ```
   netstat -n | grep lockmgr | wc -l
   ```

2. Display the current resource limit by entering the command:

   ```
   ps -eF "uname pid args" | grep lockmgr
   ```

   In the message displayed, the number following `-u` is the current resource limit.

3. Subtract the number in Step 1 from the number in Step 2. If the result is less than five, increase the resource limit of the Application Transporter.

4. Stop all Application Transporter applications. Use SMIT to stop all Application Transporter daemons by selecting **Communication -> Application -> Transporter -> Control-> Stop Daemons**.

5. Edit the following files and change the line with `lockmgr -u 75` to a number larger than the number received in Step 1 (for example, `lockmgr -u 100`):

   - /usr/lpp/mgtapptran/bin/setup.csh
   - /usr/lpp/mgtapptran/bin/setup.ksh
   - /usr/lpp/mgtapptran/bin/mgtapptrannv
   - /usr/lpp/mgtapptran/bin/mgtapptran.ksh

Then save the files.

6. Verify that you have solved the problem by running the Application Transporter and the PSMs again with the same number of users (*n+1*) that caused the problem.

Problems When Running Multiple NetView Sessions

When starting multiple NetView for AIX sessions on a management station, you may find that you cannot start **more than two** sessions. This limitation is caused by insufficient disk space in the file system **/usr/CML/OStore/cache** used to start Nways Manager-LAN daemons and processes.

You can resolve this problem by increasing the size of the file system used for the ObjectStore cache. You must increase the cache size by 5.5 MB for each additional NetView session that you want to run. To do so, follow these steps:

1. Start SMIT and select **System Storage Management (Physical & Logical Storage) -> File Systems -> ADD/Change/Show/Delete File Systems -> Journaled File Systems -> Change/Show Characteristics of a Journaled File System**
2. In the File System Name dialog box, select **/usr/CML/OStore/cache**.
3. Enter a value in the **SIZE of file system** field for the amount of 512-byte blocks that you want to increase the file system. Then click on **OK**.

   Note that you must enter **11,000** (11,000 x 512 bytes = 5.5 MB) for each additional NetView session that you want to run.

Slow Response Time Of NetView Graphical Interface

If you find that the response time of the NetView graphical interface is much slower than usual (for example, a long delay between mouse click and interface response), the **nvot_server** daemon is receiving repeated requests from the **iubmap** process. This happens when a large amount of system resources is required to resynchronize hub and LAN network views.

To solve the problem, you must decrease the initial synchronization priority set for the **iubmap** process. To do so, follow these steps:

1. From the NetView menu bar, select **File -> Describe Map**.
2. In the Map Description window, select the **IBM Nways Campus Manager:Iubmap** map and click on **Configure For This Map**.
3. In the iubmap Configuration window, reset the initial synchronizing priority to a lower priority by following these guidelines:

0	Unset
0	Normal
10	Low priority
20	Very low priority

The new value you set is valid only for the initial synchronization of the iubmap process. After initial synchronization, the priority is automatically reset to the default value **0** (Normal).

Problems Downloading Microcode to DMM Modules

If you find that the result of a software download to a master DMM module does not appear in the Download panel, this may be because there are other (slave) DMM modules in the hub. During the download operation, the microcode is downloaded to the master DMM, but the master DMM is reset and becomes *slave*. The slave DMM module becomes master. The download results displayed in the panel are then the results of the last microcode download performed to the slave DMM that is now master.

To reset the DMM module that is now slave to *master*, choose **Hub -> Control -> Reset Mastership**.

Problems with Statistics

Starting Hub Resource Statistics

If you have a problem when starting statistics for 8250 and 8260 hub resources, display the setting of the TZ (Time Zone) AIX environment variable and unset the TZ variable. (Change the TZ variable's setting to `unset TZ`).

Starting RMON Statistics

When you start RMON statistics, the following message may be displayed:

```
The MIB variable setting failed for 8260 TR1 RMON Error Report View
```

Ignore this error message if you are running the statistics for an 8260 hub with a TMAC agent that receives data from a Token-Ring network that has all RMON groups enabled.

Displaying Token-Ring Statistics from a Hub Level View

When you start Nways Manager-LAN statistics to graph the bandwidth of a Token-Ring segment by clicking on one of the Token-Ring network icons in a Hub Level view, note that the ring speed used to compute the bandwidth is **16 Mbps**.

Printing Statistics

To avoid printer problems when printing Nways Manager-LAN statistics, you are recommended to use a color printer.

Using Traps

Unknown Hub: Unable to Decode Trap

This message means that the agent has sent a trap that is not supported by Nways Manager-LAN. This occurs when you have an agent version that is newer than the one supported by Nways Manager-LAN.

Unable to Decode Trap Content

This message means that the variables sent with the trap are not in the private MIB, or that an error occurred while decoding the variables. To resolve this problem, check the **/var/opt/OV/log/trapd.log** file to find the corresponding agent's trap, and check the log to find the error.

Incorrect Trap Content Received

This message means that the number of variables sent with the trap does not correspond to what is expected by Nways Manager-LAN. To resolve this problem, check that your agent's version is fully supported by Nways Manager-LAN.

Note: If the value `unknown hub` is displayed instead of the hub's name, Nways Manager-LAN has received a trap sent by an agent in a hub that is not managed by Nways Manager-LAN.

Echo Trap

When you perform an echo test, the Echo trap from the Management module is ignored.

To display the result of the echo test, click on **Stop** in the Echo panel.

Problems Closing Copyright and Pop-up Messages

To avoid unexpected results in the NetView for AIX and Nways Manager-LAN user interfaces, always close the Copyright panel and pop-up messages by selecting the **OK** pushbutton.

Inaccurate Information Displayed About Token-Ring Stations

To ensure that accurate information is displayed about stations on monitored 8250 token-ring networks, the following prerequisites must be met:

- Lay out trunk cabling between hubs so that only one lobe is defined over hubs.
- Configure the **Ring-In** trunks of all Token-Ring modules as follows:

- If the trunk is connected to another Token-Ring module in the same hub, set the Network Map state to `INTERNAL`.
- If the trunk is connected to another Token-Ring module in a different hub, set the Network Map state to `EXTERNAL`.

Part 5. LLC Token-Ring Resources

Chapter 21. Applications and Agents

LNM OS/2 Agent Application

LAN Network Manager is a Nways Manager-LAN application that provides network management for your LAN environment. LAN Network Manager represents the topology for the resources in your LANs and provides profile, configuration, fault, and performance information for the resources.

LAN Network Manager manages the different types of networks in your LAN environment with a closely-related set of applications, each tailored to a specific network environment or group of resources. These applications communicate with agent programs located in the various networks and report information, such as topology updates or status changes, to LAN Network Manager. The agents also respond to management instructions from LAN Network Manager through the different applications.

The applications that are used by LAN Network Manager extend management function to the following areas:

- LLC-based token-ring LANs
- SNMP-managed bridges and token-ring LANs
- FDDI networks

The LNM OS/2 Agent application extends network management to environments that consist of LLC-based token-ring LANs that are interconnected by certain bridges managed by LAN Network Manager for OS/2 Version 2.0. Using information provided by the OS/2 agent, LAN Network Manager integrates the LAN hardware managed by LNM for OS/2 Version 2.0 into the views of the SNMP managed environment. Although the LLC-based segments are not merged with SNMP segments in the topology views, the flexibility of the graphical interface enables you to manage LLC-based LAN hardware and SNMP-addressable resources.

The LAN Network Manager program uses the IBM OS/2 agent program as its proxy agent in the LLC-based networks. Under the control of LAN Network Manager, the LNM OS/2 Agent application issues instructions to the OS/2 agent program and updates LAN Network Manager based on solicited and unsolicited responses.

Token-Ring OS/2 Agent

LAN Network Manager manages the different networks and resources in your LAN environment by communicating with agent programs. The agent programs report information, such as topology updates or status changes, to LAN Network Manager and also respond to management instructions from LAN Network Manager.

When you start LAN Network Manager, part of the initialization process is the discovery of all configured agent programs in your network. After the agents have been contacted by LAN Network Manager, they can exchange information with LAN Network Manager

about the segments and resources that they manage. This exchange of information takes place regardless of whether the NetView for AIX graphical interface is currently running; this ensures that the LAN submaps display up-to-date status and topology for the network environments that they represent when the graphical interface is opened.

You can modify the configuration of each agent program by using SMIT. This enables you to control certain operating parameters and optimize the interaction between the agents and LAN Network Manager. For example, to ensure that LAN Network Manager automatically discovers an agent, you can configure that agent to be discovered at startup. See the section “Methods of Discovery” in the online book **Coupling and Autodiscovery** for more information.

The LNM for OS/2 Version 2.0 program operates as the token-ring OS/2 agent for LAN Network Manager and extends its management functions to LAN Network Manager. For example, you can query adapters, add and change bridge definitions, and obtain and display performance data. The OS/2 agent communicates with LAN Network Manager through a set of run commands (RUNCMDS) that are built into the LNM for OS/2 Version 2.0 program. The OS/2 agent also converts event notifications that are generated in the token-ring network to SNMP traps and forwards these traps to LAN Network Manager.

Chapter 22. Configuring Management Parameters for LLC Token-Ring Resources

After installing the LNM OS/2 agent application, you can configure the OS/2 agent (cmol) capability for the network you are managing. To configure the OS/2 agent (cmol) capability to manage your LLC token-ring resources, use SMIT to define values for:

- LAN Network Manager general parameters
- OS/2 agent parameters

This chapter describes how to carry out these tasks.

Using SMIT to Configure LAN Network Management

The configuration parameters that you define in SMIT are saved in files with an extension of .conf in the `/usr/CML/conf/lnmlnmemon` directory. These files are read each time LAN Network Manager is started.

If you change any of these parameters, follow these steps to activate your configuration changes:

1. Stop the background daemons by entering `/usr/OV/bin/ovstop` from an AIX command line.
2. Restart the background daemons by entering `/usr/OV/bin/ovstart`.

If you use SMIT to change other configuration parameters, stop and restart the affected LAN Network Manager daemon to cause the updated parameters to take effect by entering:

```
cmlstop <daemon_short_name>
cmlstart <daemon_short_name>
```

For more information on the daemons used by LAN Network Manager applications, see the online book **Coupling and Autodiscovery**.

Configuring LNM Parameters: Age-out Time, Time-Out Period

To configure or change the LAN Network Manager general parameters:

1. Ensure you are logged on with root privileges.
2. If SMIT is not running, enter **smit cml** from an AIX operating system shell, or select **Administer -> Campus Manager SMIT** from the NetView for AIX menu bar.

   The SMIT menu is displayed.
3. Select **Configure**.
4. Select **IBM LAN general parameters**.

   The dialog box for configuring LAN general parameters is displayed.

5. Enter new values in any of the following fields. To display help information about a parameter, click on **?** and point to the field.

Age-out time	Number of days that an inactive resource remains in the database before it is deleted.
Initial time-out	Number of seconds that a LAN Network Manager application waits before updating its topology displays.
IBM LAN Root label	Window title displayed in the title bar of the LAN Network submap.

6. Press Enter or select **OK** to activate your changes.
7. Select **Exit SMIT** from the Exit pull-down menu to leave the SMIT program.

Configuring OS/2 Agents that Manage LLC Token-Ring Resources

After you have installed the LAN Network Manager component, configure OS/2 agents in your network to communicate with Nways Manager-LAN. Each OS/2 agent program is managed by the OS/2 agent capability and has a configuration file that you can modify using SMIT. With SMIT, you configure the OS/2 agent program by defining the IP address of each agent in your network and specify how you want it to be discovered.

You should also ensure that you have selected the **NetView for AIX connection** field on the NetView Parameters window in the OS/2 agent program. Refer to the OS/2 agent documentation for more information.

To define or reconfigure an OS/2 agent using SMIT, follow these steps:

1. Ensure you are logged on with root privileges.
2. If SMIT is not running, enter **smit cml** from an AIX operating system shell or select **Administer -> Campus Manager SMIT** from the NetView for AIX menu bar.

   The SMIT menu is displayed.
3. Select **Configure**.
4. Select **Configure OS/2 agent (cmol) capability**.
5. Select **Add/Change IBM LNM OS/2 agent**.
6. Enter the IP address of the LNM OS/2 agent and press Enter or select **OK**. A complete Add/Change IBM LNM OS/2 Agent menu is displayed.
7. Enter new values for any of the following LNM OS/2 agent parameters. To display help information about a parameter, click on **?** and point to the field.

   IP address
   Internet Protocol (IP) address of the agent.

   Port number
   Number of the port through which the agent communicates.

   Ensure that the value you enter in the **Port number** field matches the value defined for the port number in the CONFIG.SYS file on the OS/2 agent workstation. This value must not be used by any other application

operating on the OS/2 agent workstation. If you do not enter a value, the default value of `7605` is used. Record each unique port number in the file `/etc/services` as `LNM_OS2_AGENT nnnn/tcp` where `nnnn` is the port number to be recorded.

Automatic agent discovery
If you select **Yes**, the agent is discovered each time Nways Manager-LAN is started. This is known as *persistent discovery*.

If you select **No**, the agent is not automatically discovered. You can, however, manually configure the agent for *temporary discovery*. For information about the difference between persistent and temporary discovery, see the section ″Methods of Discovery″ in the online book **Coupling and Autodiscovery**.

Resync interval
Time period (in days, hours, minutes) used by Nways Manager-LAN to rediscover the agent, resynchronize the segment, and update LAN submaps with new or changed information. Each resynchronziation refreshes LAN submaps with the latest changes made to the network topology (for example, moving, adding, or removing LLC token-ring devices).

Response time-out
Time period (in days, hours, minutes) used by Nways Manager-LAN to wait for a response from the agent before issuing an error message.

Daily resync
Daily time (hour and minute) used by Nways Manager-LAN to rediscover the agent, resynchronize the segment, and update LAN submaps with new or changed information about resources managed by the agent.

8. Press Enter or select **OK** to activate your changes.
9. Repeat steps 4 through 8 for each OS/2 agent in your network.

Chapter 23. Managing LLC Token-Ring Networks

The LAN Network Manager program works with the LNM OS/2 agent and the NetView for AIX program to enable you to monitor and manage your Logical Link Control (LLC) token-ring networks. The OS/2 agent program acts as an agent in the LLC token-ring environment and responds to management requests sent by LAN Network Manager. The OS/2 agent also informs LAN Network Manager of any changes in the LLC token-ring environment. This enables you to manage all of your LLC token-ring resources from the NetView for AIX console.

This chapter describes the LAN Network Manager LNM OS/2 Agent application and the OS/2 agent, and tells you how to define parameters for LAN Network Manager and the OS/2 agent.

Understanding the LNM OS/2 Agent Application

The LNM OS/2 Agent application extends network management to environments that consist of LLC-based token-ring LANs that are interconnected by certain bridges managed by LAN Network Manager for OS/2 Version 2.0. Using information provided by the OS/2 agent, LAN Network Manager integrates the LAN hardware managed by LNM for OS/2 Version 2.0 into the views of the SNMP managed environment. Management of the IBM SNMP-managed 8230 concentrators and multiport bridges is provided by the SNMP Token-Ring and the SNMP Bridge applications, respectively. This management is not provided as part of the LNM OS/2 Agent application.

Although the LLC-based segments are not merged with SNMP segments in the topology views, the flexibility of the graphical interface enables you to manage LLC-based LAN hardware and SNMP-addressable resources.

The LAN Network Manager program uses the IBM OS/2 agent program as its proxy agent in the LLC-based networks. Under the control of LAN Network Manager, the LNM OS/2 Agent application issues instructions to the OS/2 agent program and updates LAN Network Manager based on solicited and unsolicited responses.

The LNM for OS/2 Version 2.0 program operates as the OS/2 agent for LAN Network Manager and extends its management functions to LAN Network Manager. For example, you can query adapters, add and change bridge definitions, and obtain and display performance data. The OS/2 agent communicates with LAN Network Manager through a set of run commands (RUNCMDS) that are built into the LNM for OS/2 Version 2.0 program. The OS/2 agent also converts event notifications that are generated in the token-ring network to SNMP traps and forwards these traps to LAN Network Manager.

Defining Parameters for LLC Token-Ring Networks

After you have installed one or more OS/2 agent programs and used SMIT to define the basic parameters the LAN Network Manager program needs to establish and maintain contact with the OS/2 agent, you can define other parameters that configure OS/2 agent more specifically to the token-ring networks you are managing.

In LLC token-ring networks, you can define two types of parameters using LAN Network Manager:

- Resource-specific parameters
- System-wide parameters

Resource-specific parameters apply to one particular resource. For example, using the **Automatic bridge link** field on the Bridge Configuration window you can specify whether the OS/2 agent automatically attempts to link to a specific bridge.

System-wide parameters apply to all instances of a resource known to an OS/2 agent, or to the operating parameters of a specific OS/2 agent. An example of a system-wide parameter is the **Bridge autolink flag** on the Bridge Parameters window. If you set this parameter to Disabled, the OS/2 agent does not attempt to automatically link bridges, regardless of the setting of the **Automatic bridge link** field for each bridge.

Resource-specific parameters are described in the following chapters according to the type of resource. The system-wide parameters are described in the remainder of this chapter.

As you use LAN Network Manager to define parameters, refer to the description and details information on the management windows for help about each field you are defining and the values that are valid for it.

Displaying LNM OS/2 Agent Configuration Information

The LNM OS/2 Agent Configuration window displays information about the adapter in the agent workstation and about the LAN segment that the agent manages. You can also display and change configuration parameters for all aspects of your token-ring network through the Actions, Lists, or Parameters menus.

To display the LNM OS/2 Agent Configuration window, follow these steps:

1. From the LAN Network submap, select the subnet icon that represents the subnet the OS/2 agent program is managing.
2. Select **Configuration** from the LAN pull-down or context menu.

   The LNM OS/2 Agent Configuration window is displayed.

   In addition to viewing the information about the adapter in the agent workstation and the LAN segment that the agent manages, you can change the value for the LNM for AIX response timeout and set the resynchronziation interval.
3. Select **OK** to save the information and close the window.

When information for a field is not available, for example, when the adapter is closed, that field is blank.

The **Comments** field of the LNM OS/2 Agent Configuration window is blank until you enter information in the field.

Setting the Resynchronization Interval

In the LNM OS/2 Agent Configuration window, you can specify how often LAN Network Manager refreshes its views of the OS/2 agent domain by setting the **resync time** parameters. When LAN Network Manager refreshes its views, it begins the process of rediscovering the OS/2 agent. The LAN Network Manager submaps are updated with the information found in the discovery process and the LAN Network Manager views are refreshed.

Refreshing the LAN Network Manager submaps resets the status of congested adapters to normal. When LAN Network Manager refreshes its views, any adapters that show a marginal status (yellow) are reset to normal status (green) after the submaps are refreshed.

You can set the resynchronization interval in either of the following ways:

- Once a day

  Specify the time (hour and minute) when you want LAN Network Manager submaps to be daily refreshed. This method is useful when you want to schedule the refresh at night in order to avoid overloading the resources used for network management.
- Once at each specified time period (day-hour-minute)

  Specify the period in days, hours, and minutes at which you want LAN Network Manager submaps to be regularly refreshed. This period starts from the time when you manually stop and restart LNM daemons by doing one of the following:
  - Enter the following commands:

    ```
    /usr/CML/bin/cmlstop lnmlnmemon
    /usr/CML/bin/cmlstart lnmlnmemon
    ```
  - From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Stop cmld daemon**. Then restart **cmld** by selecting **Start cmld daemon**.
  - From the menu bar, select **Administer -> Campus Manager SMIT**. From the SMIT menu, select **Control -> Stop cmld daemon**. Then restart **cmld** by selecting **Start cmld daemon**.

  This method is useful when you want to schedule a refresh of LAN Network Manager submaps at regular intervals.

Note that these two methods are mutually exclusive. If you set resynchronization, you must specify either a daily time or an interval of time.

To prevent LAN Network Manager submaps, from being automatically refreshed, set the resynchronization interval to **zero**. If you turn off resynchronization in this way, you can

manually refresh the views by selecting **Refresh LAN Network Manager view** from the Actions pull-down menu on the LNM OS/2 Agent Configuration window. See “Refreshing the LNM for AIX View” on page 209 for more information.

Note: Using SMIT, you can also specify the resynchronization time by selecting **Nways Campus Manager -> Configure -> Configure OS/2 agent (cmol) capability -> Edit IBM LNM for OS/2 configuration file** from the SMIT main menu.

LNM OS/2 Agent Configuration Pull-Down Menus

You can perform additional actions from the LNM OS/2 Agent Configuration window by selecting a menu choice from the Actions, Navigation, or Parameters pull-down menu.

You can select the following choices from the Actions pull-down menu:

For information about:	Read:
Add Definition	“Adding a Station Definition” on page 223 “Adding a Bridge Definition” on page 231 “Adding a Concentrator Definition” on page 245 “Adding a Concentrator Qualifier” on page 246
Delete Definition	“Deleting a Concentrator Qualifier” on page 247
Restart LNM OS/2 Agent	“Restarting the LNM OS/2 Agent” on page 214
Refresh View of LNM OS/2 Agent	“Refreshing the LNM for AIX View” on page 209

To navigate directly to one of the following windows, select a choice from the Lists pull-down menu on the LNM OS/2 Agent Configuration window:

Select:	To navigate to:
Bridges	Bridge List
Concentrators	Concentrator List
Stations	Station List

To perform additional configuration tasks on the selected OS/2 agent, you can choose one of these choices from the Parameters pull-down menu on the LNM OS/2 Agent Configuration window:

For information about:	Read:
Access Control	“Defining Access Control Parameters” on page 209
Adapter Monitoring	“Defining Adapter Monitoring” on page 210
Bridge	“Defining General Bridge Parameters” on page 211
Configuration Monitoring	“Defining Configuration Monitoring Parameters” on page 212
General	“Defining General LNM Parameters” on page 213

For information about:	Read:
Segment	“Defining Segment Parameters” on page 213

Refreshing the LNM for AIX View

To update your LAN Network Manager submaps with current information, select **Refresh LNM for AIX view** from the Actions pull-down menu on the LNM OS/2 Agent Configuration window. When you select **Refresh view of LNM OS/2 Agent**, LAN Network Manager begins the process of discovering the OS/2 agent again. The LAN Network Manager submaps are updated with the information found in the discovery process and the LAN Network Manager views are refreshed. Refreshing the LAN Network Manager view does not cause the OS/2 agent to be resynchronized.

Refreshing the LAN Network Manager submaps resets the status of congested adapters to normal. When you select **Refresh view of LNM OS/2 Agent**, any adapters that show a marginal status (yellow) are reset to normal status (green) after the submaps are refreshed.

To refresh the view of a specific segment only, select **Resync** from the Actions pull-down menu of the Segment Profile window. See “Resynchronizing a Segment” on page 216 for more information.

Defining Access Control Parameters

Parameters that you define on the Access Control Parameters window specify the conditions that cause LAN Network Manager to remove an adapter when it detects an access control violation.

Understanding Access Control

The access control function of LAN Network Manager allows you to detect and remove unauthorized adapters. The asset management function of the Controlled Access Unit captures the location information about adapters and notifies LAN Network Manager when these adapters are moved. To fully implement the access control and asset management functions, all managed adapters need to be connected to concentrators that are registered with this LAN Network Manager program. See “Registering with a Concentrator” on page 243 for more information about registration.

A registered concentrator can disable a port to which an unauthorized adapter is attached. Using the concentrator and the controlling OS/2 agent, you can disable the concentrator port so that the station cannot re-enter the network. LAN Network Manager can command the concentrator to disable a port only if the concentrator is registered to LAN Network Manager.

The authorization of stations that insert in the network is based on information in the agent’s database. A station is not authorized if its address is not in the database. Add the address to the database using the Station Definition window.

When the OS/2 agent determines that an adapter has been inserted on the LAN, it verifies the adapter against its list of defined adapters in the database. If access control is enabled and the OS/2 agent does not find the adapter address in the database, or if the time, day, or concentrator location information recorded in the database for that adapter does not match, the OS/2 agent generates an alert indicating that an access violation has occurred. LAN Network Manager can remove the unauthorized adapter or disable the port on the concentrator.

Attention: Define all bridge adapters and adapters of critical resources before you activate access control. If you do not, LAN Network Manager might remove an adapter that you need. For example, suppose you activate access control, then link to a bridge without first defining the bridge adapters. If the near adapter is on the local segment, it is authorized. However, the far adapter is considered unauthorized. Therefore, the far adapter is removed. If the adapter is removed, the link to the bridge is lost, and LAN Network Manager can no longer manage the remote segment. If neither adapter is on a managed segment, then both adapters are removed.

Displaying the Access Control Parameters Window

To display the Access Control Parameters window, follow these steps:

1. Select **Access Control** from the Parameters pull-down menu on the LNM OS/2 Agent Configuration window.

   The Access Control Parameters window is displayed.
2. Enter information in the fields.
3. Select **OK** to save the information and close the window.

You can perform additional actions from the Access Control Parameters window by selecting a menu choice from the Actions or Navigation pull-down menu.

You can make access control active or inactive by selecting the **Access Control** menu choice from the Actions pull-down menu. When you select **Access Control**, a cascade menu is displayed. Select **Active** to activate access control. Select **Inactive** to disable access control.

Defining Adapter Monitoring

Specify whether to activate adapter monitoring using the Adapter Monitoring Parameters window.

You can monitor any adapter, within the managed domain, that responds to test frames sent to the logical link control (LLC) null service access point (SAP).

When the OS/2 agent program is started or restarted, each adapter that is defined to be monitored is polled. The first time an adapter responds, the LAN Network Manager program logs an event indicating that the adapter is responding. If an adapter does not respond, LAN Network Manager continues to poll the adapter until the number of retries

specified in the Adapter Monitoring Parameters window is reached. If the adapter responds as expected during polling, no action is taken. Otherwise, a trap is generated.

To display the Adapter Monitoring Parameters window, follow these steps:

1. Select **Adapter Monitoring** from the Parameters pull-down menu on the LNM OS/2 Agent Configuration window.

   The Adapter Monitoring Parameters window is displayed.
2. Specify whether you want adapter monitoring to be **Active** or **Inactive**.
3. Select **OK** to save the information and close the window.

Defining General Bridge Parameters

Bridge parameters that control how the agent program communicates and manages bridges can be defined on the Bridge Parameters window. Examples of these parameters are the bridge autolink flag, the autolink timer, and the status of the reporting link.

Determining Reporting Links

Each IBM bridge program that is supported by LAN Network Manager has four reporting links, numbered from 0 through 3. Thus, a single bridge can communicate with up to four OS/2 agents at a time. When you configure the bridge program, you can define a password for each of the reporting links. You can also decide which OS/2 agent program is to be the controlling agent for each bridge. All other OS/2 agent programs communicating with the bridge are observing agents.

The controlling agent is assigned link number 0; the observing agents are assigned link numbers 1 through 3.

A controlling agent can issue any OS/2 agent command for the local LAN segment or a remote LAN segment, including commands that change the way LAN components operate and change the topology of the segment. Only controlling OS/2 agent programs log and transport alerts from application programs, using the alert transport facility.

A network can have more than one controlling OS/2 agent if the controlling agents do not attempt to establish links to the same bridges. For bridges that you define using LAN Network Manager, the default reporting link is used unless you modify the reporting link using run commands or the OS/2 agent user interface.

Passwords

The bridge program uses the password, which you defined for each reporting link, to determine if an OS/2 agent is authorized to establish a reporting link with the bridge. The OS/2 agent sends its password to the bridge with which it is linking. The bridge program compares the reporting link password with the password defined in the bridge

configuration for this reporting link. If the password does not match, the bridge program rejects the link, sends a notification to all of the managing stations linked to the bridge, and generates an alert.

Both the OS/2 agent program and the bridge program require a password for a reporting link. You can use the default password provided. LAN Network Manager does not require that you change this password.

Displaying Bridge Parameters

To display the Bridge Parameters window, follow these steps:

1. Select **Bridge** from the Parameters pull-down menu on the LNM OS/2 Agent Configuration window.

   The Bridge Parameters window is displayed.
2. Enter information in the fields.

   If you change the reporting link in the **Reporting link status** field, the default reporting link for the OS/2 agent program is changed.
3. Select **OK** to save the information and close the window.

Defining Configuration Monitoring Parameters

Specify the configuration monitor age-out interval and the resynchronization time for the OS/2 agent on the Configuration Monitoring Parameters window.

The value you specify for resynchronization determines how often the OS/2 agent resynchronizes the network by querying each adapter or bridge and updating the OS/2 agent database tables with current information. This information enables the OS/2 agent to maintain an accurate network configuration.

The configuration monitor age-out interval is used by the OS/2 agent program when it checks for adapters that are inactive. If an adapter has been inactive for longer than the time specified by the age-out time interval, it is deleted from the OS/2 agent database configuration table.

To display the Configuration Monitoring window, follow these steps:

1. Select **Configuration Monitoring** from the Parameters pull-down menu on the LNM OS/2 Agent Configuration window.

   The Configuration Monitoring Parameters window is displayed.
2. Specify the configuration monitoring age-out interval and how often you want the OS/2 agent to resynchronize its view of the network.
3. Select **OK** to save the information and close the window.

   Note: Ensure that the resync interval is longer than the time required to complete a discovery cycle.

Defining General LNM Parameters

Define and change parameters dealing with remote communication and attachment to the segment on the General Parameters window. These parameters include response timeout, retry interval, and number of retries. You can also specify the tracing policy for the agent and whether the adapter in the agent station attempts to automatically reopen on a beaconing ring.

To display or change the general OS/2 agent parameters, follow these steps:

1. Select **General** from the Parameters pull-down menu on the LNM OS/2 Agent Configuration window.

   The General Parameters window is displayed.
2. Enter information in the fields.

   Specify which adapters are allowed to trace on the network, for the portion of the network that the OS/2 agent controls, in the Trace field. Select the push button in the Trace field to display an option menu of the types of tracing you can authorize.

   The OS/2 agent must be controlling to change tracing authorization parameters.

   Only IBM or compatible Token-Ring Network trace and performance adapters are recognized as trace adapters.
3. Select **OK** to save the information and close the window.

Defining Segment Parameters

Specify the data collection interval and the days and times to collect data from your network on the Segment Parameters window. When you specify a collection interval on the Segment Parameters window and activate collection on the Segment Performance window, LAN Network Manager gathers data related to the performance of your segments and saves this data in history files. If you select **Graph History** from the Segment Performance window, LAN Network Manager displays a graph of the segment performance data it has collected.

For more information about data collection and segment performance, refer to “Displaying Segment Performance” on page 217.

To display the Segment Parameters window, follow these steps:

1. Select **Segment** from the Parameters pull-down menu on the LNM OS/2 Agent Configuration window.

   The Segment Parameters window is displayed.
2. Enter information in the fields.
3. Select **OK** to save the information and close the window.

Restarting the LNM OS/2 Agent

To restart the LNM OS/2 agent, select **Restart LNM OS/2 agent** from the Actions pull-down menu on the LNM OS/2 Agent Configuration window. The Restart LNM OS/2 Agent dialog box is displayed. Select **OK** to restart the LNM OS/2 agent, or select **Cancel** if you do not want to restart the LNM OS/2 agent.

When the OS/2 agent is restarted, the LAN Network Manager view is refreshed. The network resources in the LAN Network Manager view might show a status of unmanaged until the resources are rediscovered.

Chapter 24. Managing LLC Token-Ring Segments

Using its LNM OS/2 Agent application to communicate with the LNM OS/2 agent in the token-ring environment, the LAN Network Manager program monitors activity on the LAN segments to which its agents are attached and on remote LAN segments connected by bridges. This chapter describes how to monitor and manage the segments in your network.

It contains the following topics:

Displaying a LAN Segment Submap

Monitor and manage the individual resources that make up a specific segment on the Segment submap. The Segment submap displays stations, bridges, and concentrators in nearest active upstream neighbor (NAUN) order, according to their adapters. To display a Segment submap, double-click on the icon of the segment.

The Segment submap displays a graphical representation of the stations that are attached to the selected segment, including their statuses. These stations can represent workstation adapters, concentrators, and bridges.

To open a view of the ports of a particular bridge, double-click on the bridge icon.

Open a view of the ports and modules of a particular 8230 concentrator by double-clicking on the concentrator.

The color of a resource indicates the status of that resource. A change in the color of a resource indicates a corresponding change in status. For an explanation of the colors and their corresponding statuses, refer to the online book **User Interface**.

Displaying a Segment Profile

To display information about a segment, use the Segment Profile window. You can also display additional information or perform actions on the segment by using the pull-down menus on the window.

To display the Segment Profile window, select the segment for which you want profile information, then select **Profile** from either the LAN pull-down menu or the context menu.

You can select the following actions from the Actions pull-down menu on the Segment Profile window:

For information about:	Read:
Resync	"Resynchronizing a Segment"

To navigate directly to the following segment windows, select one of the following choices from the Navigation pull-down menu on the Segment Profile window:

Select:	To navigate to:
Fault	Segment Fault window
Performance	Segment Performance window

Resynchronizing a Segment

The resynchronization function maintains an accurate network configuration by querying each adapter, updating the OS/2 agent configuration and location tables with current information, and by refreshing the Segment submap.

To override the interval set in the Resync time field on the Configuration Monitoring Parameters window and to request an immediate resynchronization of the OS/2 agent's configuration table and the location table, follow these steps:

1. Select a segment.
2. Select **Profile** from either the LAN pull-down menu or the context menu.
3. Select **Resync** from the Actions pull-down menu of the Segment Profile window.

   LAN Network Manager displays a message that explains whether the resynchronization was successful.

   If the resynchronization is successful, the Segment submap is refreshed.
4. Select **OK** to close the message dialog box.

Resynchronizing a segment resets the status of congested adapters to normal. When you select **Resync**, any adapters that show a marginal status (yellow) are reset to normal status (green) after the segment is successfully resynchronized.

Displaying Segment Fault Information

The Segment Fault window provides data about segments that are experiencing *soft errors*. Soft errors are intermittent network errors that cause data to be transmitted more than once. Soft errors can have an effect on network performance.

If the segment that you selected is experiencing soft errors, the Segment Fault window displays the adapters that are experiencing the soft errors.

The Segment Fault window contains a list box that displays the first 10 adapters encountered that are experiencing soft errors on that segment at the time of the request. The list box shows the address of the adapter which is experiencing soft errors, the address of its nearest active upstream neighbor (NAUN), and the error count for the affected adapter. One asterisk (*) next to the error count value indicates that an adapter is in a pre-weight-exceeded condition; two asterisks (**) next to the error count value indicate that an adapter is in a weight-exceeded condition.

To display the Segment Fault window, select the segment for which you want fault information, select **Fault** from either the LAN pull-down menu or the context menu.

To navigate directly to the following segment windows, select one of the following choices from the Navigation pull-down menu on the Segment Fault window:

Select:	**To navigate to:**
Profile	Segment Profile window
Performance	Segment Performance window

Displaying Segment Performance

LAN Network Manager can gather and display segment performance data for each LLC token-ring segment in the network. The Segment Performance window enables you to display performance information for the segment and to activate data collection for the selected segment.

You can also display *segment utilization* information for a selected segment on the Segment Performance window. Segment utilization is the percentage of the total data-transmission capacity of the segment that is being used. To display segment utilization information, there must be a station on the segment that is currently managed by an OS/2 agent and has:

- The LAN Station Manager program installed and running
- Either the LAN Adapter and Protocol Support program (for OS/2) or the LAN Support program 1.2, or later, (for DOS) installed and running
- IBM Token-Ring adapters that support the ring utilization parameter. Contact your IBM representative for a list of the adapters that support this parameter.

To display the performance information for a segment, select the segment for which you want to display performance information, then select **Performance** from either the LAN pull-down menu or the context menu.

The data collection fields on the Segment Performance window indicate how often segment performance data is collected, and the time period in which the collection

takes place. Change the values of these fields on the Segment Parameters window. For more information about the Segment Parameters window, see “Defining Segment Parameters” on page 213.

Start or stop the collection of segment performance data by changing the value of the **Collecting** field on the Segment Performance window.

If you want to display the segment performance data graphically, select the **Graph History** push button.

To navigate directly to the following segment windows, select one of the following choices from the Navigation pull-down menu on the Segment Performance window:

Select:	To navigate to:
Profile	Segment Profile window
Fault	Segment Fault window

Exporting Segment Performance Data to Spreadsheet Format

The performance data that is collected by LAN Network Manager is saved to a file.If you want to work with this data in a spreadsheet program, you can convert the `history.01` files to a spreadsheet-readable delimited format using the *lnmexport* utility.

To use the lnmexport utility to export segment performance data, enter the following command from an AIX operating system shell:

```
lnmexport ip_address seg segment_number week_data > output_file
```

where:

IP_address IP address of the OS/2 agent that is collecting data

Segment_number The 3-digit hexadecimal number of the segment

Output_file Name of the file in which you want the converted data placed

Week_data The week from which the data was collected. `01` exports the current week’s data. `02` exports the previous week’s data.

The lnmexport utility converts the segment performance data stored in the `/usr/CML/reports/lnmlnmemon/dir_name` directory, where *dir_name* is a directory named with the IP address of the OS/2 agent. The converted data is placed in the file you specified with the lnmexport command, and stored in the same directory, or a directory you specify with the redirect symbol (>).

The format of the data is:

```
Segment_number 0 Time Utilization
```

where:

Segment_number	Number of the segment in the decimal equivalent of the hexadecimal number. Segment 000 is represented by 4096, all other segments are converted to their hexadecimal equivalent number.
Time	Time the sample was taken in seconds since January 1, 1970.
Utilization	Ring utilization value recorded during the time the sample was taken

The lnmexport utility converts the data to the following spreadsheet delimited format:

```
Segment_number Delta_time Utilization
```

where:

Segment_number	Number of the segment in hexadecimal format. Segment 000 is represented by 4096, all other segments are converted to their hexadecimal equivalent number.
Delta_time	Number of seconds since the last utilization sample.
Utilization	Ring utilization value recorded at that time.

As an example, suppose you want to convert the current week's segment performance information for a segment named 005 so you can work with the information in a spreadsheet program. Segment 005 is managed by an OS/2 agent with an IP address of 9.67.187.11. You want to put the converted information in a file called *seg005.wks*.

You would enter the lnmexport command as follows:

```
lnmexport 9.67.187.11 seg 005 01 > seg005.wks
```

This command converts the data to the following:

```
history data file                 output file (seg005.wks)
⋮
5 0 732040000  15.00               5, 0, 15.00
5 0 732040030  25.00               5, 30, 25.00
5 0 732040060  35.00               5, 30, 35.00
5 0 732040090  45.00               5, 30, 45.00
5 0 732040120  55.00               5, 30, 55.00
```

To transfer the `seg005.wks` file to a DOS or OS/2 diskette, use the following AIX DOSWRITE command:

```
doswrite -a seg005.wks seg005.wks
```

This command transfers the file to a DOS or OS/2 diskette in the diskette drive of your AIX workstation. You can then work with the file using the spreadsheet program.

Chapter 25. Managing LLC Token-Ring Stations

LAN Network Manager enables you to manage the physical aspects of the stations in your network. You can define a variety of devices as stations. This chapter describes how to define and manage stations. It contains the following topics:

Defining a Station

The OS/2 agent discovers the stations in your network even if they have not been defined. However, by defining a station you can:

- Give the station a symbolic name
- Monitor the station
- Specify whether the station's adapter can enter the network as a trace adapter

In addition, by defining the stations in your network you can use the access control function of LAN Network Manager to detect and remove unauthorized adapters from the network. The authorization of stations that insert in the network is based on whether the adapter address is in the OS/2 agent database. One way to enter the adapter address into the database is by defining the station, as described in "Adding a Station Definition" on page 223.

The adapters for a variety of devices can be defined as stations, including:

- IBM PS/2
- IBM RS/6000
- IBM 3174
- IBM 3720, 3725, or 3745 Communications Controller
- IBM 9370 Information System
- IBM System/36
- IBM AS/400
- IBM Series/1
- IBM 8232 LAN Channel Station
- IBM 8220 Optical Fiber Converter
- IBM 8230 Controlled Access Unit
- IBM 3172 Interconnect Controller

You can define stations as critical resources to be monitored by LAN Network Manager, and as authorized trace-adapter addresses.

Adapter Monitoring

You can identify adapters for monitoring by the LAN Network Manager program. Monitor the adapters of devices for which you want to be notified if the adapter is not present or is not responding to the test frame. When determining whether to monitor a station, be aware that each station you monitor increases the network traffic that is processed by both the OS/2 agent and LAN Network Manager. You can monitor any adapter within the managed domain that responds to test frames sent to the logical link control (LLC) null service access point (SAP). However, if a device is likely to be congested or busy, you might receive an unexpected alert if the adapter cannot respond to the test frame.

The default setting for the **Monitor** field on the Add Station Definition window is **No**. If you want to identify an adapter for monitoring, ensure that you have assigned a name to the adapter and set the **Monitor** field to **Yes**.

To activate adapter monitoring for the adapters you have identified to be monitored, set the **Monitor Adapters** field on the Adapter Monitoring Parameters window to **Active**. To open the Adapter Monitoring Parameters window, select **Adapter Monitoring** from the LNM OS/2 Agent Configuration window.

Devices such as file servers and print servers are good candidates for adapter monitoring.

It is usually not necessary to monitor bridge adapters, because the bridge reports to LAN Network Manager if it becomes unlinked. If you do monitor bridges, always monitor the bridge adapter that is closest to LAN Network Manager. The other bridge adapter might not be visible to the monitoring process.

Tracing Authorization

When defining an adapter, you can specify whether the adapter can enter the network as a trace adapter. LAN Network Manager supports the following trace programs:

- The IBM Token-Ring Network Trace and Performance program, which is the supporting trace program for the following adapters:
  - IBM Token-Ring Network Trace and Performance Adapter II
  - IBM Token-Ring Network Trace and Performance Adapter/A
  - Other compatible adapters
- The IBM Token-Ring Network 16/4 Trace and Performance program, which is the supporting trace program for the following adapters:
  - IBM Token-Ring Network 16/4 Trace and Performance Adapter II
  - IBM Token-Ring Network 16/4 Trace and Performance Adapter/A
  - Other compatible adapters

Adapters authorized as trace adapters function only as trace adapters if the trace program is operating on the station that contains the adapter. If the trace program is not operating on the station, the trace adapter functions as a regular token-ring network adapter.

Only a controlling LAN Network Manager program can control adapter tracing for the entire network. You have the following tracing options:

- No adapters are allowed to trace.
- All adapters are allowed to trace.
- Specific adapters are allowed to trace.

Every 8 seconds, a frame-tracing tool notifies the OS/2 agent that it has begun or ended tracing activity or that tracing activity is in progress. The OS/2 agent program takes action according to the notification it receives. If an unauthorized adapter tries to enter a segment as a trace adapter, the OS/2 agent program issues a Remove command to the trace adapter and does so each time the adapter tries to trace. The OS/2 agent program generates an alert to indicate that an unauthorized trace was attempted on the LAN.

If the OS/2 agent program is an observing OS/2 agent, all adapters are allowed to trace. A trap is sent when an adapter traces or ends tracing.

Adding a Station Definition

To add a station definition that will be passed on to the OS/2 agent and stored in the OS/2 agent database, use the Add Station Definition window. In this window you can assign a name to the station and specify whether the adapter is monitored by LAN Network Manager. You can also authorize the adapter as a trace adapter and indicate access control parameters for the station, such as when the adapter is allowed on the segment.

To add a station definition, follow these steps:

1. Select **Add definition** from the Actions pull-down menu in the LNM OS/2 Agent Configuration window.
2. Select **Station** from the Add definition cascade menu.

   The Add Station Definition window is displayed.
3. Enter information in the fields.
4. Select **OK** to add the definition and close the window. If you want to add more than one definition at a time, select **Apply** to add a definition without closing the window.

Displaying a List of Stations

To view a list of stations on the segments in your network, use the List of Stations window. This window displays a list of segments that the OS/2 agent is aware of and the stations on the segments.

You can select a segment from the list of segments to which the OS/2 agent has been linked since it was started or restarted. Selecting the **Display** push button generates a list of the adapters that are connected to the selected segment. The adapters are listed in NAUN order, and the following information for each adapter is displayed:

- The symbolic name of the adapter (if defined)
- The 12-digit hexadecimal address of the adapter
- Whether the adapter is defined to be monitored
- Whether the adapter is authorized to trace

To display a list of the stations on a segment, follow these steps:

1. Select **Stations** from the Lists pull-down menu on the LNM OS/2 Agent Configuration window.
2. Select a segment from the Segments list box.
3. Select the **Display** push button.

You can delete a station definition using the List of Stations window. To delete a station definition, select the station whose definition you want to delete and then select the **Delete** push button.

You can also remove an adapter using the List of Stations window. To remove an adapter, select the adapter you want to remove and then select the **Remove adapter** push button. See “Removing an Adapter” on page 227 for more information about removing an adapter.

Displaying a Station Profile

The Station Profile window displays information about the current operation of the selected station. In addition to identifying the adapter in the station, the window provides general information about the station, such as its LAN segment and neighboring adapters. Asset information displays details specific to the station’s hardware and physical location.

If the station you selected is inactive or an error occurs, the NAUN address and name field is blank, and the agent program retrieves the other data from its database.

To display a station profile, select the station, then select **Profile** from either the LAN pull-down menu or the context menu. The following conditions can exist:

- If the station is on a remote segment, the value for **Universal address** on the Station Profile window is the universal address returned by the bridge. If the station does not return its universal address to the bridge and the bridge is at a level 2.2 or earlier, the bridge could return a duplicate universal address.
- If the selected station is active, the OS/2 agent performs a query of the station’s adapter before displaying the window.

- If the station is inactive or an error occurs, the NAUN address and name field is blank, and the OS/2 agent program retrieves the other data from the configuration table. LAN Network Manager also displays a message box to indicate that the window contains only partial data.

Possible Functional Addresses

The following list shows the possible values for the Functional addresses field in the Station Profile window, follow these steps:

Functional Addresses	Function Name
X'00000001'	Active monitor
X'00000002'	Ring parameter server
X'00000008'	Ring-error monitor
X'00000010'	Configuration-report server
X'00000040'	Discovery locate
X'00000080'	NETBIOS
X'00000100'	Bridge
X'00000800'	LAN gateway
X'00001000'	Ring wiring concentrator
X'00002000'	IBM LAN Manager
X'00020000'	IBM LAN Station Manager
X'40000000'	Remote program update

To navigate directly to Station Configuration window, select **Configuration** from the Navigation pull-down menu on the Station Profile window.

Displaying Configuration Information for a Station

The Station Configuration window allows you to change the configuration of a particular station. You can indicate whether the station is authorized to enter the network as a trace adapter, and the days and times that the station is allowed to access the segment.

To display the Station Configuration window, select the station, then select **Configuration** from either the LAN pull-down menu or the context menu.

To display information about how a station is physically attached to the network, select the **Attachment Data** push button. For more information about the Attachment Data window, read “Accessing Attachment Data” on page 226.

You can remove an adapter by selecting the **Remove adapter** menu choice from the Actions pull-down menu on the Station Configuration window. See “Removing an Adapter” on page 227 for more information.

To navigate directly to the Station Profile window, select **Profile** from the Navigation pull-down menu.

Accessing Attachment Data

If the adapter is attached to the network through a Multi-Access Unit (MAU) or a Controlled Access Unit (concentrator), the Attachment Data window displays specific information about the adapter’s connection. The window provides identifying information such as the wall faceplate label and the port receptacle number to which the adapter is attached.

If the adapter is attached through a concentrator, this window also displays the concentrator’s identifier, the number of the module with which the adapter is associated, and the current registration status of the concentrator.

Additional workstation information, such as the serial number and location, can be displayed if the LAN Station Manager program is installed on the workstation in which the adapter is installed.

To display information about how a station is physically attached to the network, access the Station Configuration window by selecting the station and then selecting **Configuration** from either the LAN pull-down menu or the context menu.

The Station Configuration window is displayed. Select the **Attachment data** push button from the Station Configuration window. The Attachment Data window is displayed.

You can display attachment data only if the station is running the LAN Station Manager program or is attached to a concentrator.

The data displayed on this window comes from the LAN Station Manager MIB if the LAN Station Manager program is installed. If the LAN Station Manager is not installed, the data displayed in this window is incomplete.

You can change information in the window and select **OK** to update the LAN Station Manager MIB.

Removing an Adapter

Attention: Use caution when removing an adapter from the network. Removing a bridge adapter can have an adverse effect on the network. Review the functional address of the adapter to determine if it is a bridge.

You might want to remove an adapter because it is causing excessive errors or because you suspect that the adapter is the cause of slow performance. If the OS/2 agent is a controlling OS/2 agent, you can remove the adapter.

To remove an adapter from the network, follow these steps:

1. Select **Configuration** from either the LAN pull-down menu or the context menu to open the Station Configuration window.
2. Select **Remove adapter** from the Actions pull-down menu of the Station Configuration window.

   A dialog box is displayed to warn you that you are about to remove the adapter.
3. Select **OK** to remove the adapter.

Notes:

1. Removing an adapter requires removal support in the station that is to be removed. For example, the adapters in the concentrator do not support the force remove frame, and, therefore, a remove request will fail.
2. Some software has built-in automatic recovery. If the end station application detects that the adapter has closed, it issues an open adapter command.

Chapter 26. Managing LLC Token-Ring Bridges

To manage remote segments (segments other than the one the OS/2 agent is running on), OS/2 agent has to manage the bridge that links the local segment to the remote segment. This chapter tells you how to define and manage bridges. Using the LAN Network Manager program, you can display information and status for a specific bridge and link and unlink the bridges in your network.

This chapter contains the following topics:

Managing Bridges

Separate adapters in the bridge connect to each LAN segment. The bridge program passes frames from one LAN segment to the other using the two adapters.

When monitoring bridges, always monitor the bridge adapter that is closer to the OS/2 agent program. The other bridge adapter might not be visible to the monitoring process.

For LAN Network Manager to correctly manage adapters on bridged segments, the program must be linked to the bridges that are connected to the bridged segments. You can link bridges either with the **Link** action or automatically by activating automatic linking for the bridge. See "Linking Bridges" on page 237 for more information about linking bridges.

Using Bridges to Manage Remote Segments

To use LAN Network Manager to manage remote segments, enable the following functions in the bridge using the bridge configuration program.

For a token-ring network, enable:

- Ring-error monitor (REM) function
- Configuration-report server (CRS) function

- Ring parameter server (RPS) function

Some bridge programs do not support all the subvectors that are provided by some of the adapters in response to the query adapter function for the OS/2 agent. The query adapter function is used during segment resynchronization and during an adapter query. If a bridge running one of these bridge programs queries an adapter because of a request from the OS/2 agent, and that adapter provides the universal address subvector in response, the bridge returns an error to the OS/2 agent program. Therefore, the query adapter request fails. If the request was a resynchronization request, the segment resynchronization process ends when that adapter is reached and, therefore, the configuration information for that segment is incomplete.

8209 Bridge Support

LAN Network Manager provides limited support for the IBM 8209 Local Area Network Bridge. The 8209 LAN Bridge connects a token-ring segment to an Ethernet or IEEE 802.3 segment, or connects a token-ring segment to another token-ring segment. Using LAN Network Manager, you can link to and remotely configure the bridge and list and update the static entries in the transparent bridging table.

LAN Network Manager supports the following modules:

- Ethernet/IEEE 802.3
- Enhanced Ethernet/IEEE 802.3
- Token-ring module

The following restrictions apply to Ethernet segments linked by the 8209 LAN Bridge to the Ethernet/IEEE 802.3 modules.

- You cannot perform the following functions on an Ethernet segment:
  - Query or remove stations.
  - Display configuration change messages.
  - Perform a segment test.
  - Display segment status details.
- When the 8209 LAN Bridge is used with the Ethernet/IEEE 802.3 module (part number 55F4785), it does not support the ring-error monitor (REM) or configuration-report server (CRS) functions and provides only a portion of the ring parameter server (RPS) functions. Therefore, it cannot act as a reporter even for a Token-Ring Network segment.
- If the 8209 is attached to a Token-Ring Network segment that is attached to the OS/2 agent's local segment through another bridge with report capabilities, the reporting bridge might not be able to reliably report the status of the Token-Ring Network segment.
- If the 8209 is attached to a Token-Ring Network segment that is the OS/2 agent's local segment, the OS/2 agent program cannot log adapter-inserted messages. It can, however, log nearest active upstream neighbor (NAUN) changes.
- If you change some of the parameters for an 8209 bridge, the bridge will reset if it loses the link with the OS/2 agent.

Defining a Bridge

To enable the OS/2 agent to establish communication with bridges, define each bridge to LAN Network Manager, as described in this section. Also, verify that the adapter address in the Bridge Definition window matches the adapter address in the bridge program's bridge configuration.

Before the OS/2 agent can establish communications with a bridge follow these steps:

1. Define the bridge to LAN Network Manager. Verify that the adapter address you specify in the Add Bridge Definition window matches the adapter address in the bridge program's bridge configuration.
2. Specify the reporting link number and the reporting link password that the OS/2 agent is to use to communicate with all defined bridges.

If you change the bridge configuration, do the following:

1. If it was altered as part of the configuration change, change the reporting-link password. See "Determining Reporting Links" on page 211 for more information about reporting links and their passwords.
2. If the bridge number or one or both of the LAN segment numbers was changed as part of the configuration change, relink to verify the changes.

Adding a Bridge Definition

To define a bridge in your network, use the Add Bridge Definition window to enter the addresses of the two bridge adapters and to assign the bridge a symbolic name. You can also specify whether the bridge participates in the automatic bridge linking procedure with the OS/2 agent.

When monitoring bridges, always monitor the bridge adapter that is closer to the OS/2 agent program. The other bridge adapter might not be visible to the monitoring process.

For the OS/2 agent to correctly manage adapters on the remote segments, the program must be linked to the bridges that are connected to the remote segments.

To add a bridge definition, follow these steps:

1. Select **Add definition** from the Actions pull-down menu in the LNM OS/2 Agent Configuration window.
2. Select **Bridge** from the Add definition cascade menu.

   The Add Bridge Definition window is displayed.
3. Enter information in the fields.
4. Select **OK** to add the definition and close the window. If you want to add more than one definition at a time, select **Apply** to add a definition without closing the window.

When you add a definition with the Add Bridge Definition window, the definition information is passed on to the OS/2 agent and stored in the OS/2 agent's database.

Deleting a Bridge Definition

To delete a bridge definition, select **Delete definition** from the Actions pull-down menu on the Bridge Configuration window. Select **OK** from the warning dialog box to delete the definition, or select **Cancel** to cancel the delete operation.

Note: You can delete only bridges that are not currently linked.

Displaying a List of Bridges

To view a list of the bridges that are defined in your network, use the List of Bridges window. This window displays a scrollable list of defined bridges and the following information for each:

- Bridge name
- Bridge status
- LAN segments to which the bridge is attached
- Bridge number
- Whether the bridge is defined for automated linking
- Performance notifications

You can also link, unlink, and delete definitions for bridges using the List of Bridges window.

- To *display* a list of the bridges that are defined in your network, select **Bridges** from the Lists pull-down menu on the LNM OS/2 Agent Configuration window.
- To *link* a bridge using the List of Bridges window, select the bridge and then select the **Link** push button. LAN Network Manager attempts to link the selected bridge. See “Linking Bridges with the Link Action” on page 237 for more information about linking bridges.
- To *unlink* a bridge using the List of Bridges window, select the bridge and then select the **Unlink** push button. LAN Network Manager unlinks the selected bridge. See “Unlinking Bridges” on page 238 for more information about unlinking bridges.
- To *delete* a bridge definition, select the bridge and then select the **Delete** push button.

Displaying Bridge Configuration Information

Display and change basic information for a bridge and the segments that it links using the Bridge Configuration window.

To display the Bridge Configuration window, select the bridge, then select **Configuration** from either the LAN pull-down menu or the context menu.

Perform additional actions from the Bridge Configuration window by selecting a menu choice from the Actions, Navigation, or Parameters pull-down menu.

You can select the following choices from the Actions pull-down menu:

For information about:	Read:
Unlink	“Unlinking Bridges” on page 238
Link	“Linking Bridges with the Link Action” on page 237
Delete definition	“Deleting a Bridge Definition” on page 232

Navigate directly to the following bridge windows by selecting one of these choices from the Navigation pull-down menu on the Bridge Configuration window:

Select:	To navigate to:
Profile	Bridge Profile window
Performance	Bridge Performance window

To perform additional configuration tasks on the selected bridge, choose one of these choices from the Parameters pull-down menu on the Bridge Configuration window:

For information about:	Read:
Reporting link	“Displaying or Changing Reporting Link Parameters”
Forwarding	“Displaying or Changing Forwarding Parameters”
Filter definitions	“Displaying or Changing Filter Definitions” on page 234
SRTB	“Displaying or Changing SRTB Parameters” on page 234

Displaying or Changing Reporting Link Parameters

Each IBM bridge program that is supported by LAN Network Manager has four reporting links, numbered from 0 through 3. Thus, a single bridge can simultaneously communicate with up to four OS/2 agent programs that in turn report to LAN Network Manager. When you configure the bridge program, you can configure a password for each of the reporting links.

Because LAN Network Manager uses only one reporting link number at a time, all bridges for a single reporting link must have the same password if you want LAN Network Manager to link to the bridges.

Only a controlling LAN Network Manager program can change reporting link parameters.

To display or change reporting-link parameters for the selected bridge, select **Reporting Link** from the Parameters pull-down on the Bridge Configuration window.

Displaying or Changing Forwarding Parameters

The Forwarding Parameters window displays information about how the bridge is configured to forward data frames from one segment to another. You can specify parameters, such as bridge priority, which determine the bridge’s operation in the larger network, as well as parameters that apply to specific segments, such as path cost.

To display the Forwarding Parameters window, select **Forwarding** from the Parameters pull-down on the Bridge Configuration window.

Note: In a LAN Subnet submap, if one LLC token-ring bridge is configured as *Frame Forwarding Active* and the other bridge in the segment is configured as *Frame Forwarding Inactive*, both bridges are **green** and the port segment with inactive links is **red**.

Displaying or Changing Filter Definitions

The parameters that control the filter function of a bridge can be displayed and changed on the Filter Definitions Parameters window.

You can define two types of filters:

- Address range filters

  These filters prevent the frames that are originated by specific LAN stations from traversing the bridge. You can filter according to the source address, the destination address, or both. You can also specify the low and high address values of the address range for which you want to filter.
- Criteria range filters

  These filters prevent frames of a particular type from traversing the bridge or allow only a particular type to get through. You can specify the low and high address values of the filtering range.

To display the Filter Definitions Parameters window, select **Filter definitions** from the Parameters pull-down on the Bridge Configuration window.

Displaying or Changing SRTB Parameters

To view or change the Source Routing Transparent Bridging (SRTB) parameters for the bridge, use the SRTB Parameters window.

These parameters apply only to the IBM 8209 LAN Bridge, which enables the connection of a Token-Ring segment with an Ethernet or IEEE 802.3 segment. The 8209 bridge supports both the source-routing method of routing data (used in a token-ring environment) and the transparent-bridging method of routing data (used in an Ethernet or IEEE 802.3 environment). The SRTB parameters affect the way the bridge converts the format of data frames as it passes them from one network environment to another.

To display or change the SRTB parameters, select **SRTB** from the Parameters pull-down on the Bridge Configuration window.

You can also display additional SRTB windows using the following push buttons in the SRTB Parameters window:

Static entries	Displays the Static Entries window. Read “Displaying and Deleting Static Entries” for more information.
Mapped addresses	Displays the Mapped Addresses window. Read “Displaying and Deleting Mapped Addresses” for more information.

Displaying and Deleting Static Entries

Use the Static Entries window to display the predefined address entries in the bridge transparent-bridging table. These entries are retrieved from the bridge and displayed in the list. Each entry consists of the medium access control (MAC) address of a station on the local or remote Ethernet/IEEE 802.3 segment.

Only a message frame with a destination address that is not in this table is passed by the bridge to the Token-Ring segment. If the destination address is in the table, the frame is discarded.

You can also delete static entries on this window.

To display the static entries for a bridge, select **SRTB** from the Parameters pull-down on the Bridge Configuration window. The SRTB Parameters window is displayed.

Select the **Static entries** push button. The Static Entries window is displayed.

To delete one or more static entries, select the entry from the list and then select the **Delete** push button.

You can add a static entry using the **Add** menu choice from the Actions pull-down menu on the Static Entries window. For more information, see Adding Static Entries.

Adding Static Entries

To add a static entry to the bridge’s transparent-bridging table, use the Add Static Entry window. If the bridge receives a data frame with a destination address that matches a static address that you have entered on this window, the bridge discards the frame.

To add a static entry to the list of entries that are defined in the transparent-bridging table, select **Add** from the Actions pull-down menu in the Static Entries window.

Displaying and Deleting Mapped Addresses

Use the Mapped Addresses window to display the list of translated addresses for bridges that connect token-ring and carrier sense multiple access with collision detection (CSMA/CD) segments.

Some types of bridges that connect token-ring and CSMA/CD LAN segments, such as the 8209 LAN Bridge, can maintain, in memory, a database of translated destination addresses for each port. If the destination address of a logical link control (LLC) frame is in the database of the inbound port, the address is changed to the corresponding translated address before the frame is forwarded.

You can also delete mapped addresses from this window.

To display the mapped addresses for a bridge, select **SRTB** from the Parameters pull-down on the Bridge Configuration window. The SRTB Parameters window is displayed.

Select the **Mapped Addresses** push button. The Mapped Addresses window is displayed.

To delete one or more mapped addresses, select the entry from the list and then select the **Delete** push button.

You can add a mapped address using the **Add** menu choice from the Actions pull-down menu on the Mapped Addresses window. For more information, see “Adding Mapped Addresses”.

Adding Mapped Addresses

To add mapped addresses to the list of translated addresses for bridges that connect token-ring and CSMA/CD segments, use the Add Mapped Addresses window. If the bridge receives a data frame with a destination address that you have entered on this window, the bridge changes the address to the corresponding translated address before the frame is forwarded.

Select **Add** from the Actions pull-down menu in the Mapped Addresses window. The Add Mapped Addresses window is displayed.

Displaying a Bridge Profile

The Bridge Profile window displays information about the bridge and its current operation. The window provides general bridge and routing information and describes the bridge adapter connection to a segment.

To display the profile information for a bridge, select the bridge and then select **Profile** from either the LAN pull-down menu or the context menu.

You can select the following actions from the Actions pull-down menu on the Bridge Profile window:

For information about:	Read:
Unlink	“Unlinking Bridges” on page 238
Link	“Linking Bridges with the Link Action”

To navigate directly to the other bridge windows, select one of these choices from the Navigation pull-down menu on the Bridge Profile window:

Select:	To navigate to:
Configuration	Bridge Configuration window
Performance	Bridge Performance window

Linking Bridges

The OS/2 agent links a bridge to manage remote segments connected to the network by the bridge. You can define bridges so that they are automatically linked. See “Linking Bridges Automatically” on page 238 for more information. However, if you have not defined a bridge to link automatically, or if the automatic link option is set to **Disabled**, you can use the link function to link the bridge.

When you use the link function, the bridge checks the reporting link number and password that is sent by the OS/2 agent. The bridge rejects the link attempt if the specified authorization level is in use or if the password does not match the password defined to the bridge program for the specified authorization level.

If you have unlinked a bridge or started LAN Network Manager and then try to link the bridge, the OS/2 agent notifies LAN Network Manager that the link was successful or that the link failed. If the link failed, OS/2 agent returns a reason code for the failure, but additional link requests for that bridge do not result in another trap sent to LAN Network Manager unless the reason for the failure is different from the reason last logged for this bridge.

The performance notification interval for each bridge is set when LAN Network Manager links to the bridge. To change the performance notification interval, see “Displaying or Changing Performance Data” on page 239.

Linking Bridges with the Link Action

To link a bridge which has not been defined to automatically link (described in “Linking Bridges Automatically” on page 238),you can select **Link** from the Actions pull-down menu on either the Bridge Profile or Bridge Configuration windows.

To link a bridge, follow these steps:

1. Select the bridge to which you want to link.
2. Select **Profile** or **Configuration** from either the LAN pull-down menu or the context menu.

The Bridge Profile or Bridge Configuration window is displayed.

3. Select **Link** from the Actions pull-down menu.

   LAN Network Manager displays a message indicating whether the link succeeded or failed.

4. Select **OK** to close the dialog box.

Linking Bridges Automatically

When you define a bridge, you can activate automatic linking for that bridge. If you activate automatic bridge linking, the OS/2 agent tries to automatically link to the bridge when a bridge definition is changed or added and each time the OS/2 agent is started or restarted.

If you activate automatic linking for a bridge, ensure that you have selected **Enabled** in the Bridge autolink flag field on the Bridge Parameters window. If this field is set to **Disabled** in the Bridge Parameters window, automatic bridge linking is turned off for all bridges, regardless of their individual automatic bridge linking status.

If you activate automatic bridge linking for a bridge but the OS/2 agent is not able to link, or if the link is terminated, the OS/2 agent tries to re-establish the link every *n* minutes, where *n* is the **Autolink timer** value defined in the Bridge Parameters window. The OS/2 agent logs a trap the first time the bridge fails to link and again when the link is established.

Read “Defining General Bridge Parameters” on page 211 for more information about changing parameters in the Bridge Parameters window.

Unlinking Bridges

To unlink specific bridges, follow these steps:

1. Select the bridge that you want to unlink.
2. Select **Profile** or **Configuration** from either the LAN pull-down menu or the context menu.

   The Bridge Profile or Bridge Configuration window is displayed.

3. Select **Unlink** from the Actions pull-down menu.

   LAN Network Manager displays a message indicating whether the link was successfully terminated.

4. Select **OK** to close the dialog box.

Displaying or Changing Performance Data

The Bridge Performance window displays performance counter information for the selected bridge. You can also specify threshold levels to control the frequency of data collection and notification. Values for the various performance counters are listed for each segment to which the bridge is attached.

Performance counters accumulate the number of bytes and frames that are forwarded and not forwarded from each LAN segment to the other through the bridge. Frames and bytes forwarded are categorized by type; frames not forwarded are categorized by reason. The bridge program maintains several performance counters for each LAN segment that is connected to a bridge. The bridge program also controls the bridge counters, and LAN Network Manager cannot reset them.

To display the performance information for a bridge, follow these steps:

1. Select the bridge for which you want performance information.
2. Select **Performance** from either the LAN pull-down menu or the context menu.

   The Bridge Performance window is displayed.
3. Enter any changes to the information in the performance counters fields.

   The data collection fields indicate how often bridge performance data is collected, and the time period in which the collection takes place. You can change the values of these fields on the Bridge Parameters window. For more information about the Bridge Parameters window, see “Defining General Bridge Parameters” on page 211.

   To start or stop the collection of bridge performance data, change the value of the **Collecting** field on the Bridge Performance window. To start collecting data, the **Collecting** field must be set to **Enabled**, the **Performance notification interval** field must be set to an interval greater than zero, and the bridge must have a controlling link.
4. If you want to display the bridge performance data graphically, select the **Performance Graphing** push button. See “Displaying Bridge Performance Graphically” for more information.
5. Select **OK** to save the changed information and close the window.

Displaying Bridge Performance Graphically

The Bridge Performance Graphing window enables you to generate a graph of historical bridge data by selecting the types of data you want to graph.

To generate a graph of bridge performance data, follow these steps:

1. Select the **Performance graphing** push button on the Bridge Performance window.

   The Bridge Performance Graphing window is displayed.
2. Select the types of data you want to display in the graph.
3. Select the **Graph history** push button to generate the graph.

Using lnmexport to Export Bridge Data in Spreadsheet Format

The bridge performance data that is collected by LAN Network Manager is saved in a file.If you want to work with this data in a spreadsheet program, you can convert the `history.01` files to a spreadsheet-readable delimited format using the *lnmexport* utility.

To use the lnmexport utility to export bridge performance data, enter the following command from an AIX operating system shell:

```
lnmexport ip_address brg bridge_name week_data > output_file
```

where:

IP_address IP address of the OS/2 agent that is collecting data

Bridge name The symbolic name of the bridge

Output_file Name of the file in which you want the converted data placed

Week_data The week from which the data was collected. `01` exports the current week's data. `02` exports the previous week's data.

The lnmexport utility converts the bridge performance data stored in the `/usr/CML/reports/lnmlnmemon/dir_name` directory, where *dir_name* is a directory named with the IP address of the OS/2 agent. The converted data is placed in the file you specified with the lnmexport command, and stored in the same directory, or a directory you specify with the redirect symbol (>).

The format of the bridge data consists of a comment linefollowed by the performance data, which is organized in groups of 20 rows. The comment line looks like the following:

```
#         B7:   A06   A01
```

`B7` represents the name of the bridge. `A06` and `A01` are the names of the two segments that the bridge connects.

The comment line is followed by groups of 20 rows, each row containing four columns, such as the following:

```
1  0 767622262   3
2  0 767622262   0.00
3  0 767622262   17
4  0 767622262   1000.00
5  0 767622262   0
6  0 767622262   0
7  0 767622262   0
8  0 767622262   0
9  0 767622262   0.00
10 0 767622262   0
11 0 767622262   279651
12 0 767622262   11231000.00
13 0 767622262   13
14 0 767622262   0.00
```

```
15 0 767622262   0
16 0 767622262   0
17 0 767622262   0
18 0 767622262   0
19 0 767622262   0.00
20 0 767622262   0
```

This group contains 10 types of performance data recorded for the two ports of the bridge at a particular sample time. The first column of each row represent a specific type of performance statistic, such as broadcast bytes or broadcast frames. Rows numbered 1 through 10 contain data measured at the bridge port connected to one of the attached segments, while rows 11 through 20 contain the same type of data for the bridge port connected to the other attached segment. The following table shows the performance statistic associated with each numbered row:

Rows for Bridge Port 1	Rows for Bridge Port 2	Performance Statistic
1	11	Broadcast bytes
2	12	Broadcast frames
3	13	Non-broadcast bytes
4	14	Non-broadcast frames
5	15	Link error bytes
6	16	Link error frames
7	17	Target LAN inoperative
8	18	Other reasons
9	19	Adapter congestion
10	20	Filtered

The time the data was recorded is stored in the third column of each row. This value is recorded as the number of seconds since January 1, 1970.

The value for each performance statistic is stored in the fourth column of each row.

As an example, suppose you want to convert the current week'sbridge performance information for a bridge named B7, so you can work with the information in a spreadsheet program. Bridge B7 is managed by an OS/2 agent with an IP address of 9.67.187.11. You want to put the converted information in a file called *brgb7.wks*.

You would enter the lnmexport command as follows:

```
lnmexport 9.67.187.11 brg B7 01 > brgb7.wks
```

The lnmexport command converts the source data to the spreadsheet format by putting all the values for each group on one line of the output file. For example, if the source file contained data for bridge B7 sampled at 10 different times over a particular time interval, and therefore had 10 groups of data, the exported spreadsheet-format file has 10 lines of data, each corresponding to a group in the source file.

To transfer the `brgb7.wks` file to a DOS or OS/2 diskette, you can use the following AIX DOSWRITE command:

```
doswrite -a brgb7.wks brgb7.wks
```

This command transfers the file to a DOS or OS/2 diskette in the diskette drive of your AIX workstation. You can then work with the file using the spreadsheet program.

Chapter 27. Managing LLC Token-Ring Concentrators

The LLC token-ring application of LAN Network Manager communicates with the OS/2 agent to manage the CMIP-based IBM 8230 Model 1 and Model 2 Controlled Access Units (concentrators). Using LAN Network Manager, you can display a graphical view of a concentrator, display information and status for a specific concentrator, enable a concentrator for a program update, and control network access for the adapters attached to the concentrator.

This chapter contains the following topics:

Managing Concentrators

The 8230 Controlled Access Unit uses a version of the IBM heterogeneous LAN management (HLM) protocol to communicate with the OS/2 agent. A LAN Network Manager program can display information about a concentrator, and, if the OS/2 agent registers with a concentrator on behalf of LAN Network Manager, LAN Network Manager can perform actions on that concentrator.

Registering with a Concentrator

When a concentrator is started or reset, it announces its presence on the network by sending a function present event. If a controlling OS/2 agent receives this notification from a concentrator that is in its managed domain, OS/2 agent then attempts to register with the concentrator by sending a register request.

When the OS/2 agent program attempts to register a concentrator, the concentrator verifies the password. If the password matches, the OS/2 agent program registers with the concentrator. During resynchronization, OS/2 agent confirms that the concentrator is still registered by sending a register check.

When the OS/2 agent program is started or restarted, the program issues a register request to concentrators that are already active.

After the concentrator is registered, LAN Network Manager can:

- Set the password and concentrator internal parameters.
- Enable and disable ports and modules.
- Reset the concentrator.
- Change the wrap state of the concentrator.

If you change the password, record the new password. If the OS/2 agent loses communication with the concentrator, another OS/2 agent will have to contact the concentrator and will need the new password.

The concentrator sends events to the OS/2 agent program (to which it is registered) to indicate changes in the following:

- Concentrator communication address
- Port and module status
- Backup-path status
- Wrap status

The concentrator also informs the registered OS/2 agent program of the following conditions, which are passed on to LAN Network Manager as traps:

- A configuration error occurred in the network that is attached to the concentrator ports.
- A forced-remove frame was received and ignored.

  The OS/2 agent program can remove any adapter that is attached to a concentrator, but the concentrator ignores a force-remove command that is sent to one of its adapters (PO, PI, or S).
- An adapter is inserted.
- Ports or lobe attachment modules are removed by the concentrator.
- An error occurred and was detected by the concentrator.

The concentrator registers with only one OS/2 agent at a time. If the password does not match, the OS/2 agent program deregisters the concentrator. The concentrator becomes unregistered when one of the following occurs:

- The OS/2 agent program terminates.
- The OS/2 agent program is terminated and the concentrator attempts to send events.
- The OS/2 agent program loses the link to the bridge that connects the concentrator's segment.
- The path between the concentrator and the OS/2 agent program is no longer operational. (the bridge is down or one of the segments along the path is not operational) and the concentrator attempts to send events.

If the concentrator sends an event to the OS/2 agent program and does not receive a confirmation after six attempts, the concentrator assumes that it is no longer registered and again announces its presence on the network to the OS/2 agents that are active on the domain. The concentrator does not send unsolicited events to the OS/2 agent program to ensure that it is still registered.

An LAN Network Manager program can retrieve information from an unregistered concentrator but it cannot set concentrator parameters or change its status. When a concentrator is unregistered, LAN Network Manager can receive and display the following information:

- Concentrator ID
- Port and module status
- Vital information
  - Microcode level
  - Controlled Access Unit adapter address
- Configuration parameters
- Topology information

If the registered OS/2 agent program is terminated or is isolated from the concentrator because of a ring fault, so that the concentrator is not deregistered, the only way for another OS/2 agent program to register with the concentrator is for the concentrator to send an event; for example, by an adapter insertion. If the event is not confirmed by the registered OS/2 agent program, the concentrator considers itself deregistered and can be registered by any other OS/2 agent program with which it can communicate.

Concentrator Wrap States

When a segment is in a wrapped condition, the segment is using its backup path. When the wrapped condition recovers, the status of the segment might remain wrapped for up to six minutes. The status of a segment is wrapped when:

- A Controlled Access Unit:
  - Is in a wrapped condition.
  - Does not have a cable plugged into either its ring-in or ring-out module.
  - Is not started.
- A device such as an IBM 8220 Token-Ring Optical Fiber Converter is powered off or detects a wrapped condition.
- A main ring cable is disconnected somewhere on the token-ring segment and an 8220 Token-Ring optical fiber converter or a concentrator is on the ring.

Adding a Concentrator Definition

Use the Add Concentrator Definition window to define a Controlled Access Unit (concentrator) in your network. In this window you can specify an identifier (ID) for the concentrator and enter information about the concentrator's physical location.

You can also define as many as four modules for the concentrator by using the toggle buttons on the window. Selecting one or more of the modules brings up an Add Port Definition window for each module.

To add a concentrator definition, follow these steps:

1. Select **Add definition** from the Actions pull-down menu in the LNM OS/2 Agent Configuration window.
2. Select **Concentrator** from the Add definition cascade menu.

   The Add Concentrator Definition window is displayed.
3. Enter information in the fields.
4. Select **OK** to add the definition and close the window. If you want to add more than one definition at a time, select **Apply** to add a definition without closing the window.

Adding a Port Definition

Specify information about each of the ports on a module with the Add Port Definition window. A concentrator supports as many as four modules; each module supports up to 20 ports. As part of the module definition, you can enter information about the ports that indicate their location by building and room number.

To define one or more ports in a module, follow these steps:

1. Select one of the module toggles in the **Add module** field on the Add Concentrator Definition window and press **Enter**.

   The Add Port Definition window is displayed.
2. Enter information in the fields.
3. Select **OK** to add the definition.

Adding a Concentrator Qualifier

Use the Add Concentrator Qualifier window to specify qualifiers that are to be managed by LAN Network Manager. A *qualifier* is a segment number that represents a segment which contains a concentrator but that may not be connected to the OS/2 agent by a linked bridge. Qualifiers are provided by the OS/2 agent program to enable support of 8230 concentrators that are attached on the other side of routers.

To add a definition for a concentrator qualifier, follow these steps:

1. Select **Add definition** from the Actions pull-down menu in the LNM OS/2 Agent Configuration window.
2. Select **Concentrator qualifier** from the Add Definition cascade menu.

   The Add Concentrator Qualifier window is displayed.
3. Enter any changes to the information in the fields.
4. Select **OK** to save the definition and close the window.

Deleting a Concentrator Qualifier

Using the Delete Concentrator Qualifier window, you can delete a concentrator qualifier that you previously defined. A *qualifier* is a segment number that represents a segment which contains a concentrator but that may not be connected to the OS/2 agent by a linked bridge. Qualifiers are provided by the OS/2 agent program to enable support of 8230 concentrators that are attached on the other side of routers.

To delete a definition for a concentrator qualifier, follow these steps:

1. Select **Delete definition** from the Actions pull-down menu in the LNM OS/2 Agent Configuration window.
2. Select **Concentrator qualifier** from the Delete definition cascade menu.

   The Delete Concentrator Qualifier window is displayed.
3. Select the segment for the qualifier you want to delete.
4. Select **Delete** to delete the qualifier.

Displaying a Concentrator Submap

Open a Concentrator submap to display a graphical representation of the concentrator. Points of attachment and other physical features of the hardware are recognizable in the submap, and managed elements of the concentrator are represented by icons. The icons give you access to the managed elements of the device and to the stations inserted into the device.

To display a Concentrator submap, double-click on a concentrator icon in a Segment submap. The Concentrator submap is displayed.

The top portion of the graphical representation of the concentrator includes up to three diamond-shaped icons, representing the primary-in, primary-out, and secondary adapters of the concentrator. Directly to the right of the top portion of the Concentrator submap is a square icon that represents the concentrator itself.

The remaining portions of the submap represent the modules of the concentrator. As many as four modules can be connected to a concentrator and represented in the submap. The diamond-shaped icons to the right of each module represent that module.

Each module can contain up to 20 ports. The ports in a module are represented by a pair of icons. The diamond-shaped icon to the left of each pair represents the port. If a device is connected to a port, it is represented by another icon directly to the right of the port icon. The shape of the icon to the right indicates the type of device that is connected to the port:

Icon Shape	**Device**
Square	Station
Oval	OS/2 agent station

Diamond Bridge

You can access management windows for each device represented in the submap by selecting the device and then using the LAN pull-down or context menu to select the type of information you want to see for that device. You can also double-click on the icons that represent stations or ports to open a Node submap for the station or port.

Note: If you change the access control parameters to make access control active, the Concentrator submap contains the most recent information *before* access control is activated.

Displaying a List of Concentrators

To view a list of the concentrators that are defined in your network, use the List of Concentrators window. This window displays a scrollable list of defined concentrators and the following information for each:

- Concentrator ID
- Concentrator status
- Number of the LAN segment containing the concentrator
- Whether the concentrator is registered

The list of concentrators includes concentrators that are currently active and those that have been defined but are not active. The concentrators on the window are listed in order of concentrator ID.

To display a list of the defined concentrators in your network, select **Concentrators** from the Lists pull-down menu on the LNM OS/2 Agent Configuration window.

Use the List of Concentrators window to register or deregister a concentrator. To register or deregister a concentrator, select the concentrator, then select the **Register** or **Deregister** push button. See “Registering with a Concentrator” on page 243 for more information about registering and deregistering concentrators.

To delete a concentrator definition using the List of Concentrators window, select the concentrator, then select the **Delete** push button.

Displaying a Concentrator Profile

The Concentrator Profile window displays information about the current operation and configuration of the Controlled Access Unit (concentrator). In addition to providing such general information as the attached segment number and the registration status, this window displays the adapter addresses for the primary-in, primary-out, and secondary adapters of the concentrator. The window also indicates the status of modules that are attached to the concentrator.

If the concentrator you selected is not active, or if the query is not successful, the status displayed in this window includes the information available from the last access to that concentrator.

To display a concentrator profile, select the concentrator, then select **Profile** from either the LAN pull-down menu or the context menu. If the concentrator you selected is not active, or if the query is not successful, some fields on the window are blank.

You can navigate directly to the following concentrator windows by selecting one of these choices from the Navigation pull-down menu on the Concentrator Profile window:

Select:	**To navigate to:**
Configuration	Concentrator Configuration window
Fault	Concentrator Fault window

Displaying Configuration Information for a Concentrator

The Concentrator Configuration window provides location and status information about the Controlled Access Unit (concentrator). The window displays the concentrator identifier (ID) for the resource, and you can add or change the text in the location field to reflect current configuration.

To display the Concentrator Configuration window, select the concentrator for which you want configuration information, then select **Configuration** from either the LAN pull-down menu or the context menu.

You can select the following actions from the Actions pull-down menu on the concentrator Configuration window:

For information about:	**Read:**
Reset	“Resetting the Concentrator” on page 250
Code Update	“Enabling Program Update” on page 250
Delete definition	“Deleting a Concentrator Definition” on page 251
Register	“Registering a Concentrator” on page 251
Deregister	“Deregistering a Concentrator” on page 251
Wrap forced by OS/2 agent	“Changing the Wrap State for a Concentrator” on page 251

You can navigate directly to the following concentrator windows by selecting one of these choices from the Navigation pull-down menu on the Concentrator Configuration window:

Select:	**To navigate to:**
Profile	Concentrator Profile window
Fault	Concentrator Fault window

Resetting the Concentrator

To reset the selected concentrator, select **Reset concentrator** from the Actions pull-down menu on the Concentrator Configuration window.

Resetting the concentrator can disrupt normal network activity.

Enabling Program Update

To update the microcode for the selected Controlled Access Unit (concentrator), use the Concentrator Code Update window. The window displays the identifier (ID) of the concentrator and its location, and you can specify the name of the program to be loaded and the adapter address of the loader device.

This option enables the concentrator for updates but does not load the program file into the concentrator. The option enables a concentrator under one of the following conditions:

- The concentrator is registered with this OS/2 agent program.
- The concentrator is not registered with an OS/2 agent program, and the concentrator has detected the need for a microcode update.

Under either of these conditions, the concentrator then initiates the update of program code from the loader device.

To enable a selected concentrator for a program update (to update the concentrator with new code), select **Code Update** from the Actions pull-down menu on the Concentrator Configuration window.

The concentrator wraps while loading and is inoperative until the program has been updated. As a result, if you are loading more than one concentrator, a concentrator that you are loading might break the path between the remote program loader and other concentrators that you are loading. To avoid problems when loading concentrators on the same segment, load the concentrators one at a time, ensuring that the program update of one concentrator is complete before you begin to update the program of the next concentrator.

You can navigate directly to the following concentrator windows by selecting one of these choices from the Navigation pull-down menu on the Concentrator Code Update window:

Select:	**To navigate to:**
Profile	Concentrator Profile window
Fault	Concentrator Fault window

Deleting a Concentrator Definition

To delete a concentrator definition from the LAN Network Manager concentrator table, follow these steps:

1. Select the **Delete definition** from the Actions pull-down menu on the Concentrator Configuration window.

   An error message is displayed if the definition cannot be deleted.
2. Select **OK** to delete the concentrator definition and close the dialog box.

Registering a Concentrator

A concentrator can be registered to one OS/2 agent at a time. By registering a concentrator with an OS/2 agent, the OS/2 agent can follow these steps:

- Set the password and internal concentrator parameters
- Enable and disable ports and modules
- Reset the concentrator
- Change the wrap state of the concentrator

Only a controlling OS/2 agent can register with a concentrator.

To register an OS/2 agent with a concentrator, select **Register** from the Actions pull-down menu on the Concentrator Configuration window of the concentrator you want to register.

For more information about concentrator registration, refer to “Registering with a Concentrator” on page 243.

Deregistering a Concentrator

To deregister an OS/2 agent from a concentrator, select **Deregister** from the Actions pull-down of the Concentrator Configuration window of the concentrator you want to deregister.

For more information about concentrator registration, refer to “Registering with a Concentrator” on page 243.

Changing the Wrap State for a Concentrator

To change the wrap state for the concentrator, follow these steps:

1. Select **Wrap forced by LNM OS/2 agent** from the Actions pull-down menu on the Concentrator Configuration window.

This choice is not available if an error occurred while LAN Network Manager was obtaining the profile.

2. Select a wrap status from the cascade menu.

   LAN Network Manager displays a dialog box confirming the change in the wrap status of the concentrator.

3. Select **OK** to close the dialog box.

Attention: Changing the wrap state of a concentrator can disrupt ring operation or host communication with some devices.

If you change the wrap state and an error condition exists on the segment that prevents the concentrator from running effectively under the new wrap state, the change does not take effect until the error is removed.

Displaying Fault Information for a Concentrator

The Concentrator Fault window displays error data for the Controlled Access Unit (concentrator). In addition to providing general identifying file information, such as the concentrator identifier (ID) and the concentrator registration status, the window displays error data for both the ring-in and ring-out sides of the concentrator, and for the backup path.

To display fault information for a concentrator, select the concentrator for which you want fault information, then select **Fault** from either the LAN pull-down menu or the context menu.

You can navigate directly to the following Concentrator windows by selecting one of these choices from the Navigation pull-down menu on the Concentrator Fault window:

Select:	**To navigate to:**
Profile	Concentrator Profile window
Configuration	Concentrator Configuration window

Displaying Configuration Information for a Module

To view configuration information about a specific port module, use the Module Configuration window. This window provides the current operating status of the modules and additional information about the Controlled Access Unit (concentrator) to which the module is attached. The window also indicates whether there is a mismatch between a particular port and its expected adapter address.

To display the Module Configuration window, select the module for which you want configuration information, then select **Configuration** from either the LAN pull-down menu or the context menu.

To change the operating status of the module, select **Enable** or **Disable** from the Actions pull-down menu on the Module Configuration window. See “Changing Module Status” for more information.

Changing Module Status

To change the operating status of a module, follow these steps:

1. Select the module for which you want to display status.
2. Select **Configuration** from either the LAN pull-down menu or the context menu.

   The Module Configuration window is displayed.
3. Select **Enable** or **Disable** from the Actions pull-down menu on the Module Configuration window.

   LAN Network Manager displays a dialog box warning you that the module status is going to be changed. An error message is displayed if the status change is not successful.
4. Select **OK** to close the dialog box.

Changing module status can disrupt normal network activity.

Displaying Configuration Information for a Port

To view configuration information about a specific port, use the Port Configuration window. In addition to providing the current operating status of the port, this window displays information about the module to which it is attached and about the Controlled Access Unit (concentrator) that controls the module.

To display the Port Configuration window, select the port for which you want configuration information, then select **Configuration** from either the LAN pull-down menu or the context menu.

To change the operating status of the port, select **Enable** or **Disable** from the Actions pull-down menu on the Port Configuration window. For more information, see “Changing Port Status”.

Changing Port Status

To change the status of a port, follow these steps:

1. Select the port for which you want to display status.
2. Select **Configuration** from either the LAN pull-down menu or the context menu.

   The Port Configuration window is displayed.
3. Select **Enable** or **Disable** from the Actions pull-down menu on the Port Configuration window.

LAN Network Manager displays a dialog box warning you that the port status is going to be changed. An error message is displayed if the status change is not successful.

4. Select **OK** to close the dialog box.
5. Select **OK** to close the Port Configuration window.

If the concentrator loses power, this setting is not maintained.

Displaying a PI, PO, S Profile

To view profile information for a specific adapter in the Controlled Access Unit (concentrator), use the PI/PO/S Profile window. This window displays the concentrator identifier (ID) and segment number of the selected adapter.

The information that is provided on this window pertains only to the adapter that you selected on the Concentrator submap. For example, if you select the primary-out adapter on the concentrator, the PI/PO/S Profile window displays information only for the primary-out adapter.

To display a profile for the adapters in the concentrator, select a PI, PO, or S icon, then select **Profile** from either the LAN pull-down menu or the context menu.

Displaying a Port Device Profile

Use the Profile window to display information about a specific adapter or bridge port.

The ports in a module are represented in the Concentrator submap by a pair of icons. The diamond-shaped icon to the left of each pair represents the port. If a device is connected to a port, it is represented by another icon directly to the right of the port icon. The shape of the icon to the right indicates the type of device that is connected to the port:

Icon Shape	**Device**
Square	Station
Oval	OS/2 agent station
Diamond	Bridge

To display a profile window for a device, select the device, then select **Profile** from either the LAN pull-down menu or the context menu. A Profile window for the station or bridge port is displayed. For more information, see “Displaying a Station Profile” on page 224.

Navigate directly to the Configuration window for the selected adapter or bridge port by selecting **Configuration** from Navigation pull-down menu on the Profile window.

Chapter 28. Traps

Understanding Traps

LAN Network Manager obtains information about the LAN environments that it is managing by communicating with agents that reside in those environments. The agents send traps to LAN Network Manager, both in response to commands from the program and as unsolicited notifications of network changes. LAN Network Manager then processes these traps to enable proper correlation between the resource to which the trap pertains and the topological display of that resource.

All traps that are sent from the LAN environments are received first by NetView for AIX. When LAN Network Manager is installed, it registers with NetView for AIX to receive traps from specific types of agents in the network. The individual agents are collectively identified by an enterprise identifier, which is a dotted decimal representation of the enterprise-specific MIB that the different types of agents use. LAN Network Manager subscribes to traps that are broadcast from agents with a particular enterprise ID, and in doing so LAN Network Manager receives traps from all agents that share the ID.

As part of LAN Network Manager configuration, you specify which agents will be communicating with LAN Network Manager. When LAN Network Manager starts, the discovery process begins for the LAN Network Manager agent programs that you have configured in SMIT. As agents respond to the discovery process, NetView for AIX begins to receive traps from the newly identified agents and then forward them to LAN Network Manager.

The traps received from agents do not contain enough information to enable NetView for AIX to correlate its topology display with the NetView for AIX event display, and the NetView for AIX event history. To ensure that this correlation information is provided to NetView for AIX, LAN Network Manager processes the traps that NetView for AIX has forwarded. In doing so, LAN Network Manager creates a new trap that combines the original information with the name of the affected resource.

When LAN Network Manager completes its trap processing, the trap is sent to NetView for AIX, where it is recorded in the trapd log. The trap is also recorded in the event card display, if the LAN Network Manager filter is active and if the trap's format allows it. For more information on the LAN Network Manager filter, read "Using Filters" on page 256.

Note: The first instance of a trap in the trapd log does not contain correlation information, so the information in the trap may contain unformatted hexadecimal data. When you view the trapd log for entries pertaining to LAN Network Manager, look for the second instance of each trap.

When LAN Network Manager is installed, the **addtrap** command is invoked to generate customized trap definitions for the /usr/OV/conf/trapd.conf file. These definitions provide a more meaningful display of LAN Network Manager traps when they are logged by the NetView for AIX trapd log. You can modify these trap definitions to tailor the information

that appears in the event display to your own needs. For more information about how to customize the trap formats, refer to the *NetView for AIX User's Guide*.

Using Filters

LAN Network Manager provides NetView for AIX with event filters to ensure that the traps from appropriate agents are forwarded to LAN Network Manager for processing and that the correlated traps are properly recorded in the event display.

One kind of filter that specifies which traps are to be displayed in the NetView for AIX event display is located in /usr/OV/filters/lnm.filter. When LAN Network Manager is first installed, the filter indicates that all traps originating from the LAN Network Manager enterprise are to be displayed.

You can specify that a trap not be sent to the event card display by customizing the trap's format. Using the Event Configuration window in NetView for AIX, you can change the trap logging category. For example, if a particular trap is not of much interest to you, you can prevent it from being displayed with the event cards by setting the Event Category of the trap to `Log Only`. Although the trap is not displayed with the event cards, you can still access it through the trapd log. For more extensive control of what goes into the event card display, you can create filters for use with the LAN Network Manager traps.

As part of the trap conversion process, LAN Network Manager creates a new trap that contains a modified enterprise ID, so that the enterprise ID for LAN Network Manager is now associated with the trap, instead of the enterprise ID of the agent. The name of the affected resource is also attached to the trap, and the trap is then sent to NetView for AIX.

Note: Use care when making any changes to the lnm.filter filter. If you are not thoroughly familiar with the NetView for AIX process for customizing trap formats or for creating event filters, refer to the *NetView for AIX User's Guide*.

Another type of filter is located in the /usr/lpp/cml/filters directory. The filters in this directory register LAN Network Manager with NetView for AIX to receive traps from the

agents in the network. There are several filter files in this directory that are used by the LAN Network Manager applications to gather crucial trap information from agents in the network.

Attention: Do not modify the filters in the /usr/lpp/cml/filters directory, other than the lnm.filter as previously described. If LAN Network Manager is unable to receive traps from its agent programs, operation can be impaired.

LNM OS/2 Agent Application Traps

The following types of traps are processed by the OS/2 agent application:

- Generic traps
- Traps generated by the OS/2 agent application
- Traps generated by the OS/2 agent program

If you are checking the trapd log for traps that have originated from an OS/2 agent program, be aware that there are times when the first instance of a trap contains unreadable information because the data is represented in hexadecimal format. Due to the way that NetView for AIX records trap information, if each character in the string is a legitimate ASCII value, the value is recorded as an ASCII string, including special characters. However, if one or more of the characters in the string is not an ASCII value, the value is represented in hexadecimal format.

For example, the hexadecimal value of `21 22 23 24` is recorded as `! " # $` in the first instance of the trap in the trapd log. LAN Network Manager converts hexadecimal values to meaningful ASCII values, so that `21 22 23 24` is represented as `21 22 23 24` in the second instance of the trap, which LAN Network Manager sends to NetView for AIX after processing.

Generic Traps

The section lists the generic traps that are processed by the OS/2 agent application. However, these traps are not processed by LAN Network Manager for correlation information and are not sent back to NetView for AIX for display with the event cards.

0

Description: coldStart

LNM for AIX Response: Wait 5 minutes and then attempt to establish the connection. If successful, poll the agent for the latest status, otherwise, repeat the attempt to establish the connection at 5 minute intervals.

1

Description: warmStart

LNM for AIX Response: Wait 5 minutes and then attempt to establish the connection. If successful, poll the agent for the latest status, otherwise, repeat the attempt to establish the connection at 5 minute intervals.

2

Description: linkDown

LNM for AIX Response: Mark the agent unknown. Wait 5 minutes and then attempt to establish the connection. If successful, poll the agent for the latest status, otherwise, repeat the attempt to establish the connection at 5 minute intervals.

3

Description: linkUp

LNM for AIX Response: Wait 5 minutes and then attempt to establish the connection. If successful, poll the agent for the latest status, otherwise, repeat the attempt to establish the connection at 5 minute intervals.

4

Description: authenticationFailure

LNM for AIX Response: Log in the nettl log.

OS/2 Agent Application-Generated Traps

This section lists the traps that can be sent by the OS/2 agent application and suggested actions.

The traps in this section are defined under the 1.2.3.1.4.1.2.6.21.1.2 enterprise ID, which is associated with LAN Network Manager.

bridgeHistoryDataComplete

Description: A time period for collecting bridge history data has expired. This trap is issued only if history data is being collected.

Action: None

segHistoryDataComplete

Description: A time period for collecting segment history data has expired. This trap is issued only if history data is being collected.

Action: None

LNMOS2AgentSocketError

Description: The socket connection between LAN Network Manager and the OS/2 agent has failed.

Action: The socket connection between LAN Network Manager and the OS/2 agent has failed. Check the nettl log for any socket-related messages logged by LAN Network Manager. Also verify the state of the OS/2 agent. You may need to do one or more of the following:

- Restart the machine that is running the OS/2 agent.
- Restart the OS/2 agent.
- Stop and restart LAN Network Manager.

LNMOS2AgentSocketClosed

Description: The socket connection between LAN Network Manager and the OS/2 agent is closed.

Action: The socket connection between LAN Network Manager and the OS/2 agent has closed unexpectedly. Verify the state of the OS/2 agent. You may need to either restart the machine that is running the OS/2 agent or restart the OS/2 agent.

LNMOS2AgentNotResponding

Description: The OS/2 agent is not responding to requests for information from LAN Network Manager.

Action: The OS/2 agent is no longer able to respond to run command requests. Verify the state of the OS/2 agent. You may need to either restart the machine that is running the OS/2 agent or restart the OS/2 agent.

OS/2 Agent Traps

This section lists the traps that can be sent by the OS/2 agent program and the actions that LAN Network Manager takes when these traps are received.

Note: These traps correspond to the DFIPD messages that are generated by the OS/2 agent program and have the same number. You can look up a trap in the Messages chapter of the LAN Network Manager for OS/2 Version 2.0 documentation to obtain more information about the event that a trap is reporting on, such as error code descriptions and possible corrective actions.

When the LAN Network Manager Response indicates that the status will be set to a particular setting, this actually indicates the best, or worst, status that can be set for the resource from processing the trap. For example, if the LAN Network Manager Response indicates to set the status to marginal and it is currently in a critical state, the resource will remain in the critical state until the condition causing the critical state is resolved. Similarly, if multiple resources can affect the status of a resource, a response that indicates to set the status to normal may be overriden by the state of another resource.

The traps in this section are defined under the 1.3.6.1.4.1.2.6.20 enterprise ID, which is associated with OS/2 agent.

The redirected traps are defined under the 1.3.6.1.4.1.2.6.21.1.1 enterprise ID, which is associated with LAN Network Manager.

001

Description: LAN Network Manager started.

LNM for AIX Response: Poll the agent to update topology. Add correlation information and return to NetView for AIX.

030

Description: Data Loss started.

LNM for AIX Response: Set the LAN Submap marginal. Stop communicating with this OS/2 agent until trap 031 is received. Add correlation information and return to NetView for AIX.

031

Description: Data loss stopped.

LNM for AIX Response: Refresh topology views by polling the agent. Add correlation information and return to NetView for AIX.

049

Description: LAN Network Manager ended.

LNM for AIX Response: Set the LAN Submap unknown. Add correlation information and return to NetView for AIX.

101

Description: Excessive Token-Ring errors.

LNM for AIX Response: Set segment status marginal. Add correlation information and return to NetView for AIX.

102

Description: Soft errors increasing.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

103

Description: Soft errors decreasing.

LNM for AIX Response: Set the segment status normal. Add correlation information and return to NetView for AIX.

104

Description: Recovered error counters.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

106

Description: Ring error report.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

107

Description: Adapter congested.

LNM for AIX Response: Set the station status marginal. Add correlation information and return to NetView for AIX.

108

Description: Ring poll failure.

LNM for AIX Response: Filter out.

109

Description: Ring monitor error: segment recovered.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

110

Description: Adapter no longer congested.

LNM for AIX Response: Set the station status normal. Add correlation information and return to NetView for AIX.

120

Description: Error reporter failure: processing continues.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

123

Description: Monitored adapter not responding.

LNM for AIX Response: Change the status of the adapter to critical. Add correlation information and return to NetView for AIX.

124

Description: Monitored adapter returned to network.

LNM for AIX Response: Change the status of the adapter to normal. Add correlation information and return to NetView for AIX.

180

Description: Bridge link failure.

LNM for AIX Response: Change the bridge to unlinked and critical. Check the affected segments. The segment status changes if there is no other linked bridge, and if this is not the segment OS/2 agent is on and there is not a concentrator qualifier for this segment. Add correlation information and return to NetView for AIX.

181

Description: Bridge port status change.

LNM for AIX Response: Filter out.

182

Description: Bridge security breach: unauthorized manager.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

183

Description: LAN Network Manager rejected by bridge.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

187

Description: Bridge performance threshold exceeded.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

188

Description: Bridge congested.

LNM for AIX Response: Change the status of the bridge to marginal. Add correlation information and return to NetView for AIX.

190

Description: Invalid message length.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

191

Description: Duplicate data in message.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

192

Description: Missing data in message.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

202

Description: Token-Ring inoperative.

LNM for AIX Response: Set the segment status critical. Add correlation information and return to NetView for AIX.

203

Description: Token-Ring temporary error: recovered and operating normally.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

204

Description: Token-Ring temporary error: adapter(s) removed.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

205

Description: Fault information changed.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

206

Description: Manual intervention complete: segment recovered.

LNM for AIX Response: Set the segment status normal. Add correlation information and return to NetView for AIX.

209

Description: Auto-removal error.

LNM for AIX Response: Set arcs in LAN Submap critical. Add correlation information and return to NetView for AIX.

210

Description: Unable to initialize LAN Network Manager's adapter.

LNM for AIX Response: Set arcs in LAN Submap critical. Add correlation information and return to NetView for AIX.

212

Description: LAN Network Manager's adapter hardware failure.

LNM for AIX Response: Set arcs in LAN Submap critical. Add correlation information and return to NetView for AIX.

213

Description: LAN Network Manager's adapter interface failed.

LNM for AIX Response: Set arcs in LAN Submap critical. Add correlation information and return to NetView for AIX.

214

Description: Unable to close LAN Network Manager's adapter.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

215

Description: Wire fault: LAN Network Manager's adapter or lobe failed.

LNM for AIX Response: Set arcs in LAN Submap critical. Add correlation information and return to NetView for AIX.

216

Description: LAN Network Manager's adapter closed.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

220

Description: NAUN change.

LNM for AIX Response: Determine if the trap indicates an adapter insertion or the removal of one or more adapters. If an adapter is inserted, issue adapter query run command for label and positioning data. Update the topology view. This trap is not returned to NetView for AIX.

221

Description: Adapter insertion.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

222

Description: Remove adapter command received.

LNM for AIX Response: Set LAN Submap critical. Add correlation information and return to NetView for AIX.

224

Description: New ring monitor.

LNM for AIX Response: Filter out.

225

Description: Adapter removed by LAN Network Manager.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

230

Description: Unable to open LAN Network Manager's adapter.

LNM for AIX Response: Set LAN Submap critical. Add correlation information and return to NetView for AIX.

231

Description: Unable to close LAN Network Manager's adapter.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

300

Description: Bridge failed to link.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

306

Description: Bridge taken off-line.

LNM for AIX Response: Change the bridge to unlinked. Check the affected segments. The segment status changes if there is no other linked bridge and this is not the segment the OS/2 agent is on and there is not a concentrator qualifier for this segment. Add correlation information and return to NetView for AIX.

322

Description: Ring trace notification.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

323

Description: Unauthorized trace attempt.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

326

Description: Main path wrapped to backup.

LNM for AIX Response: Change the status of the segment to wrapped. Add correlation information and return to NetView for AIX.

327

Description: Backup path inoperative.

LNM for AIX Response: Change the status of the segment to marginal. Add correlation information and return to NetView for AIX.

328

Description: Main path wrap condition recovered.

LNM for AIX Response: Change the status of the segment to normal. Add correlation information and return to NetView for AIX.

329

Description: Backup path recovered.

LNM for AIX Response: Add correlation information and return to NetView for AIX. The status of the segment is not changed to normal because, although the backup path has been recovered, the segment is still wrapped.

436

Description: Concentrator back-up path inoperable.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

437

Description: Concentrator has wrapped the main ring onto the back-up path.

LNM for AIX Response: The status of the concentrator changes to marginal. Add correlation information and return to NetView for AIX.

438

Description: Concentrator merged the token ring from a wrapped condition.

LNM for AIX Response: The status of the concentrator changes to normal. Add correlation information and return to NetView for AIX.

439

Description: Concentrator Internal Error.

LNM for AIX Response: The status of the concentrator changes to critical. Add correlation information and return to NetView for AIX.

440

Description: Concentrator has recovered from an internal error.

LNM for AIX Response: The status of the concentrator changes to normal. Add correlation information and return to NetView for AIX.

441

Description: Concentrator port receptacles to addresses mismatch.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

442

Description: Concentrator port receptacles to addresses mismatch corrected.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

443

Description: Force remove command ignored by a concentrator.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

444

Description: Concentrator port receptacle or module deactivated.

LNM for AIX Response: Issue run commands to get status of module and port. Update status to reflect status in run command response. NAUN changes provide updated status of the adapters. Add correlation information and return to NetView for AIX.

445

Description: Unauthorized adapter on LAN.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

446

Description: Adapter on wrong concentrator lobe receptacle.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

447

Description: Unauthorized bridge adapter.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

448

Description: Duplicate adapter address on a token ring.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

449

Description: Adapter inserted at unauthorized time or day.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

457

Description: Bridge unlink completed successfully.

LNM for AIX Response: Change the bridge to unlinked. Check the affected segments. The segment status changes if there is no other linked bridge and this is not the segment OS/2 agent is on. Add correlation information and return to NetView for AIX.

458

Description: Bridge link completed successfully.

LNM for AIX Response: Send bridge query. Check the affected segments. The segment status changes if there was no other linked bridge and this is not the segment OS/2 agent is on. Update topology view. Add correlation information and return to NetView for AIX.

459

Description: Bridge no longer congested.

LNM for AIX Response: Change the status of the bridge to normal. Add correlation information and return to NetView for AIX.

464

Description: Error detected by remote device during remote program update (RPU).

LNM for AIX Response: The status of the concentrator changes to critical. Add correlation information and return to NetView for AIX.

465

Description: Remote Program Update completed.

LNM for AIX Response: The status of the concentrator changes to normal. Refresh the concentrator view. Add correlation information and return to NetView for AIX.

466

Description: Critical error detected during remote program update (RPU).

LNM for AIX Response: The status of the concentrator changes to critical. Add correlation information and return to NetView for AIX.

467

Description: User alert filter program exit not available.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

468

Description: Unable to initialize the adapter for remote program update (RPU).

LNM for AIX Response: Add correlation information and return to NetView for AIX.

494

Description: Unable to initialize Station Manager Support.

LNM for AIX Response: Add correlation information and return to NetView for AIX.

751

Description: A new concentrator on the network.

LNM for AIX Response: Do all of the steps listed in the discovery process for a concentrator. Add correlation information and return to NetView for AIX.

800

Description: Concentrator port status change event.

LNM for AIX Response: If the trap indicates an adapter has been inserted, create the element if it is a new adapter, and plug the adapter into the port. Add correlation information and return to NetView for AIX.

801

Description: Bridge performance notification.

LNM for AIX Response: If history collection is enabled for the bridge and the time is within the collection period, write bridge history records. Add correlation information and return to NetView for AIX.

990

Description: LAN Network Manager abended.

LNM for AIX Response: Set the LAN Submap unknown. Add correlation information and return to NetView for AIX.

Part 6. SNMP Token-Ring

Chapter 29. Applications and Agents

SNMP Token-Ring and Bridge Applications

In addition to managing LLC-based token-ring networks, LAN Network Manager also manages token-ring networks that communicate through the Simple Network Management Protocol (SNMP). LAN Network Manager uses two of its applications, the SNMP bridge application and the SNMP token-ring application, to manage the token-ring segments in the networks and the SNMP devices that interconnect them.

The SNMP token-ring application reports dynamic status changes on the token-ring network and enables LAN Network Manager to retrieve station information and set management parameters. LAN Network Manager receives its configuration information about the token-ring resources from the following SNMP proxy agents:

- Token-ring surrogate agents that implement the AWP 7607 MIB (IBM private MIB), such as the IBM 8229 Bridge and H-TMAC.
- Remote monitor agents that implement the RFC 1513 MIB, such as IBM SNMP-managed 8230 Token-Ring Concentrators.
- Concentrator agents that implement the IBM 8230 MIB, such as the IBM 8230 Controlled Access Unit Model 3.

The SNMP bridge application provides LAN Network Manager with the management of the SNMP bridging devices and shows the connectivity of the bridges to other environments, such as X.25, Frame Relay, Ethernet, and FDDI. The SNMP bridge application notifies LAN Network Manager of status changes in the SNMP bridges and relays management instructions from LAN Network Manager to the bridges.

LAN Network Manager manages several types of bridges through the SNMP bridge application:

- Source-routing bridges
- Transparent bridges
- Source-route transparent bridges
- Bridges that function as both source-routing and transparent bridges, such as the IBM 6611 Network Processor
- Translational bridges that act as a gateway between a source-routing and a transparent bridge network (the IBM 8229 Bridge, for example)

The SNMP bridge application obtains resource information from agent resources that implement the RFC 1286 and RFC 1213 (MIB II) MIBs (or the RFC 1493 and 1213 MIBs), along with other MIBs.

SNMP Token-Ring and Bridge Agents

LAN Network Manager communicates with several agent resources in the SNMP token-ring networks to retrieve configuration information and to send management instructions to stations. These agents vary depending on whether the information pertains to a segment or station or to an SNMP bridge.

Token-ring segment information is acquired from the following kinds of agents:

- Token-ring surrogate agents that implement the AWP 7607 MIB, such as the IBM 8229 or the IBM 8260 TMAC
- Remote monitor (RMON) agents that implement the RFC 1513 MIB, such as the IBM SNMP-managed 8230 concentrators
- Concentrator agents that implement the IBM 8230 MIB, such as the IBM 8230 Controlled Access Unit Model 3.

Sometimes the value of a parameter displayed in a window is simultaneously reported by more than one agent. When this happens, LAN Network Manager displays the value from the agent MIB according to the following priority scheme, beginning with the highest priority agent: token-ring surrogate agent, remote-monitor agent, and concentrator agent.

The reporting agent can change when other agents are discovered. For example, if a remote-monitor agent is discovered first, LAN Network Manager displays the value provided by the RMON agent until a surrogate agent is discovered. Management of the segment then shifts to the surrogate agent.

Also, using SMIT you can disable the automatic priority scheme used by LAN Network Manager. By specifying whether or not you want an agent to be discovered, you can change the agent that has the highest priority. For more information, refer to the section describing the **Manage the agent** parameter in “Configuring SNMP Agents that Manage Token-Ring Segments” on page 270.

LAN Network Manager manages SNMP bridges through agents that are resident in the bridging devices. LAN Network Manager supports those agents that implement either RFC 1286 and RFC 1213 (MIB II), or RFC 1213 (MIB II) and RFC 1493. LAN Network Manager can also provide information from agents that support the following MIBs:

RFC 1231 IEEE Token-Ring 802.5 MIB

RFC 1232 DS1 Interface Type MIB

RFC 1315 Frame Relay DTE MIB

RFC 1317 RS-232-like Hardware Device MIB

RFC 1381 SNMP MIB Extension for X.25 LAPB

RFC 1382 SNMP MIB Extension for the X.25 Packet Layer

RFC 1398 Ethernet-like Interface Types MIB

Chapter 30. Configuring Management Parameters for SNMP Token-Ring Resources

After installing the SNMP Bridge and SNMP Token-Ring application, you can configure SNMP Token-Ring and SNMP bridge capability for the network you are managing by using SMIT to define values for:

- LAN Network Manager general parameters
- General parameters for SNMP agents
- SNMP token-ring proxy agent parameters
- SNMP bridge parameters

This chapter describes how to carry out these tasks.

Using SMIT to Configure LAN Network Management

The configuration parameters that you define in SMIT are saved in files with an extension of .conf in the `/usr/CML/conf/lnmbrmon` and `/usr/CML/conf/trmon` directories. These files are read each time LAN Network Manager is started.

Configuring General Parameters for SNMP Agents

In order for SNMP agent programs to forward trap information to LAN Network Manager applications, the agents must be specifically configured. There are two parameters that you might need to configure in the agent programs to communicate with LAN Network Manager and NetView for AIX:

- IP address of the machine on which Nways Manager-LAN is running
- Community name, time-outs, and retries as defined in NetView for AIX

IP Address of the Management Station

The IP address of the station on which Nways Manager-LAN is installed must be configured in each of the SNMP agent programs. If an agent is not configured with the correct IP address, LAN Network Manager applications cannot correlate traps and provide network topology and status changes.

The steps for configuring an agent program depend on the type of SNMP agent you are configuring. Refer to the documentation for each agent for configuration instructions.

Agent Community Names

A community name is a password that enables SNMP access to MIB values on an agent. To retrieve and update MIB values, LAN Network Manager applications use the SNMP community names defined in NetView for AIX to build SNMP queries. For these

queries to be successful, the community name defined in each SNMP agent program must match the following values defined in NetView for AIX for the agent:

- Read community name for retrieved MIB values
- Write community name for updated MIB values

To ensure that the community names match, check the community defined in each agent program, then verify that the names match those defined on the NetView for AIX SNMP Configuration window. To open the SNMP Configuration window, select **Options -> SNMP Configuration** from the NetView for AIX menu bar.

If the community names do not match, you can change the community name defined either on the NetView for AIX SNMP Configuration window or in the agent program. If the community name defined for an agent in the agent program is `public`, you do not have to define the community name in NetView for AIX; `public` is the default community name.

Any change you make to a community name takes effect immediately. It is not necessary to stop and restart Nways Manager-LAN to activate the change. For more information about configuring agent community names, refer to the *NetView for AIX User's Guide*.

Agent Time-Outs

In order for an SNMP bridge or SNMP token-ring to be fully managed by LAN Network Manager, you must configure its time-out parameter with a large enough value so that the resources can be discovered by Nways Manager-LAN.

If you have a large network, be sure to define a longer time-out period so that the agent has enough time to provide all its configuration information before Nways Manager-LAN updates the LAN topology in the LAN submaps.

To change the time-out period defined for an agent program, select **Options -> SNMP Configuration** from the NetView for AIX menu bar and enter a new time-out value in the SNMP Configuration window.

Configuring SNMP Agents that Manage Token-Ring Segments

You can configure three types of SNMP proxy agents to manage SNMP token-ring segments:

- Token-ring surrogate
- RMON
- SNMP-managed 8230

To define or reconfigure a token-ring SNMP proxy agent using SMIT, follow these steps:

1. Ensure you are logged on with root privileges.

2. If SMIT is not running, enter **smit cml** from an AIX operating system shell, or select **Administer -> Campus Manager SMIT** from the NetView for AIX menu bar.

   The SMIT menu is displayed.
3. Select **Configure**.
4. Select **Configure SNMP token-ring capability**.
5. Select **Configure IBM SNMP token-ring proxy agent**.
6. Select the type of proxy agent you want to configure.
7. Enter the IP address of the proxy agent and press Enter or select **OK**.
8. Enter new values for any of the following configuration parameters. To display help information about a parameter, click on **?** and point to the field.

IP address	Internet Protocol (IP) address of the agent.
Resync interval	Time period (in days, hours, minutes) used by Nways Manager-LAN to rediscover the agent, resynchronize the segment, and update LAN submaps with new or changed information about the resources managed by the agent. Each resynchronziation refreshes LAN submaps with the latest changes made to the network topology (for example, moving, adding, or removing token-ring devices).
Polling interval	Time period (in days, hours, minutes) used by Nways Manager-LAN to poll the agent and update database information on the status of token-ring resources managed by the agent. Each polling gathers information only from the token-ring resources that were reported during the last resynchronization.
Manage this agent	Specify whether or not you want this agent to be discovered by Nways Manager-LAN. This setting is useful when more than one type of SNMP proxy agent manages the same token-ring segment. For example, you can disable one agent in order to allow the other agent to manage the segment. In this way, you can have an agent with lower priority manage a segment that is also discovered by an agent with higher priority. The priority in which token-ring SNMP agents are discovered is: a. Token-ring surrogate b. RMON c. SNMP-managed 8230

For RMON agents, you must also define the following parameter:

RMON agent MAC address display policy
Format in which MAC address of the agent is reported. Valid values: canonical or non-canonical (default).

9. To activate changes made to any of the parameters, press Enter or select **OK** and then do one of the following:
   - Stop and restart the lnmtrmon daemon by entering the following commands:

     ```
     /usr/CML/bin/cmlstop lnmtrmon
     /usr/CML/bin/cmlstart lnmtrmon
     ```

   - Delete and then rediscover the agent by entering the commands:

     ```
     cml_agent_delete <agent_IP_address>
     cml_agent_add <agent_IP_address>
     ```

10. If necessary, repeat steps 4 through 9 for each Token-Ring SNMP proxy agent in your network.

Configuring SNMP Agents that Manage SNMP Bridges

You use SMIT to modify parameters related to the SNMP Bridge application; for example, you can:

- Change the operating parameters of the bridge application.
- Add, change, or delete the label that identifies a bridge subnet.

For information about how to define SNMP bridges that can be discovered by Nways Manager-LAN, see the online book **Coupling and Autodiscovery**.

Editing SNMP Bridge Parameters

Using SMIT, you can modify parameters such as the resync interval, polling interval, and the bridge discovery period for the SNMP bridges in your network. To edit the configuration parameters of SNMP bridges, follow these steps:

1. Ensure you are logged on with root privileges.
2. If SMIT is not running, enter **smit cml** from an AIX operating system shell, or select **Administer -> Campus Manager SMIT** from the NetView for AIX menu bar.

   The SMIT menu is displayed.
3. Select **Configure**.
4. Select **Configure SNMP bridge capability**.
5. Select **Edit bridge parameters**. The Edit Bridge Parameters menu is displayed.
6. Enter new values for any of the following SNMP bridge parameters. To display help information about a parameter, click on **?** and point to the field.

   Resync interval
   Time period (in days, hours, minutes) used by Nways Manager-LAN to check the status and verify the connections between bridges and segments, and then update LAN submaps with new or changed information. Each resynchronziation refreshes LAN submaps with

	the latest changes made to the network topology (for example, moving, adding, or removing SNMP bridges).
Polling interval	Time period (in days, hours, minutes) used by Nways Manager-LAN to poll SNMP bridge agents and update database information on the status of bridges managed by the agents. Each polling gathers information only from the SNMP bridges reported during the last resynchronization.
Discovery period	Time period used by Nways Manager-LAN to discover SNMP bridges and refresh network views containing bridges. For large networks, ensure that this value is large enough to allow all SNMP bridges to be discovered before Nways Manager-LAN redraws the submaps.

7. Press Enter or select **OK** to activate your changes.
8. Select **Exit SMIT** from the Exit pull-down menu to leave the SMIT program.

Adding, Changing, and Deleting SNMP Bridge Subnet Labels

Each LAN Network Manager bridge subnet icon is identified with a subnet label. The default subnet label LAN Network Manager uses is the hexadecimal bridge identifier, which is composed of a priority field and the MAC address of the designated root bridge of the subnet. To add or change the label for a SNMP bridge subnet, follow these steps:

1. Ensure you are logged on with root privileges.
2. If SMIT is not running, enter **smit cml** from an AIX operating system shell, or select **Administer -> Campus Manager SMIT** from the NetView for AIX menu bar.

   The SMIT menu is displayed.
3. Select **Configure**.
4. Select **Configure SNMP bridge capability**.
5. Select **Add/Change bridge subnet labels**.
6. In the MIB-defined designated root label field, enter the label that is currently displayed as the label for the subnet you want to change. Then press Enter or select **OK**.

   The User defined designated root label field is displayed.
7. Enter the new label for the subnet in the User defined designated root label field.
8. Press Enter or select **OK** to save your changes.
9. Select **Exit SMIT** from the Exit pull-down menu to leave the SMIT program.

The new or modified subnet label is displayed with the subnet icon the next time LAN Network Manager is restarted

Chapter 31. Managing SNMP Token-Ring and SNMP Bridge Networks

LAN Network Manager works with the SNMP agent resources and the NetView for AIX program to enable you to monitor and manage SNMP token-ring resources. LAN Network Manager communicates with several agent resources in the SNMP token-ring network to retrieve configuration information and to send management instructions to stations. In addition, LAN Network Manager shows the connectivity between SNMP-managed bridges and other network environments, such as X.25, Frame Relay, Ethernet, and FDDI. LAN Network Manager enables you to perform token-ring network management tasks by selecting a token-ring resource from a topological view of your network and then use menu choices to perform a specific management task.

This chapter describes the following topics:

Understanding the SNMP Token-Ring and Bridge Applications

In addition to managing LLC-based token-ring networks, LAN Network Manager also manages token-ring networks that communicate through the Simple Network Management Protocol (SNMP). LAN Network Manager uses two of its applications, the SNMP bridge application and the SNMP token-ring application, to manage the token-ring segments in the networks and the SNMP devices that interconnect them.

The SNMP token-ring application reports dynamic status changes on the token-ring network and enables LAN Network Manager to retrieve station information and set management parameters. LAN Network Manager receives its configuration information about the token-ring resources from the following SNMP proxy agents:

- Token-ring surrogate agents that implement the AWP 7607 MIB (IBM private MIB), such as the IBM 8229 bridge and the IBM 8260 TMAC
- Remote monitor agents that implement the RFC 1513 MIB, such as the IBM 8260 TMAC
- Concentrator agents that implement the IBM 8230 MIB, such as the IBM 8230 Controlled Access Unit Model 3

The SNMP bridge application provides LAN Network Manager with the management of the SNMP bridging devices and shows the connectivity of the bridges to other environments, such as X.25, Frame Relay, Ethernet, and FDDI. The SNMP bridge application notifies LAN Network Manager of status changes in the SNMP bridges and relays management instructions from LAN Network Manager to the bridges.

LAN Network Manager manages several types of bridges through the SNMP bridge application:

- Source-routing bridges
- Transparent bridges
- Source-route transparent bridges
- Bridges that function as both source-routing and transparent bridges, such as the IBM 6611 Network Processor
- Translational bridges that act as a gateway between a source-routing and a transparent bridge network (the IBM 8229 Bridge, for example)

The SNMP bridge application obtains resource information from agent resources that implement the RFC 1493 and RCF 1213 (MIB II), or RCF 1286 and RCF 1213 (MIB II).

SNMP Agents

LAN Network Manager communicates with several agent resources in the SNMP token-ring networks to retrieve configuration information and to send management instructions to stations. These agents vary depending on whether the information pertains to a segment or station or to an SNMP bridge.

Token-ring segment information is acquired from the following kinds of agents:

- Token-ring surrogate agents that implement the AWP 7607 MIB, such as the IBM 8229
- Remote monitor (RMON) agents that implement the RFC 1513 MIB, such as the IBM 8260 TMAC
- Concentrator agents that implement the IBM 8230 MIB, such as the IBM 8230 Controlled Access Unit Model 3.

LAN Network Manager manages SNMP bridges through agents that are resident in the bridging devices. LAN Network Manager supports those agents that implement either RFC 1286 and RFC 1213 (MIB II), or RFC 1213 (MIB II) and RFC 1493. LAN Network Manager can also provide information from agents that support the following MIBs:

RFC 1231 IEEE Token-Ring 802.5 MIB

RFC 1232 DS1 Interface Type MIB

RFC 1315 Frame Relay DTE MIB

RFC 1317 RS-232-like Hardware Device MIB

RFC 1381 SNMP MIB Extension for X.25 LAPB

RFC 1382 SNMP MIB Extension for the X.25 Packet Layer

RFC 1398 Ethernet-like Interface Types MIB

Resynchronizing SNMP Subnets

To maintain an accurate network configuration, LAN Network Manager periodically resynchronizes the submaps of your network. The SNMP token-ring network and SNMP bridge subnets are resynchronized separately.

Resynchronization of an SNMP token-ring network consists of rediscovering the SNMP agents that you defined using the Add/Change IBM token-ring SNMP proxy agent menu in SMIT. As the agents are rediscovered, the appropriate LAN Network Manager submaps are refreshed.

Resynchronization of SNMP bridges consists of rediscovering the bridges that you specified to be automatically discovered on the Add Bridges to be Automatically Discovered menu in SMIT. As the bridges are rediscovered, the appropriate LAN Network Manager submaps are refreshed. This allows LAN Network Manager to redraw an up-to-date topology of bridges and switches that interconnect networks and takes into account the last physical moves and configuration changes made to network devices.

By default, LAN Network Manager automatically resynchronizes the SNMP token-ring network every hour and SNMP bridges every 4 hours. To reset the automatic resynchronization to a different time interval, enter a new value for **Resync interval** as follows:

- To reset the resync interval for all SNMP bridges, select **Administer -> Campus Manager SMIT** to start SMIT and then **Configure -> Configure SNMP bridge capability -> Edit bridge parameters**.
- To reset the resync interval for individual SNMP token-ring agents, select **Administer -> Campus Manager SMIT** to start SMIT and then **Configure -> Configure SNMP token-ring capability -> Configure IBM SNMP token-ring proxy agent**. Select the type of proxy agent and enter its IP address.

Also, you can manually resynchronize the SNMP token-ring network or SNMP bridges at any time.

For information about:	Read:
Resynchronizing SNMP token-ring network	“SNMP Token-Ring Subnets”
Resynchronizing an SNMP Bridge subnet	“SNMP Bridge Subnets” on page 278

SNMP Token-Ring Subnets

To ensure that the SNMP token-ring configuration displayed by LAN Network Manager is accurate at any time, manually resynchronize the token-ring network. Resynchronizing causes LAN Network Manager to rediscover the SNMP token-ring agents you have defined and to update LAN Network Manager submaps as necessary. You can also resynchronize a single token-ring segment. See “Resynchronizing an SNMP Segment” on page 285 for more information.

To manually resynchronize the SNMP token-ring network, follow these steps:

1. Select **Applications** from the LAN pull-down menu.
2. Select **SNMP Token-Ring** from the Applications cascade menu.
3. Select **Resync all** from the SNMP Token-Ring cascade menu.

   Information windows inform you when the resynchronization is started and when it is completed.

SNMP Bridge Subnets

To ensure that the SNMP bridge configuration displayed by LAN Network Manager in an SNMP bridge subnet is accurate at any time, manually resynchronize the subnet. Resynchronizing causes LAN Network Manager to rediscover the bridges you have defined to be automatically discovered and to update LAN Network Manager submaps as necessary.

To manually resynchronize an SNMP Bridge subnet, follow these steps:

1. Select the subnet.
2. Select **Applications** from the LAN pull-down menu.
3. Select **SNMP Bridge** from the Applications cascade menu.
4. Select **Resync** from the SNMP Bridge cascade menu.

   Information windows inform you when the resynchronization is started and when it is completed.

Defining SNMP Bridge Parameters

The LNM for AIX SNMP Bridge Configuration window displays the parameters that control bridge resynchronization, polling, and discovery. You can adjust these values to ensure quick notification of errors and timely updates on the status and connections of the bridges.

To display the LNM for AIX SNMP Bridge Configuration window, follow these steps:

1. Select **Applications** from the LAN pull-down menu.
2. Select **SNMP Bridge** from the Applications cascade menu.
3. Select **Parameters** from the SNMP Bridge cascade menu.

   The LNM for AIX SNMP Bridge Configuration window is displayed.
4. Use the slider bars to change the current values of the fields.
5. Select **OK** to save the changes and close the window.

Defining SNMP Token-Ring Access Control Parameters

Set a general access control policy for all SNMP segments and concentrators managed by the SNMP token-ring application using the SNMP Token-Ring Application - Access Control Policy window. This window enables you to specify whether access control is active, whether the general policy should overwrite resource specific access control parameters, and the conditions under which adapters are removed or disabled.

For segments, an adapter is removed from the segment if that adapter violates the access control conditions you have selected and access control for that segment is active. For concentrators, a port is disabled if the adapter violates the access control conditions you have selected and access control for that concentrator is active.

For a segment, an adapter attached to a segment can be removed if the adapter is:

- Unknown to the segment
- Inserted at an unauthorized date or time

For a concentrator, the port for an adapter attached to a concentrator can be disabled if the adapter is:

- Unknown to the concentrator
- Known to the concentrator but inserted in an unassigned port
- Inserted at an unauthorized date or time

On the SNMP Token-Ring Application - Access Control Policy window, you define an access control policy that applies to all segments and concentrators managed by the SNMP token-ring application. You can also define access control settings for individual segments using the Segment Configuration - Access Control window (described in “Access Control Information” on page 283),and define access control settings for individual concentrators using the Concentrator Configuration - Access Control window.

Specify whether you want any changes that you make to the general access control policy to overwrite the settings for individual segments or concentrators by selecting **Yes** in the Overwrite resource specific field on the SNMP Token-Ring Application - Access Control Policy window. If you select **No** in the Overwrite resource specific field, the access control settings you specify for individual segments and concentrators are not affected by changes you make to the general policy on the specific Configuration - Access Control window. If you have not defined the settings for a specific segment or concentrator, the general access control policy is used for that segment or concentrator.

Note that due to the way the RMON standard is defined in RFC 1513, when you define access control parameters for a segment being managed by an RMON agent, the access control policy is only enforced when the segment is resynchronized. This means that, for RMON segments only, unauthorized adapters remain inserted on a segment until the segment is resynchronized, either manually or at the resync interval defined for the agent in SMIT (the default resync interval is 1 hour). To reduce the time an unauthorized adapter remains on a segment, lower the resynchronization interval for the RMON agent. To ensure that unauthorized adapters are immediately removed from a segment, manually resynchronize the segment.

To display the SNMP Token-Ring Application - Access Control Policy window, follow these steps:

1. Select **SNMP token-ring** from the Applications cascade menu on the LAN pull-down menu.
2. Select **Access Control Policy** from the SNMP token-ring cascade menu.

   The SNMP Token-Ring Application - Access Control Policy window is displayed.

   On this window, specify the conditions under which an adapter should be removed from a segment and the conditions under which a port should be disabled from a concentrator.
3. Set access control to be **Active** or **Inactive**.
4. Specify whether you want the access control settings you define on this window to overwrite access control settings you have previously defined for individual segments and concentrators. If you select **Yes**, the general access control policy you define applies to all SNMP segments and concentrators.
5. Specify the access control conditions for the selected subnet.

   When access control is **active**, LAN Network Manager immediately records the current network configuration. This configuration is used to determine whether unauthorized adapters have attempted to enter the network. Adapters that are in the network at the time access control is made active are considered authorized.
6. Select **OK** to save the changes and close the window.

Chapter 32. Managing SNMP Segments and Stations

Using its SNMP token-ring application to communicate with SNMP proxy agents, LAN Network Manager monitors activity on SNMP segments and the stations inserted on those segments. This chapter describes how to monitor and manage the segments and stations in your network.

Displaying SNMP Segments Graphically

You manage your SNMP token-ring segments by monitoring their status on the LAN Network and Segment submaps and by accessing information about them using the segment management windows.

The LAN Network submap provides a detailed view of a particular subnet that LAN Network Manager manages. The different types of LAN segments, such as token-ring and FDDI, are represented with icons, along with the bridging devices that provide their connectivity.

SNMP segments are represented by an ring icon in the LAN Network submap.

To access management windows that provide profile, fault, and performance information for a segment, click on a segment icon with mouse button 3, select **LAN**, and then select a menu choice from the context menu. Actions available from these management windows enable you to resynchronize the segment and set access control parameters.

Double-click on a specific segment in the LAN Network submap to open a Segment submap. The Segment submap shows a detailed view of the segment resources. Stations and SNMP-managed 8230 concentrators are displayed in nearest active upstream neighbor (NAUN) order, according to their adapters.

From the Segment submap, you can determine the current status of a resource by its color, use management windows to obtain profile, configuration, fault, and performance information for a resource, and navigate to other submaps for a detailed view of a particular resource.

The merging function of LAN Network Manager enables LAN Network Manager to combine overlapping views of SNMP segments that are being monitored by more that one SNMP agent. The merging function simplifies the graphical representation of the network and makes the job of managing it easier.

If you have SNMP-managed bridges in your network, along with your SNMP agent programs, the merging function integrates the information provided by both the bridge

and segment agents. If LAN Network Manager recognizes a segment that is attached to a bridge, the Segment submap is moved to the Bridge submap, so that you can access information about the bridge and the segment from the same submap.

Note: An overlapping surrogate or RMON agent is required for an SNMP-managed 8230 to be merged within a bridge submap.

You can also navigate to a view of the segment stations from the Bridge submap.

Displaying Segment Information

View and change specific information about SNMP segments using the SNMP segment profile, configuration, fault, and performance management windows. To display a segment management window, select a segment from the LAN Network submap and then select the type of information you want to display from the LAN pull-down or LAN context menu.

For information about:	Read:
Segment profile	"Segment Profile Information"
Segment configuration	"Segment Configuration Information"
Segment fault	"Displaying Segment Fault Information" on page 285
Segment performance	"Displaying Segment Performance Information" on page 285

Segment Profile Information

Display information about a segment on the Segment Profile window. This window displays general information about the token-ring segment and the proxy agent it communicates with, as well as basic information about the activity on that segment.

To display the profile information for a segment, select the segment, then select **Profile** from either the LAN pull-down menu or the context menu.

Segment Configuration Information

Display and change configuration information for a segment on the Segment Configuration window. This window contains a field for you to enter information about who to contact for problems with the segment and, for proxy agents that support AWP 7607, allows you to control whether Ring Error Monitoring (REM) is enabled for the segment.

To view or change access control information for the segment, select the **Access control** push button on the Segment Configuration window.

To display the configuration information for a segment, select the segment, then select **Configuration** from either the LAN pull-down menu or the context menu.

For information about:	Read:
Access control	“Access Control Information”
Adding authorized MAC addresses	“Adding Authorized MAC Addresses” on page 284
Removing access to a segment	“Removing Network Access” on page 284
Resync	“Resynchronizing an SNMP Segment” on page 285

Access Control Information

Set access control parameters for a specific segment on the Segment Configuration - Access Control window. Using this window, you can make access control **active** or **inactive** for this segment and specify the conditions under which an adapter should be removed from the segment.

The access control settings in the Segment Configuration - Access Control window override the general policy defined on the SNMP Token-Ring Application - Access Control Policy window. For example, assume you have set access control to be active for all segments on the SNMP Token-Ring Application - Access Control Policy window and you select the **Unknown to segment** condition. If you then set access control to be inactive for segment 005 on the Segment Configuration - Access Control window, adapters will not be removed from segment 005, even if they are unknown to that segment. See “Defining SNMP Token-Ring Access Control Parameters” on page 279 for more information.

The access control settings of individual segments are overwritten by changes to the general access control policy if the Overwrite resource specific field on the SNMP Token-Ring Application - Access Control Policy window (described in “Access Control Information”) is set to **Yes**. To ensure that the settings you define on the Segment Configuration - Access Control window are used even if the general access control policy is changed on the SNMP Token-Ring Application - Access Control Policy window, the Overwrite resource specific field on the SNMP Token-Ring Application - Access Control Policy window should be set to **No**.

Note that due to the way the RMON standard is defined in RFC 1513, when you define access control parameters for a segment being managed by an RMON agent, the policy is only enforced when the segment is resynchronized. This means that, for RMON segments only, unauthorized adapters remain inserted on a segment until the segment is resynchronized, either manually or at the resync interval defined for the agent in SMIT (the default resync interval is 1 hour). To ensure that unauthorized adapters are immediately removed from a segment, manually resynchronize the segment.

To display the Segment Configuration - Access Control window, follow these steps:

1. Select the segment for which you want to specify access control parameters.
2. Select **Configuration** from the LAN pull-down or context menu.
   The Segment Configuration window is displayed.
3. Select the **Access control** push button from the Segment Configuration window.

The Segment Configuration - Access Control window is displayed.

4. Specify the access control conditions for the selected segment.
5. Set access control to be active or inactive.

   When access control is **active**, LAN Network Manager immediately records the current configuration of the segment. Any adapter that is not attached to the segment at the time access control is made active is considered unauthorized.
6. Select **OK** to save the changes and close the window.

Adding Authorized MAC Addresses

From the Segment Configuration - Access Control window, you can add new MAC addresses to the list of MAC addresses authorized to access the segment. This allows you to attach new stations to the segment without having to turn off security by de-activating access control.

To add a MAC addresses to the list of authorized MAC addresses, follow these steps:

1. Display the Segment Configuration - Access Control window as described in "Access Control Information" on page 283. Make sure that access control is **active**.
2. Select **Add/Remove Authorized MAC Address**.
3. Enter the new MAC address that you want to add to the list and select **Add MAC**.

Removing Network Access

You can remove access to an SNMP segment for a token-ring resource by deleting the resource's MAC address from the list of authorized MAC addresses. To do so, follow these steps:

1. Display the Segment Configuration - Access Control window as described in "Access Control Information" on page 283. Make sure that access control is **active**.
2. Select **Add/Remove Authorized MAC Address**.
3. Select the resource's MAC address in the list of authorized MAC addresses.
4. Select **Remove**.

This removes the resource from the list of authorized MAC addresses, but not from the SNMP segment. The resource continues to send and receive token-ring frames.

To remove the resource from the SNMP segment, manually resynchronize the segment as described in "Resynchronizing an SNMP Segment" on page 285 or follow these steps:

1. Select the resource in an SNMP token-ring segment submap.
2. Select **Configuration** from either the LAN pull-down menu or the context menu.
3. In the Station Configuration panel, select **Remove Station** from the Actions pull-down menu.

This removes the resource from the segment.

Resynchronizing an SNMP Segment

To ensure the configuration for a segment is accurate, manually resynchronize the segment. When you resynchronize a segment, LAN Network Manager queries each adapter, updates the database with current information, and refreshes the Segment submap. To resynchronize a segment, select **Resync** from the Actions pull-down menu on the Segment Configuration window.

Displaying Segment Fault Information

Fault information for a segment is displayed on the Segment Fault window. This window displays the status of the segment and provides data for the fault domain and the soft errors on the segment.

To display the fault information for a segment, select the segment, then select **Fault** from either the LAN pull-down menu or the context menu.

To display additional information about the soft errors, select the **Soft error table** push button on the Segment Fault window.

To display additional information about the ring maintenance activity on the segment, select the **Ring maintenance activity table** push button on the Segment Fault window.

Soft Error Information

The Segment Fault - Soft Error window displays detailed information about the soft errors that are occurring on the selected segment. Soft errors are intermittent errors on a network that cause data to have to be transmitted more than once to be received.

To display the Segment Fault - Soft Error window, select the **Soft error table** push button from the Segment Fault window.

Maintenance Activity Information

The Segment Fault - Maintenance Activity window displays information about administrative activity occurring on the segment. The statistics on this window detail such activity as the number of times active monitor negotiation has taken place and the number of times the claim-token process was performed.

To display the Segment Fault - Maintenance Activity window, select the **Ring maintenance activity table** push button from the Segment Fault window.

Displaying Segment Performance Information

Performance information for a segment is displayed on the Segment Performance window. This window displays the ring utilization for the selected segment. Ring utilization is the percentage of the total data-transmission capacity of the segment that is currently being utilized.

To display the performance information for a segment, select the segment, then select **Performance** from either the LAN pull-down menu or the context menu.

Displaying SNMP Stations Graphically

You manage token-ring stations by monitoring the status of the stations on the Segment submap and by accessing information about the stations using the station management windows.

The Segment submap shows the adapter name and current status of each station on a segment, and you can obtain more information about a particular station using the profile and configuration menu choices.

Double-clicking on a station in a submap displays the Node submap. The Node submap represents the contents of the selected resource, according to protocol. The icons in the submap show which protocols are present in the resource elements.

Displaying Station Information

View and change specific information about SNMP stations using the SNMP station profile, configuration, and fault management windows. To display a station management window, select a station from the Segment submap and then select the type of information you want to display from the LAN pull-down or LAN context menu.

For information about:	Read:
Station profile	“Station Profile Information”
Station configuration	“Station Configuration Information”
Station fault	“Station Fault Information” on page 287

Station Profile Information

Basic information for a station is displayed on the Station Profile window. This window contains information identifying the adapter in the station, information about the operation of the station, and data describing how the station is attached to the segment.

To display information about how the station is physically attached to the network, select the **Attachment data** push button on the Station Profile window.

To display the profile information for a station, select the station, then select **Profile** from either the LAN pull-down menu or the context menu.

Station Configuration Information

The Station Configuration window enables you to control aspects of a station’s configuration. You can indicate whether a station should be monitored and specify the days and times that the station is allowed to access the ring.

To display information about how the station is physically attached to the network, select the **Attachment data** push button on the Station Configuration window.

To display the configuration information for a station, select the station, then select **Configuration** from either the LAN pull-down menu or the context menu.

Station Fault Information

Fault information for a station is displayed on the Station Fault window. This window contains data related to the fault conditions on the station.

To display the fault information for a station, select the station, then select **Fault** from either the LAN pull-down menu or the context menu.

Chapter 33. Managing SNMP Bridges

LAN Network Manager enables you to manage SNMP bridges that interconnect segments. LAN Network Manager uses its SNMP bridge application to send bridge management instructions and to receive bridge status changes. LAN Network Manager manages bridges that support RFC 1286 or 1493, and RFC 1213 (MIB II), such as the IBM 8229, the 8250, the 6611, 8281, and OEM bridges. In addition to bridges, switches that implement the bridge MIB (1493) also can be managed. You can display a submap showing a graphical representation of a bridge, and display profile, configuration, fault, and performance information for bridges, bridge interfaces, and bridge ports.

Specifically, this chapter describes:

SNMP Bridge Discovery

SNMP bridges are discovered in the following ways when LAN Network Manager is started:

- You can define the bridges that you want to be discovered by specifying the IP addresses in SMIT. To do so, start SMIT and select **Nways Campus Manager -> Configure -> Nways Campus Manager general configuration -> Add an IP address for forced discovery**.
- You can allow bridges to be automatically discovered by the autodiscovery function of Nways Manager-LAN. See the online book **Coupling and Autodiscovery** for more information about how to define bridges for autodiscovery.

As bridges are discovered, they are placed into various subnets, which show the bridges and the segments that they interconnect. The subnets they are put into depend on the characteristics of the bridge, its current status, and its spanning tree.

A new subnet is created if the bridge is in the spanning tree of a root bridge that has not been discovered. If the bridge is part of the spanning tree of a discovered root bridge, it is put into that bridge's subnet. When a bridge is not part of an active spanning tree, it is put into a standalone subnet, which contains one or more standalone bridges.

If a bridge cannot be discovered due to SNMP errors, the bridge is placed with other undiscovered bridges into a submap called Undiscovered Bridges. The status color of all undiscovered bridges in the Undiscovered Bridges submap is blue. If LAN Network Manager is later able to discover a bridge that is in the Undiscovered Bridges submap,

for instance when polling the network, it is removed from the Undiscovered Submap and placed in the appropriate SNMP bridge subnet.

Displaying SNMP Bridges

The SNMP bridges in your network are displayed in the LAN Subnet submap. Each Subnet submap contains bridges in a particular spanning tree, and the segments which the bridges interconnect. The status of the bridges and segments are indicated by the color of their icon.

In some cases, a Subnet submap might show bridges and segments that are not connected.

In this case, Bridge 2 is put into the Undiscovered Bridges submap until LAN Network Manager is able to discover it.

Double-clicking on a bridge icon in the LAN Subnet submap displays a Bridge submap for that bridge.

The Bridge submap shows a graphical representation of the bridge with icons representing the bridge and the bridge interfaces of that bridge. Double-clicking on one of the interface icons displays an interface submap of an interface and the port or ports it is operating on. Read “Displaying SNMP Bridge Interfaces and Ports” on page 291 for more information about bridge interfaces and ports.

To display management windows for a bridge, select a bridge icon from the LAN Subnet submap or Bridge submap and select an action from the LAN pull-down or LAN context menu. Depending on the type of bridge, you can display and change profile, configuration, fault, and performance information for the bridge through the management information windows.

The merging function of LAN Network Manager simplifies the graphical representation of the network by combining overlapping views provided by different SNMP-managed agents. If you have SNMP agent programs in your network, such as token-ring surrogate and RMON agents, the merging function integrates the information provided by these SNMP agents with information maintained by your SNMP-managed bridges. If LAN Network Manager recognizes a segment that is attached to a bridge, the Segment submap is moved to the Bridge submap, so that you can access information about the bridge and the segment from the same submap. You can also navigate to a view of the segment stations from the Bridge submap.

Displaying SNMP Bridge Interfaces and Ports

When you double-click on a interface icon in the Bridge submap, the Interface submap for that interface is displayed.

The interface submap contains port and interface icons.

The port icon represents the port or ports the selected bridge interface is operating on. Depending on the type of bridge, the following types of bridge ports can be displayed:

- Source route
- Transparent bridging
- Source route transparent

If the selected interface is operating on more than one port, an icon for each port is displayed in the Interface submap.

The interface icon represents a specific interface that is operating on the bridge. Depending on the type of bridge you have selected, the following types of bridge interfaces can be displayed:

- X.25 LAPB
- X.25 packet
- DS1
- Frame relay
- Token-ring
- Ethernet

Most of these interfaces are associated with a single bridge port. For frame relay and X.25 interfaces, more than one port can be associated with each interface.

Double-click on an interface icon in the Interface submap to display a node submap for the interface. This is similar to the Interface submap except that an icon is displayed for the interface, but not for the bridge ports. You can perform protocol-switching from either the interface or node submaps in the following ways:

- Select **View -> Nways -> Nways Protocols** from the NetView for AIX menu bar.
- Select **Nways Protocols** from the context menu of the interface or node.

To display management windows for a bridge interface, select an interface icon from the Bridge submap, the Interface submap, or the Node submap and then select an action from the LAN pull-down or LAN context menu. To display management windows for a bridge port, select the port icon from the Interface submap. Depending on the type of interface or port you select, you can display and change profile, configuration, fault, and performance information for the interface or port through the management information windows.

Displaying SNMP Bridge Information

View and change specific information about SNMP bridges using the SNMP bridge profile, configuration, fault, and performance management windows. The exact type of information displayed on each of these windows varies depending on the type of bridge you have selected.

For information about:	Read:
Bridge profile	“Bridge Profile Information”
Bridge configuration	“Bridge Configuration Information”
Bridge fault	“Bridge Fault Information” on page 294
Bridge performance	“Bridge Performance Information” on page 293

Bridge Profile Information

Profile information for a selected bridge is displayed on the Bridge Profile window. This window displays a description of the bridge and contains fields that enable you to provide information about the name, location, and contact person for the bridge.

To poll the selected bridge, select **Poll** from the Actions pull-down menu on the Bridge Profile window. Read “Polling a Bridge” for more information.

To display the profile information for a bridge, select the bridge, then select **Profile** from either the LAN pull-down menu or the context menu.

You can display profile information for any type of SNMP bridge.

Polling a Bridge

To poll a selected bridge, select **Poll** from the Actions pull-down menu on the Bridge Profile, Configuration, or Fault windows. When you select **Poll**, LAN Network Manager checks the status of the selected bridge. If the bridge is down, LAN Network Manager rediscovers the bridge.

LAN Network Manager also automatically polls all bridges at the defined polling interval, which you can set when you configure the SNMP bridge application. The default polling interval is 5 minutes.

Bridge Configuration Information

Display and change basic information for a bridge on the Bridge Configuration window. This window displays information about the type of bridge and the protocol the bridge is using.

To poll the selected bridge, select **Poll** from the Actions pull-down menu on the Bridge Configuration window. Read “Polling a Bridge” for more information.

To display the configuration information for a bridge, select the bridge, then select **Configuration** from either the LAN pull-down menu or the context menu.

To display a window with more information about the bridge spanning tree, select the **Spanning tree** push button.

To start a user-defined device configuration program, select the **Device configuration** push button. When you select the **Device configuration** push button, an AIX script file called lnmbrdevcfg (provided with LAN Network Manager) is called. By customizing the contents of this script file, you can use it to invoke device-specific configuration programs that you might already use to set up specific bridges.

For more information about starting a user-defined configuration program, see the `lnmbrdevcfg` file in the `/usr/CML/bin` directory.

Bridge Spanning Tree Configuration Information

The Bridge Spanning Tree window displays information related to the spanning tree for the selected bridge. In addition, you can modify the values for other parameters that affect the bridge and the selected spanning tree.

To display spanning tree information for a bridge, select the **Spanning tree** push button from the Bridge Configuration window.

Bridge Performance Information

Performance information for a bridge is displayed on the Bridge Performance window. The performance information displayed on this window depends on the type of bridge you have selected. Each window includes data that indicates how well the selected bridge is performing.

You can display the following types of bridge performance windows:

Source Route Performance

The Source Route Performance window displays information about the performance of the selected source route bridge. Performance is described in terms of frames transmitted, received, the total number of frames, and the frame ratio.

To display the source route performance information for a bridge, select the bridge, then select **Performance** from either the LAN pull-down menu or the context menu.

To display additional information about the bridge traffic for the selected bridge, select the **Traffic analysis** push button.

Transparent Bridging Performance

The Transparent Bridging Performance window displays information about the performance of the selected transparent bridge.

Performance is described in terms of frames transmitted, received, the total number of frames, and the frame ratio.

To display the transparent bridging performance information for a bridge, select the bridge, then select **Performance** from either the LAN pull-down menu or the context menu.

Source Route Transparent Bridge Performance

The Source Route Transparent Bridging Performance window displays information about the performance of the selected source route transparent bridge. Performance is described in terms of frames transmitted, received, the total number of frames, and the frame ratio.

To display performance information for a source route transparent bridge, select the bridge, then select **Performance** from either the LAN pull-down menu or the context menu.

Source Route Traffic Analysis Information

The Source Route Traffic Analysis window displays traffic statistics for the selected source route bridge. The statistics provided on this window are the number of frames received and transmitted for specifically routed traffic, path explorer traffic, and spanning tree explorer traffic.

To display traffic analysis information for a source route bridge, select the **Traffic analysis** push button from the Source Route Performance window.

Bridge Fault Information

Basic fault information for a selected bridge is displayed on the General Fault window. This window displays information about the frames discarded by the selected bridge, including the ratio of discarded frames to total traffic.

Select the **Type specific** push button from the General Fault window to display additional fault information for the bridge you selected.

To poll the selected bridge, select **Poll** from the Actions pull-down menu on the Bridge Fault window. Read “Polling a Bridge” on page 292 for more information.

To display general fault information for a bridge, select the bridge, then select **Fault** from either the LAN pull-down menu or the context menu. The General Fault window is displayed.

You can display the following types of bridge fault windows by selecting the **Type specific** push button on the General Fault:

Source Route Fault

The Source Route Fault window displays the number of discarded frames for the selected bridge, categorized by the reason the frames were discarded. The window also displays the ratio of discarded frames to total traffic.

Transparent Bridging Fault

The Transparent Bridging Fault window displays the number of discarded frames for the selected transparent bridge, categorized by the reason the frames were discarded. The window also displays the ratio of discarded frames to total traffic.

Source Route Transparent Fault

The Source Route Transparent Bridging Fault window displays the number of discarded frames for the selected source route transparent bridge, categorized by the reason the frames were discarded. The window also displays the ratio of discarded frames to total traffic.

Displaying SNMP Bridge Interface and Port Information

View and change specific information about SNMP bridge interfaces and ports using the SNMP bridge interface and port management windows. Information about your SNMP bridge interfaces and ports is displayed on the profile, configuration, fault, and performance windows. The exact type of information displayed on each of these windows varies depending on the type of bridge interface or port you have selected.

For information about:	Read:
Bridge port profile	"Bridge Port Profile"
Bridge interface and port configuration	"Bridge Port and Interface Configuration Information"
Bridge port fault	"Bridge Port Fault Information" on page 298
Bridge interface fault	"Bridge Interface Fault Information" on page 299
Bridge interface and port performance	"Bridge Interface and Port Performance Information" on page 300

Bridge Port Profile

Profile information for a selected bridge port is displayed on the Port Profile window. This window displays information about the bridge port such as the type and address of the port interface, whether the port is currently operational, and statistics related to the traffic that is passing through the port. In addition, for bridges that support the set function, you can select the port state.

Bridge Port and Interface Configuration Information

To display and change basic information for bridge ports and bridge interfaces, use the Port or Interface Configuration windows.

For source route ports, you can also display a window with more information about the bridge port spanning tree by selecting the **Spanning tree** push button from the Port Source Route window.

You can display the following types of bridge port and bridge interface configuration windows:

Source Route Configuration

Configuration information for the selected source route bridge port is displayed on the Port Source Route Configuration window.

To display the configuration information for a source route port, select the source route port, then select **Configuration** from either the LAN pull-down menu or the context menu.

To display information about the bridge spanning tree, select the **Spanning tree** push button from the Port Source Route Configuration window.

Transparent Bridge Configuration

Configuration information for the selected transparent bridge port is displayed on the Transparent Configuration window.

To display the configuration information for a transparent bridge port, select the transparent bridge port, then select **Configuration** from either the LAN pull-down menu or the context menu.

To display information about the bridge spanning tree, select the **Spanning tree** push button from the Transparent Configuration window.

Source Route Transparent Configuration

Configuration information for the selected source route transparent bridge port is displayed in the Source Route Transparent Configuration window.

To display the configuration information for a source route transparent port, select the source route transparent port, then select **Configuration** from either the LAN pull-down menu or the context menu.

To display information about the bridge spanning tree, select the **Spanning tree** push button from the Source Route Transparent Configuration window.

X.25 Packet Interface Configuration

Configuration information for an X.25 packet bridge interface is displayed on the X.25 Packet Interface Configuration window. You can also open the following windows from the X.25 Packet Interface Configuration window:

- X.25 Packet Circuit Configuration
- X.25 Packet Cleared Circuit

- X.25 Packet Call Parameters
- X.25 LAPB Interface Configuration

To display the X.25 packet configuration information for an X.25 bridge interface, select the X.25 bridge interface, then select **Configuration** from either the LAN pull-down menu or the context menu.

X.25 Packet Circuit Configuration

Configuration information for a specific X.25 packet bridge interface circuit is displayed on the X.25 Packet Interface Circuit Configuration window.

To display the X.25 packet circuit configuration information for an X.25 bridge interface, select an X.25 channel from the Circuit listbox on the X.25 Packet Interface Configuration window, and then select the **Select** push button next to the listbox. The X.25 Packet Circuit Configuration window is displayed.

X.25 Packet Call Parameters

You can display the call parameters for a specific X.25 packet bridge interface using the X.25 Packet Interface Call Parameters window.

To display the X.25 packet call parameters information for an X.25 bridge interface, select an X.25 channel from the Call listbox on the X.25 Packet Interface Configuration window, and then select the **Select** push button next to the listbox. The X.25 Packet Call Parameters window is displayed.

X.25 Packet Cleared Circuit

Information about the cleared circuit for an X.25 packet bridge interface is displayed on the X.25 Packet Interface Cleared Circuit window.

To display the X.25 packet cleared circuit information for an X.25 bridge interface, select an X.25 channel from the Cleared listbox on the X.25 Packet Interface Configuration window, and then select the **Select** push button next to the listbox. The X.25 Packet Cleared Circuit window is displayed.

X.25 LAPB Interface Configuration

To display the X.25 LAPB configuration information for an X.25 bridge interface, select the **LAPB Configuration** push button on the X.25 Packet Interface Configuration window. The X.25 LAPB Interface Configuration window is displayed.

DS1 Interface Configuration

The DS1 Interface Configuration window displays configuration information for the selected DS1 bridge interface.

To display the DS1 configuration information for a DS1 bridge interface, select the DS1 bridge interface, then select **Configuration** from either the LAN pull-down menu or the context menu.

Frame Relay Interface Configuration

Configuration information for the selected frame relay bridge interface is displayed on the Frame Relay Interface Configuration window.

To display the frame relay configuration information for a frame relay bridge interface, select the frame relay bridge interface, then select **Configuration** from either the LAN pull-down menu or the context menu.

Token-Ring Interface Configuration

Basic information for a token-ring bridge interface is displayed on the Token-Ring Interface Configuration window. This window displays general information about the token-ring segment the interface is attached to, as well as information related to timers.

To display the configuration information for a token-ring bridge interface, select the token-ring bridge interface, then select **Configuration** from either the LAN pull-down menu or the context menu.

Port Spanning Tree Configuration Information

The Port Spanning Tree window displays information related to the spanning tree for the selected port. In addition, you can modify the port priority and the path cost for the spanning tree, and select whether the spanning tree is enabled for the selected port.

To display spanning tree information for a port, select the **Spanning tree** push button from the Configuration window of the port.

Bridge Port Fault Information

Basic fault information for a selected bridge port is displayed on the Port General Fault window. This window displays information about the frames discarded by the selected bridge port, including the ratio of discarded frames to total traffic.

In addition, you can select the **Type specific** push button from the Port General Fault window to display additional fault information for the bridge port you selected.

To display general fault information for a bridge port, select the bridge port, then select **Fault** from either the LAN pull-down menu or the context menu. The Port General Fault window is displayed.

You can display the following types of bridge port fault windows by selecting the **Type specific** push button on the General Fault window:

Source Route Port Fault

To display the source route fault information for a bridge port, select the source route bridge port, then select **Fault** from either the LAN pull-down menu or the context menu.

Transparent Bridging Port Fault

To display the transparent bridging fault information for a bridge port, select the transparent bridging port, then select **Fault** from either the LAN pull-down menu or the context menu.

Source Route Transparent Port Fault

To display the fault information for a source route transparent bridge port, select the source route transparent bridge port, then select **Fault** from either the LAN pull-down menu or the context menu.

Bridge Interface Fault Information

Basic fault information for a selected bridge interface is displayed on the Interface Fault windows.

To display fault information for a bridge interface, select the bridge interface, then select **Fault** from either the LAN pull-down menu or the context menu. The fault window for the type of bridge interface you selected is displayed.

You can display the following types of bridge interface fault windows:

X.25 Packet Interface Fault

To display the X.25 packet fault information for an X.25 bridge interface, select the X.25 bridge interface, then select **Fault** from either the LAN pull-down menu or the context menu.

X.25 Packet Circuit Fault

To display the X.25 packet circuit fault information for an X.25 bridge interface, select an X.25 channel from the Circuit listbox on the X.25 Packet Interface Fault window, and then select the **Select** push button next to the listbox. The X.25 Packet Circuit Fault window is displayed.

X.25 LAPB Interface Fault

To display the X.25 LAPB interface fault information for an X.25 bridge interface, select the **LAPB Fault** push button on the X.25 Packet Interface Fault window. The X.25 LAPB Interface Fault window is displayed.

DS1 Interface Fault

The DS1 Interface Fault window displays fault information for the selected DS1 bridge interface.

To display the DS1 fault information for a DS1 bridge interface, select the DS1 bridge interface, then select **Fault** from either the LAN pull-down menu or the context menu.

Frame Relay Interface Fault

The Frame Relay Interface Fault window displays the fault information for the selected frame relay bridge interface. The window displays the type of error last detected on this interface, as well as the contents of the error packet and the time at which the error was detected.

To display the frame relay fault information for a frame relay bridge interface, select the frame relay bridge interface, then select **Fault** from either the LAN pull-down menu or the context menu.

Ethernet Interface Fault

The Ethernet Interface Fault window displays detailed fault information for the selected Ethernet bridge interface.

To display fault information for an Ethernet bridge interface, select the Ethernet bridge interface, then select **Fault** from either the LAN pull-down menu or the context menu.

Token-Ring Interface Fault

The Token-Ring Interface Fault window displays fault information for the selected token-ring bridge interface.

To display the fault information for a token-ring bridge interface, select the token-ring bridge interface, then select **Fault** from either the LAN pull-down menu or the context menu.

Bridge Interface and Port Performance Information

Performance information for a bridge port or bridge interface is displayed on the Port Performance and Interface Performance windows. The performance information displayed on these windows depends on the type of bridge port or bridge interface you have selected. Each window includes data that gives you an indication of how well the selected bridge port or interface is performing.

You can display the following types of bridge interface and port performance windows:

Source Route Port Performance

To display port source route performance information for a source route bridge port, select the source route bridge port, then select **Performance** from either the LAN pull-down menu or the context menu.

Transparent Bridging Port Performance

To display the transparent bridging performance information for a bridge port, select the transparent bridge port, then select **Performance** from either the LAN pull-down menu or the context menu.

Source Route Transparent Bridge Port Performance

To display performance information for an source route transparent bridge port, select the source route transparent bridge port, then select **Performance** from either the LAN pull-down menu or the context menu.

X.25 Packet Interface Performance

To display the X.25 packet performance information for an X.25 bridge interface, select the X.25 bridge interface, then select **Performance** from either the LAN pull-down menu or the context menu.

X.25 Packet Circuit Performance

To display the X.25 packet circuit performance information for an X.25 bridge interface, select an X.25 channel from the Circuit listbox on the X.25 Packet Interface Performance window, and then select the **Select** push button next to the listbox. The X.25 Packet Circuit Performance window is displayed.

X.25 LAPB Interface Performance

To display the X.25 LAPB performance information for an X.25 bridge interface, select the **LAPB Performance** push button on the X.25 Packet Interface Performance window. The X.25 LAPB Interface Performance window is displayed.

DS1 Interface Performance

The DS1 Interface Performance window displays performance information for the selected DS1 bridge interface.

To display the DS1 performance information for a DS1 bridge interface, select the DS1 bridge interface, then select **Performance** from either the LAN pull-down menu or the context menu.

Frame Relay Interface Performance

The Frame Relay Interface Performance window displays information about the performance of the DLCI associated with the selected frame relay bridge interface. Performance is described in terms of the frames and octets that pass through the bridge interface.

To display the frame relay performance information for a frame relay bridge interface, select the frame relay bridge interface, then select **Performance** from either the LAN pull-down menu or the context menu. The Frame Relay DLCI Circuits window is displayed. Select the DLCI circuit for which you want performance information from the listbox, then select the **Select** push button next to the listbox.

RS232 Interface Performance

The RS232 Interface Performance window displays information about the performance of the selected RS232 bridge interface. Performance is described in terms of input signals and input speeds.

To display the RS232 performance information for an RS232 bridge interface, select the RS232 bridge interface, select **Performance** from either the LAN pull-down menu or the context menu.

Token-Ring Interface Performance

The Token-Ring Interface Performance window displays performance information for the selected token-ring bridge interface.

To display the performance information for a token-ring bridge interface, select the token-ring bridge interface, then select **Performance** from either the LAN pull-down menu or the context menu.

Chapter 34. Displaying SNMP Bridge and SNMP Token-Ring Statistics

SNMP Bridge Statistics

- Ethernet_Interface_Fault

Names	MIB Variables
Alignment_errors_frames	dot3StatsAlignmentErrors
Frame_check_errors_frames	dot3StatsFCSErrors
Single_collision_frames	dot3StatsSingleCollisionFrames
Multiple_collision_frames	dot3StatsMultipleCollisionFrames
SQE_test_error_message	dot3StatsSQEtestErrors
Deferred_transmission_frames	dot3StatsDeferredTranmissionFrames
Late_Collisions	dot3StatsLateCollisions
Excessive_collisions	dot3StatsExcessiveCollisions
Internal_MAC_transmit_error_frames	dot3StatsDot3StatsInternalMACTransmitErrorFrames
Carrier_Sense_Errors	dot3StatsCarrierSenseErrors
Too_long_frames	dot3StatsFrameTooLong
Internal_MAC_receive_errors_frames	dot3StatsInternalMacReceiveErrors
Collision_count	dot3CollCount
Collision_frequency	dot3CollFrequencies

- Frame_Relay_Interface_Performance

Names	MIB Variables
Forward_congestion_frames_received	frCircuitReceivedFECNs
Backward_congestion_frames_received	frCircuitReceivedBECNs
Frames_transmitted	frCircuitSentFrames
Octets_transmitted	frCircuitSentOctets
Frames_received	frCircuitReceivedFrames
Octets_received	frCircuitReceivedOctets

- General_Fault

Names	MIB Variables
Delay_exceeded_discards	dot1dBasePortDelayExceededDiscards
MTU_exceeded_discards	dot1dBasePortMtuExceededDiscards

- Source_Route_Traffic_Analysis

Names	MIB Variables
Specifically_routed_frames_received	dot1dSrPortSpecInFrames
Specifically_routed_frames_transmitted	dot1dSrPortSpecOutFrames

```
 Path_explorer_frames_received              dot1dSrPortApeInFrames
 Path_explorer_frames_transmitted           dot1dSrPortApeOutFrames
 Spanning_tree_explorer_frames_received     dot1dSrPortSteInFrames
 Spanning_tree_explorer_frames_transmitted  dot1dSrPortSteOutFrames

- Source_Route_Fault

 Names                                      MIB Variables
 ---------------------------------------    ------------------------------
 Segment_mismatch_discards                  dot1dSrPortSegmentMismatchDiscards
 Duplicate_segment_discards                 dot1dSrPortDuplicateSegmentDiscards
 Hop_count_exceeded_discards                dot1dSrPortHopCountExceededDiscards


- Transparent_Bridging_Fault

 Names                                      MIB Variables
 ---------------------------------------    ------------------------------
 Learned_entry_discards                     dot1dTpLearnedEntryDiscards


- General_Fault                             // for 6611 Transparent Bridge

 Names                                      MIB Variables
 ---------------------------------------    ------------------------------
 Delay_exceeded_discards                    IBMdot1dBasePortDelayExceededDiscards
 MTU_exceeded_discards                      IBMdot1dBasePortMtuExceededDiscards


- Transparent_Bridging_Fault                // for 6611 Transparent Bridge

 Names                                      MIB Variables
 ---------------------------------------    ------------------------------
 Learned_entry_discards                     IBMdot1dTpLearnedEntryDiscards


- General_Fault                             // for IBM 8250

 Names                                      MIB Variables
 ---------------------------------------    ------------------------------
 Delay_exceeded_discards                    8250Dot1dBasePortDelayExceededDiscards
 MTU_exceeded_discards                      8250Dot1dBasePortMtuExceededDiscards
- Transparent_Bridging_Fault                // for IBM 8250

 Names                                      MIB Variables
 ---------------------------------------    ------------------------------
 Learned_entry_discards                     8250Dot1dTpLearnedEntryDiscards


- DS1_Interface_Fault

 Names                                      MIB Variables
 ---------------------------------------    ------------------------------
 Errored_seconds                            ds1TotalESS
 Severely_errored_seconds                   ds1TotalSESS
```

```
 Severely_errored_framing_seconds          ds1TotalSEFSS
 Unavailable_seconds                       ds1TotalUASS
 Controlled_slip_seconds                   ds1TotalCSSS
 Bipolar_violations                        ds1TotalBPVS
 Code_violation_error_events               ds1TotalCVS


- DS1_Interface_Performance

 Names                                     MIB Variables
 ----------------------------------------  ------------------------------
 Errored_seconds                           ds1CurrentESS
 Severely_errored_seconds                  ds1CurrentSESS
 Severely_errored_framing_seconds          ds1CurrentSEFSS
 Unavailable_seconds                       ds1CurrentUASS
 Controlled_slip_seconds                   ds1CurrentCSSS
 Bipolar_violations                        ds1CurrentBPVS
 Code_violation_error_events               ds1CurrentCVS


- RS232_Interface_Performance

 Names                                     MIB Variables
 ----------------------------------------  ------------------------------
 Number_of_input_signals                   RS232InSigChanges
 Number_of_output_signals                  RS232OutSigChanges


- X25_Interface_LAPB_Performance

 Names                                     MIB Variables
 ----------------------------------------  ------------------------------
 REJ_or_SREJ_frames_sent                   lapbFlowRejOutPkts
 REJ_or_SREJ_frames_received               lapbFlowRejInPkts
 T1_timeouts                               lapbFlowT1Timeouts

- X25_LAPB_Interface_Fault

 Names                                     MIB Variables
 ----------------------------------------  ------------------------------
 Busy_defer                                lapbFlowBusyDefers


- X.25 Packet_Interface_Performance

 Names                                     MIB Variables
     ------------------------------------------------------------------------
     Incoming_calls_received               x25StatInCalls
     Data_packets_received                 x25StatInDataPackets
     Call_attempts                         x25StatOutCallAttempts
     Data_packets_sent                     x25StatOutDataPackets
     Active_outgoing_circuit               x25StatOutGoingCircuits
     Active_incoming_circuit               x25StatInComingCircuits
     Active_two-way_circuits               x25StatTwowayCircuits
     Restart_timer_expired                 x25StatRestartTimeouts
```

Call_timer_expired	x25StatCallTimeouts
Reset_timer_expired	x25StatResetTimeouts
Clear_timer_expired	x25StatClearTimeouts
Data_timer_expired	x25StatDatarxmtTimeouts
Interrupt_timer_expired	x25StatInterruptTimeouts

- X.25_Circuit_Performance

Names	MIB Variables
Octects_received	x25CircuitInOctets
PDUs_received	x25CircuitInPdus
Interrupt_packets_received	x25CircuitInInterrupts
Octects_transmitted	x25CircuitOutOctets
PDUs_transmitted	x25CircuitOutPdus
Interrupt_packets_transmitted	x25CircuitOutInterrupts
Data_transmission_timer_expired	x25CircuitDataRetransmissionTimeouts
Reset_timer_expired	x25CircuitResetTimeouts
Interrupt_timer_expired	x25CircuitInterruptTimeouts

- X.25_Packet_Interface_Fault

Names	MIB Variables
Incoming_calls_refused	x25StatInCallRefusals
Clear_request_number	x25StatInProviderInitiatedClears
Remotely_reset_request_received	x25StatInRemotelyInitiatedResets
Reset_request_received	x25StatInProviderInitiatedResets
Restarts_received	x25StatInRestarts
Protocol_error_packets_received	x25StatInAccusedOfProtocolErrors
Interrupt_packets_received	x25StatInInterrupts
Fail_call_attempted	x25StatOutCallFailures
Interrupt_packets_sent	x25StatOutInterrupts
Retry_counter_exceeded	x25StatRetryCountExceededs
Clear_count_exceeded	x25StatClearCountExceededs

- X.25_Circuit_Fault

Names	MIB Variables
Remotely_received_resets	x25CircuitInRemotelyInitiatedResets
Resets_received	x25CircuitInProviderInitiatedReset

SNMP Token-Ring Statistics

- Segment

Names	MIB Variables
Number_of_NAUN_changes	crsNAUNChgs
Number_of_active_monitor_changes	crsActMonChgs

```
- Segment_Soft_Errors

 Names                                    MIB Variables
 ---------------------------------------  ------------------------------
     Lost_frames                          remTotalSoftErrorLostFrCounts
     Congestion                           remTotalSoftErrorRecCongCounts
     Frames_copied                        remTotalSoftErrorFrCopiedCounts
     Frequency                            remTotalSoftErrorFreqCounts
     Token                                remTotalSoftErrorTokenCounts
     Table_full                           remTotalSoftErrorTableFullCounts
     Decrement_below_minimum              remTotalSoftErrorMinDecrCounts
     Receiver_congestion_table_full       remTotalSoftErrorRecCngFullCounts


- Segment_Performance

 Names                                    MIB Variables
 ---------------------------------------  ------------------------------
 Ring_utilization                         surrRingUtilization
- Segment

 Names                                    MIB Variables
 ---------------------------------------  ------------------------------
 Number_of_NAUN_changes                   tokenRingMLStatsNAUNChanges
 Number_of_active_monitor_changes         ringStationControlChanges


- Segment_Fault

 Names                                    MIB Variables
     ---------------------------------------------------------------------
     Beacon_events                        tokenRingMLStatsBeaconEvents
     Beacon_packets                       tokenRingMLStatsBeaconPkts
     Number_of_soft_errors                tokenRingMLStatsSoftErrorReports
     Ring_maintenance_activity_counter    tokenRingMLStatsRingPollEvents


- Segment_Soft_Errors

 Names                                    MIB Variables
     ---------------------------------------------------------------------
     Lost_frames                          tokenRingMLStatsLostFrameErrors
     Congestion                           tokenRingMLStatsCongestionErrors
     Frames_copied                        tokenRingMLStatsFrameCopiedErrors
     Frequency                            tokenRingMLStatsFrequencyErrors
     Token                                tokenRingMLStatsTokenErrors
     Line                                 tokenRingMLStatsLineErrors
     Internal                             tokenRingMLStatsInternalErrors
     Burst                                tokenRingMLStatsBurstErrors
     Address_copied                       tokenRingMLStatsACErrors
     Abort                                tokenRingMLStatsAbortErrors


- Segment_Maintenance_Activity
```

```
   Names                                    MIB Variables
       ------------------------------------------------------------------------
       Number_of_ring_purged_events         tokenRingMLStatsRingPurgeEvents
       Number_of_ring_purge_MAC_packets     tokenRingMLStatsRingPurgePkts
       Number_of_monitor_contention_events  tokenRingMLStatsMonitorContentionEvents
       Number_of_claim_tokens               tokenRingMLStatsClaimTokenTkts


Station

   Names                                    MIB Variables
   ---------------------------------------  ------------------------------
   Number_of_insertions                     ringStationInsertions

  - Station_Fault

   Names                                    MIB Variables
       ------------------------------------------------------------------------
       Duplicate_addresses                  ringStationDuplicateAddress
       Probe_detected_line                  ringStationInLineErrors
       NADN_detected_line                   ringStationOutLineErrors
       Probe_detected_burst                 ringStationInternalErrors
       Probe_detected_burst                 ringStationInBurstErrors
       NADN_detected_burst                  ringStationOutBurstErrors
       Address_copied_errors                ringStationACErrors
       Frame_copied                         ringStationFrameCopiedErrors
       Probe_detected_beacon_frames         ringStationInBeaconErrors
       NADA_detected_beacon_frames          ringStationOutBeaconErrors


  - Segment_Performance

   Names                                    MIB Variables
   ---------------------------------------  ------------------------------
   Ring_utilization                         cauRingUtilStat
```

Traps

For information on traps, refer to “Chapter 28. Traps” on page 255.

Part 7. Managing FDDI Resources

Chapter 35. Applications and Agents

FDDI SNMP Application

You can monitor and manage FDDI networks by using the FDDI application of LAN Network Manager. The FDDI application provides management for devices that support levels 6.2 and 7.3 of the FDDI station management (SMT) standard that is defined by the American National Standards Institute (ANSI). You can manage both single- and dual-attached stations and concentrators that support SMT 6.2 or 7.3.

LAN Network Manager uses the FDDI SNMP Proxy Agent program as its proxy agent in the FDDI networks. The FDDI SNMP Proxy Agent passes requests from LAN Network Manager to the managed FDDI segment and obtains status and change information pertaining to the FDDI resources on the segment by means of status reporting frames (SRFs) from the FDDI segment. These are converted into SNMP traps and passed to LAN Network Manager.

FDDI SNMP Proxy Agent

The FDDI SNMP Proxy Agent program serves as the FDDI proxy agent for LAN Network Manager and provides monitoring and management of an FDDI segment. The FDDI proxy agent can manage devices that support levels 6.2 or 7.3 of the FDDI station management (SMT) protocol. An FDDI proxy agent is required for each FDDI segment that is managed.

To communicate with LAN Network Manager, the FDDI proxy agent program uses SNMP and forwards problem information and configuration changes to LAN Network Manager with SNMP traps. These traps are not solicited by LAN Network Manager, although you must configure the proxy agents so that they send their traps to the correct host. The FDDI proxy agent implements both the RFC 1512 MIB and the RFC 1285 MIB, along with the IBM extensions to RFC 1285 that further define FDDI segment and resource management. LAN Network Manager uses these MIB definitions to query and change parameters in FDDI stations and concentrators and to obtain information about how the FDDI ring is logically configured.

Chapter 36. Configuring Management Parameters for FDDI Resources

After installing the FDDI application, you can configure the FDDI capability for the network you are managing. To configure the FDDI capability to manage your FDDI resources, you use SMIT to define values for:

- LAN Network Manager general parameters
- General parameters for SNMP agents
- FDDI proxy agent parameters

This chapter describes how to carry out these tasks.

Using SMIT to Configure LAN Network Management

The configuration parameters that you define in SMIT are saved in files with an extension of .conf in the `/usr/CML/conf/lnmfddimon` directory. These files are read each time LAN Network Manager is started.

Configuring General Parameters for SNMP Agents

In order for SNMP agent programs to forward trap information to LAN Network Manager applications, the agents must be specifically configured. There are two parameters that you might need to configure in the agent programs to communicate with LAN Network Manager and NetView for AIX:

- IP address of the machine on which Nways Manager-LAN is running
- Community name, time-outs, and retries as defined in NetView for AIX

Configuring the IP Address of the Management Station

The IP address of the station on which Nways Manager-LAN is installed must be configured in each of the SNMP agent programs. If an agent is not configured with the correct IP address, LAN Network Manager applications cannot correlate traps and provide network topology and status changes.

The steps for configuring an agent program depend on the type of SNMP agent you are configuring. Refer to the documentation for each agent for configuration instructions.

Configuring Agent Community Names

A community name is a password that enables SNMP access to MIB values on an agent. To retrieve and update MIB values, LAN Network Manager applications use the SNMP community names defined in NetView for AIX to build SNMP queries. For these queries to be successful, the community name defined in each SNMP agent program must match the community name defined in NetView for AIX for the agent.

To ensure that the community names match, check the community defined in each agent program, then verify that the names match those defined on the NetView for AIX SNMP Configuration window. To open the SNMP Configuration window, select **Options -> SNMP Configuration** from the NetView for AIX menu bar.

If the community names do not match, you can change the community name defined either on the NetView for AIX SNMP Configuration window or in the agent program. If the community name defined for an agent in the agent program is `public`, you do not have to define the community name in NetView for AIX; `public` is the default community name.

Any change you make to a community name takes effect immediately. It is not necessary to stop and restart Nways Manager-LAN to activate the change. For more information about configuring agent community names, refer to the *NetView for AIX User's Guide*.

Configuring Agent Time-Outs

In order for an SNMP bridge or SNMP token-ring to be fully managed by LAN Network Manager, you must configure its time-out parameter with a large enough value so that the resources can be discovered by Nways Manager-LAN. The time-out parameter defines the number of seconds that Nways Manager-LAN waits before updating its LAN submaps.

If you have a large network, be sure to define a longer time-out period so that the agent has enough time to provide all its configuration information before Nways Manager-LAN updates the LAN topology in the LAN submaps.

To change the time-out period defined for an agent program, select **Options -> SNMP Configuration** from the NetView for AIX menu bar and enter a new time-out value in the SNMP Configuration window.

Configuring FDDI SNMP Agents

After you have installed an FDDI SNMP proxy agent on a workstation in each segment that you are managing, configure each agent so that Nways Manager-LAN can communicate with it.

Each FDDI SNMP agent is managed by the LAN Network Manager component and has a configuration file that you can modify using SMIT. With SMIT, you can define the IP address of the agent, the number of the segment on which the agent resides, and the polling interval that the agent uses.

To modify the configuration of an FDDI agent, follow these steps:

1. Ensure you are logged on with root privileges.
2. If SMIT is not running, enter **smit cml** from an AIX operating system shell, or select **Administer -> Campus Manager SMIT** from the NetView for AIX menu.

The SMIT menu is displayed.

3. Select **Configure**.
4. Select **Configure FDDI capability**.
5. Select **Configure IBM FDDI proxy agent**.
6. Enter the IP address of the FDDI agent you want to add or change. Press Enter or **OK**. A complete Add/Change IBM FDDI proxy agent menu is displayed.
7. Enter new values of any of the following FDDI agent parameters For help on an input field, select **?** and point to the field.

IP address	Internet Protocol (IP) address of the agent.
Segment number	Number used to identify the segment that is managed by the agent.
Resync interval	Time period (in days, hours, minutes) used by the agent to resynchronize the segment and update adapter information. Each resynchronziation refreshes LAN submaps with the latest changes made to the network topology (for example, moving, adding, or removing FDDI devices).

8. Press Enter or select **OK** to activate your changes.
9. Select **Exit SMIT** from the Exit pull-down menu to leave the SMIT program.

Chapter 37. Managing FDDI Networks

LAN Network Manager works with the FDDI SNMP Proxy Agent and SystemViewto extend your network management environment to FDDI LAN segments. LAN Network Manager works with the FDDI SNMP Proxy Agent to pass instructions from LAN Network Manager to the managed FDDI segment and to obtain status and change information pertaining to the FDDI resources. Using LAN Network Manager, you can perform FDDI network management tasks by selecting an FDDI resource from a topological view of your network and using menu choices to perform a specific task.

This chapter describes the FDDI application, the IBM FDDI SNMP proxy agent, and the MIBs that the FDDI application uses to obtain information about your FDDI network resources. Specifically, this chapter contains the following topics:

Understanding the FDDI Application

You can monitor and manage FDDI networks by using the FDDI application of LAN Network Manager. The FDDI application provides management for devices that support levels 6.2 and 7.3 of the FDDI station management (SMT) standard that is defined by the American National Standards Institute (ANSI). You can manage both single- and dual-attached stations and concentrators that support SMT 6.2 or 7.3.

LAN Network Manager uses the FDDI SNMP Proxy Agent program as its proxy agent in the FDDI networks. The FDDI SNMP Proxy Agent passes requests from LAN Network Manager to the managed FDDI segment and obtains status and change information pertaining to the FDDI resources on the segment by means of status reporting frames (SRFs) from the FDDI segment. These are converted into SNMP traps and passed to LAN Network Manager.

IBM FDDI SNMP Proxy Agent

The FDDI SNMP Proxy Agent program serves as the FDDI proxy agent for LAN Network Manager and provides monitoring and management of an FDDI segment. The FDDI proxy agent can manage devices that support levels 6.2 or 7.3 of the FDDI station management (SMT) protocol. An FDDI proxy agent is required for each FDDI segment that is managed.

To communicate with LAN Network Manager, the FDDI proxy agent program uses SNMP and forwards problem information and configuration changes to LAN Network Manager with SNMP traps. These traps are not solicited by LAN Network Manager, although you must configure the proxy agents so that they send their traps to the correct host. The FDDI proxy agent implements both the RFC 1512 MIB and the RFC

1285 MIB, along with the IBM extensions to RFC 1285 that further define FDDI segment and resource management. LAN Network Manager uses these MIB definitions to query and change parameters in FDDI stations and concentrators and to obtain information about how the FDDI ring is logically configured.

Defining Parameters for FDDI Networks

After you have installed one or more IBM FDDI SNMP proxy agent programs and defined the basic parameters LAN Network Manager needs to establish and maintain contact with the IBM FDDI SNMP proxy agent, you can define additional parameters for each proxy agent program using the FDDI Proxy Agent Configuration window. From this window, you can open the Resync Interval window, from which you can define how often LAN Network Manager resynchronizes the FDDI segment the proxy agent is managing.

Displaying FDDI Proxy Agent Configuration Information

Display and change basic information for the FDDI proxy agent program using the FDDI Proxy Agent Configuration window. This window displays information about the agent program installed on a workstation in the selected segment.

To display the FDDI Proxy Agent Configuration window, follow these steps:

1. Select the icon that represents the segment on which the FDDI proxy agent is installed.
2. Select **Configuration** from the LAN pull-down or context menu.

   The FDDI Proxy Agent Configuration window is displayed.
3. Enter the configuration information.
4. If you want to display or change the resynchronization interval, select **Resync interval** from the Actions pull-down menu. See “Displaying and Changing the FDDI Segment Resynchronization Interval” for more information.
5. Select **OK** to save the information and close the window.

Displaying and Changing the FDDI Segment Resynchronization Interval

The Resync Interval window enables you to specify how frequently LAN Network Manager resynchronizes the FDDI segment. By resynchronizing the FDDI segment, LAN Network Manager can maintain a more accurate network configuration by updating adapter information on a regular basis.

The days, hours, and minutes fields are considered together to specify a single time interval.

The default value for this parameter is 60 minutes. To ensure better performance and accurate network discovery, do not specify a resync interval that is less than 30 minutes.

To display the Resync Interval window, follow these steps:

1. Select **Resync interval** from the Actions pull-down menu on the FDDI Proxy Agent Configuration window.

   The Resync Interval window is displayed.
2. Enter changes to the days, hours, or minutes fields.
3. To perform an immediate resynchronization of the segment, select **Resync** from the Actions pull-down menu.
4. Select **OK** to save the information and close the window.

Chapter 38. Managing FDDI Stations

To manage FDDI stations, use LAN Network Manager to monitor and view information about stations and make changes as necessary to improve station performance.

This chapter describes the information that you can view for a station, identifies which parts of the information you can change, and describes other actions you can perform to help manage the station. The information in this chapter is organized according to each type of resource object included in a station.

This chapter contains the following topics:

Note: Some of the fields on the FDDI management windows contain information that is supported by only level 6.2 or level 7.3 of the SMT standard. These fields may be grayed if they display information for devices that do not support the appropriate level of the SMT standard.

Some selections on pull-down menus may be grayed if the actions cannot be performed for the selected device.

Displaying an FDDI Station Submap

LAN Network Manager provides a FDDI Station submap to represent the managed elements of an FDDI station. If you double-click on an FDDI station in an FDDI Segment submap, the FDDI Station submap opens to display a graphical representation of a computer workstation. Icons representing the SMT, attachment, MAC, path, path class, and ports are displayed in the submap.

The color of a managed element indicates the element's current status. Select a managed element from the FDDI Station submap to obtain profile, configuration, fault, and performance information for that element. To open a Node submap for the selected station, double-click on the SMT icon.

Displaying SMT Information

Station Management (SMT) is the component in an FDDI station or concentrator that coordinates basic operation of the resource, such as connection to the FDDI segment and interaction with other stations on the segment. The SMT object represents an FDDI station or an FDDI concentrator.

Display information about the SMT object of a station by accessing one of the following windows:

For information about:	Read:
Profile	“Displaying the Station Management Profile Window”
Configuration	“Using the Station Management Configuration Window” on page 324
Fault	“Displaying Station Management Fault Window” on page 325

Displaying the Station Management Profile Window

The Station Management Profile window enables you to access information about how a station is currently configured and how it is operating.

To display the Station Management Profile window, select a station from a Segment submap or select the SMT icon from the FDDI station submap, then select **Profile** from either the LAN pull-down menu or the context menu. The Station Management Profile window is displayed.

To perform additional actions from the Station Management Profile window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Connect	“Connecting a Station” on page 323
Disconnect	“Disconnecting a Station” on page 323
Test path	“Testing a Station’s Path” on page 323
Self-test	“Running a Self-Test” on page 323
Disable a	“Disabling the A Port of a Station” on page 323
Disable b	“Disabling the B Port of a Station” on page 324
Disable m	“Disabling the M Ports of a Station” on page 324

To navigate directly to other SMT windows, select one of the following choices from the Navigation pull-down menu on the Station Management Profile window:

Select:	To navigate to:
Configuration	To display the Station Management Configuration window
Fault	To display the Station Management Fault window

Connecting a Station

To connect an FDDI station to the segment, select **Connect** from the Actions pull-down menu on the Station Management Profile window.

Disconnecting a Station

To disconnect an FDDI station from the segment, select **Disconnect** from the Actions pull-down menu on the Station Management Profile window.

When you disconnect an FDDI station, LAN Network Manager removes the station from the segment and from the graphical submaps. Disconnecting severs the communication link to the station. Reconnecting the station requires manual intervention.

Testing a Station's Path

The path test function in an FDDI station is used to verify the data path through the station and locate faulty MACs.

To perform a path test on a station, select **Test path** from the Actions pull-down menu on the Station Management Profile window.

LAN Network Manager cannot verify the results of this action. If the FDDI station performs a path test and identifies a problem, it disconnects itself from the ring. LAN Network Manager is notified of the topology change through its normal neighbor notification operation.

Running a Self-Test

To initiate a self test in a station, select **Self test** from the Actions pull-down menu on the Station Management Profile window.

LAN Network Manager cannot verify the results of this action. If the FDDI station executes its self-test function and identifies a problem, it disconnects itself from the ring. LAN Network Manager becomes aware of the change in topology through its normal neighbor notification operation.

Disabling the A Port of a Station

The A port in a dual-attached FDDI station is designated as the inbound path for the primary ring and the outbound path for the secondary ring.

You can use LAN Network Manager to disable the A port of a dual-attached FDDI station.

From this window, this action is valid only for devices that support the 7.3 level of the SMT standard. You can disable the port of a station that supports the 6.2 level of the SMT standard using the Port Profile window. See “Disabling a Port” on page 331 for more information.

To disable the A port of a station, select **Disable A** from the Actions pull-down menu on the Station Management Profile window.

Disabling the B Port of a Station

The B port in a dual-attached FDDI station is designated as the outbound path for the primary ring and the inbound path for the secondary ring.

You can use LAN Network Manager to disable the B port of a dual-attached FDDI station.

From this window, this action is valid only for devices that support the 7.3 level of the SMT standard. You can disable the port of a station that supports the 6.2 level of the SMT standard using the Port Profile window. See “Disabling a Port” on page 331 for more information.

To disable the B port of a station, select **Disable B** from the Actions pull-down menu on the Station Management Profile window.

Disabling the M Ports of a Station

Ports of type M provide connections to the concentrator tree.

This action disables all M ports. This action is valid only for devices that support the 7.3 level of the SMT standard. You cannot perform this action on devices that only support the 6.2 level of the SMT standard.

To disable the M ports, select **Disable** from the Actions pull-down menu on the Station Management Profile window.

To disable a single M port, select the port you want to disable, and then select **Profile**, **Configuration**, or **Fault** from the LAN pull-down or context menu. Then select **Disable** from the Actions pull-down on the Port Profile, Configuration, or Fault management window to disable the selected port.

Using the Station Management Configuration Window

The Station Management Configuration window enables you to access and change station configuration information.

To display the Station Management Configuration window, select a station from a Segment submap or select the SMT icon from the FDDI station submap. Then select **Configuration** from either the LAN pull-down menu or the context menu.

To perform additional actions from the Station Management Configuration window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Connect	“Connecting a Station” on page 323
Disconnect	“Disconnecting a Station” on page 323
Test path	“Testing a Station’s Path” on page 323
Self-test	“Running a Self-Test” on page 323
Disable a	“Disabling the A Port of a Station” on page 323
Disable b	“Disabling the B Port of a Station” on page 324
Disable m	“Disabling the M Ports of a Station” on page 324

To navigate directly to other SMT windows, select one of the following choices from the Navigation pull-down menu on the Station Management Configuration window:

Select:	To navigate to:
Profile	To display the Station Management Profile window
Fault	To display the Station Management Fault window

Displaying Station Management Fault Window

The Station Management Fault window allows you to access detailed information about how a station is operating and enables you to set threshold values and monitor fault conditions.

To display the Station Management Fault window, select a station from a Segment submap or select the SMT icon from the FDDI station submap. Then select **Fault** from either the LAN pull-down menu or the context menu.

To perform additional actions from the Station Management Fault window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Connect	“Connecting a Station” on page 323
Disconnect	“Disconnecting a Station” on page 323
Test path	“Testing a Station’s Path” on page 323
Self-test	“Running a Self-Test” on page 323
Disable a	“Disabling the A Port of a Station” on page 323
Disable b	“Disabling the B Port of a Station” on page 324
Disable m	“Disabling the M Ports of a Station” on page 324

To navigate directly to other SMT windows, select one of the following choices from the Navigation pull-down menu on the Station Management Fault window:

Select:	To navigate to:
Profile	To display the Station Management Profile window
Configuration	To display the Station Management Configuration window

Displaying MAC Information

The media access control (MAC) of an FDDI station ensures that the station has data access to the ring, performs any checking of data frames, and handles address recognition. The MAC is also responsible for delivering packet data, including frame generation, repetition, and removal. A station can have multiple instances of a MAC.

Display MAC information by accessing one of the following windows:

For information about:	Read:
Profile	"Using the MAC Profile Window"
Configuration	"Using the MAC Configuration Window" on page 328
Performance	"Using the MAC Performance Window" on page 329

Using the MAC Profile Window

The MAC Profile window provides information about MAC configuration and operation.

To display the MAC Profile window, select the MAC icon from the FDDI Station submap, then select **Profile** from either the LAN pull-down menu or the context menu.

To perform additional actions from the MAC Profile window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Enable LLC service	"Enabling LLC Service" on page 327
Disable LLC service	"Disabling LLC Service" on page 327
Connect MAC	"Connecting a MAC" on page 327
Disconnect MAC	"Disconnecting a MAC" on page 327

To navigate directly to other MAC windows, select one of the following choices from the Navigation pull-down menu on the MAC Profile window:

Select:	To navigate to:
Configuration	To display the MAC Configuration window
Fault	To display the MAC Fault window
Performance	To display the MAC Performance window

To display additional information, select one of the following push buttons on the MAC Profile window:

For information about:	Read:
Operation	“MAC Profile Operation Window”
Capabilities	“MAC Profile Capabilities Window”

MAC Profile Operation Window

To access the MAC Profile Operation window, select the **Operation** push button on the MAC Profile window. The MAC Profile — Operation window is displayed.

MAC Profile Capabilities Window

To access the MAC Profile Capabilities window, select the **Capabilities** push button on the MAC Profile window. The MAC Profile — Capabilities window is displayed.

Enabling LLC Service

To enable the local logical link control entity to communicate with that of a peer station, select **Enable LLC service** from the Actions pull-down menu on the MAC Profile window.

This action is valid only for devices that support the 6.2 level of the SMT standard.

Disabling LLC Service

To terminate communication between the local logical link control entity and that of a peer station, select **Disable LLC service** from the Actions pull-down menu on the MAC Profile window.

Note: If you perform this action for the station that is running the FDDI SNMP Proxy Agent program, TCP/IP is terminated and you lose connection to the local segment.

This action is valid only for devices that support the 6.2 level of the SMT standard.

Connecting a MAC

To enable the MAC to transfer data on the ring, select **Connect MAC** from the Actions pull-down menu on the MAC Profile window.

This operation fails if there is no path to the disconnected MAC.

This action is valid only for devices that support the 6.2 level of the SMT standard.

Disconnecting a MAC

To detach the MAC from the ring and inhibit transfer of data, select **Disconnect MAC** from the Actions pull-down menu on the MAC Profile window.

This action is valid only for devices that support the 6.2 level of the SMT standard.

Using the MAC Configuration Window

The MAC Configuration window enables you to access information about how the MAC is configured and allows you to change the configuration.

To display and change MAC configuration information, select the MAC icon from the FDDI Station submap, then select **Configuration** from either the LAN pull-down menu or the context menu. The MAC Configuration window is displayed.

To perform additional actions from the MAC Configuration window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Enable LLC service	“Enabling LLC Service” on page 327
Disable LLC service	“Disabling LLC Service” on page 327
Connect MAC	“Connecting a MAC” on page 327
Disconnect MAC	“Disconnecting a MAC” on page 327

To navigate directly to other MAC windows, select one of the following choices from the Navigation pull-down menu on the MAC Configuration window:

Select:	To navigate to:
Profile	To display the MAC Profile window
Fault	To display the MAC Fault window
Performance	To display the MAC Performance window

Using the MAC Fault Window

The MAC Fault window enables you to access detailed information about how a MAC is operating and allows you to set threshold values and monitor fault conditions.

To display the MAC Fault window, select the MAC icon from the FDDI Station submap, then select **Fault** from either the LAN pull-down menu or the context menu.

To perform additional actions from the MAC Fault window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Enable LLC service	“Enabling LLC Service” on page 327
Disable LLC service	“Disabling LLC Service” on page 327
Connect MAC	“Connecting a MAC” on page 327
Disconnect MAC	“Disconnecting a MAC” on page 327

To navigate directly to other MAC windows, select one of the following choices from the Navigation pull-down menu on the MAC Fault window:

Select:	To navigate to:
Profile	To display the MAC Profile window
Configuration	To display the MAC Configuration window
Performance	To display the MAC Performance window

To display additional information, select one of the following push buttons on the MAC Fault window:

For information about:	Read:
Error counters	“MAC Fault Error Counters Window”
Copy failure counters	“MAC Fault Copy Failure Counters Window”

MAC Fault Error Counters Window

To access the MAC Fault Error Counters window, select **Error Counters** on the MAC Fault window. The MAC Fault — Error Counters window is displayed.

MAC Fault Copy Failure Counters Window

To access the MAC Fault Copy Failure Counters window, select **Copy Failure Counters** on the MAC Fault window. The MAC Fault — Copy Failure Counters window is displayed.

Using the MAC Performance Window

The MAC Performance window provides detailed information about how efficiently a MAC is operating and processing data.

To display the MAC Performance window, select the MAC icon from the FDDI Station submap, then select **Performance** from either the LAN pull-down menu or the context menu.

To perform additional actions from the MAC Performance window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Enable LLC service	“Enabling LLC Service” on page 327
Disable LLC service	“Disabling LLC Service” on page 327
Connect MAC	“Connecting a MAC” on page 327
Disconnect MAC	“Disconnecting a MAC” on page 327

To navigate directly to other MAC windows, select one of the following choices from the Navigation pull-down menu on the MAC Performance window:

Select:	To navigate to:
Profile	To display the MAC Profile window
Configuration	To display the MAC Configuration window
Fault	To display the MAC Fault window

Displaying Port Information

The object management of ports for an FDDI station deals either with port attributes, such as configuration, operation, and status, or with error conditions experienced by a port.

Display port information by accessing one of the following windows:

For information about:	Read:
Profile	“Using the Port Profile Window”
Configuration	“Using the Port Configuration Window” on page 331
Fault	“Using the Port Fault Window” on page 332

Using the Port Profile Window

The Port Profile window provides configuration and operation information for a port.

To display the Port Profile window, select a port icon from the FDDI Station submap, then select **Profile** from either the LAN pull-down menu or the context menu.

To perform additional actions from the Port Profile window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Maintain	“Maintaining a Port” on page 331
Enable	“Enabling a Port” on page 331
Disable	“Disabling a Port” on page 331
Start	“Starting a Port” on page 331
Stop	“Stopping a Port” on page 331

To navigate directly to other port windows, select one of the following choices from the Navigation pull-down menu on the Port Profile window:

Select:	To navigate to:
Configuration	To display the Port Configuration window
Fault	To display the Port Fault window

Maintaining a Port

Within the FDDI station, the maintenance state is provided to support port maintenance functions for troubleshooting problems between ports, such as line faults. To put the resource in maintenance state, you need to force the port into a known line state.

To put a port in the maintenance state, select **Maintain** from the Actions pull-down menu on the Port Profile window.

To perform maintenance on a port, first terminate port activity. For more information, see “Stopping a Port”.

Enabling a Port

To indicate that port maintenance is complete and that the port is ready to be started, select **Enable** from the Actions pull-down menu on the Port Profile window.

Disabling a Port

To terminate activity in a port and cause it to enter the maintenance state, select **Disable** from the Actions pull-down menu on the Port Profile window.

Starting a Port

To indicate that the port is available for communication, select **Start** from the Actions pull-down menu on the Port Profile window.

Stopping a Port

To terminate activity in a port without directly entering the maintenance state, select **Stop** from the Actions pull-down menu on the Port Profile window.

Using the Port Configuration Window

The Port Configuration window enables you to access information about how the port is configured and allows you to change the configuration.

To display the Port Configuration window, select a port icon from the FDDI Station submap, then select **Configuration** from either the LAN pull-down menu or the context menu.

To perform additional actions from the Port Configuration window, select one of the following menu choices from the Actions pull-down menu:

For information about:	**Read:**
Maintain	“Maintaining a Port”
Enable	“Enabling a Port”

For information about:	Read:
Disable	“Disabling a Port” on page 331
Start	“Starting a Port” on page 331
Stop	“Stopping a Port” on page 331

To navigate directly to other port windows, select one of the following choices from the Navigation pull-down menu on the Port Configuration window:

Select:	To navigate to:
Profile	To display the Port Profile window
Fault	To display the Port Fault window

Using the Port Fault Window

The Port Fault window enables you to access detailed information about how a port is operating and allows you to set threshold values and monitor fault conditions.

To display the Port Fault window, select a port icon from the FDDI Station submap, then select **Fault** from either the LAN pull-down menu or the context menu.

To perform additional actions from the Port Fault window, select one of the following menu choices from the Actions pull-down menu:

For information about:	Read:
Maintain	“Maintaining a Port” on page 331
Enable	“Enabling a Port” on page 331
Disable	“Disabling a Port” on page 331
Start	“Starting a Port” on page 331
Stop	“Stopping a Port” on page 331

To navigate directly to other port windows, select one of the following choices from the Navigation pull-down menu on the Port Fault window:

Select:	To navigate to:
Profile	To display the Port Profile window
Configuration	To display the Port Configuration window

Port Fault - Link Errors Push Button

Display additional port fault information for a selected port on the Port Fault — Link Errors window. The Port Fault — Link Errors window displays the values for a variety of link error counters and enables you to set threshold values that determine when the number of link errors causes an alarm to be generated or the link connection to be terminated.

To display the Port Fault — Link Errors window, select the **Port link errors** push button on the Port Fault window.

Displaying Path Information

The path in an FDDI station represents the segment or segments of the logical ring that pass through the station. The path object can have multiple instances within a node.

Display path information by accessing one of the following windows:

For information about:	Read:
Profile	"Using the Path Profile Window"
Configuration	"Using the Path Configuration Window"
Fault	"Using the Path Fault Window" on page 334

Using the Path Profile Window

The Path Profile window provides configuration and operation information for a path.

To display the Path Profile window, select the path icon from the FDDI Station submap, then select **Profile** from either the LAN pull-down menu or the context menu.

Navigate to the Path Configuration window by selecting **Configuration** from the Navigation pull-down menu on the Path Profile window.

Using the Path Configuration Window

The Path Configuration window enables you to access information about how the path is configured and allows you to change the configuration.

To display the Path Configuration window, select the path icon from the FDDI Station submap, then select **Configuration** from either the LAN pull-down menu or the context menu.

Navigate to the Path Profile window by selecting **Profile** from the Navigation pull-down menu on the Path Configuration window.

Using the Path Class Configuration Window

The Path Class Configuration window displays information about transmission timers used on the path to detect ring inactivity and about time values that affect the target token rotation time (TTRT) used on the path.

To display the Path Class Configuration window, select **More** in the Path class configuration field.

Using the Path Fault Window

The Path Fault window enables you to access detailed information about how a path is operating and allows you to set threshold values and monitor fault conditions.

To display the Path Fault window, select the path icon from the FDDI Station submap, then select **Fault** from either the LAN pull-down menu or the context menu.

Navigate to the Path Profile window by selecting **Profile** from the Navigation pull-down menu on the Path Fault window.

Displaying Attachment Information

The attachment object represents a port or a pair of ports plus the optional associated optical bypass. There is always an association between the attachment resource and the port.

Display attachment information by accessing one of the following windows:

For information about:	Read:
Profile	“Using the Attachment Profile Window”
Configuration	“Using the Attachment Configuration Window”

Using the Attachment Profile Window

The Attachment Profile window provides configuration and operation information for the attachment components of a station.

This action is valid only for devices that support the 6.2 level of the SMT standard.

To display the Attachment Profile window, select the attachment icon from the FDDI Station submap, then select **Profile** from either the LAN pull-down menu or the context menu.

Navigate to the Attachment Configuration window by selecting **Configuration** from the Navigation pull-down menu on the Attachment Profile window.

Using the Attachment Configuration Window

The Attachment Configuration window enables you to access information about how the attachment components of a station are configured and allows you to change their configuration.

This action is valid only for devices that support the 6.2 level of the SMT standard.

To display the Attachment Configuration window, select the attachment icon from the FDDI Station submap, then select **Configuration** from either the LAN pull-down menu or the context menu.

Navigate to the Attachment Profile window by selecting **Profile** from the Navigation pull-down menu on the Attachment Configuration window.

Chapter 39. Managing FDDI Concentrators

LAN Network Manager provides graphical views of the IBM 8240 and 8244 Concentrators in your network and provides information and status about these concentrators. You can also display a generic graphical view that represents other types of FDDI concentrators, such as the IBM 8250 Concentrator or OEM FDDI concentrators.

This chapter contains the following topics:

Displaying a Concentrator Submap

LAN Network Manager supports both IBM and non-IBM FDDI concentrators. You manage the concentrators in your network by monitoring the status of the concentrators on the Segment submap and Concentrator submaps.

The FDDI concentrators in your network are represented by icons in the Segment submap. Double-clicking on the concentrator icon in a Segment submap opens a Concentrator submap.

The Concentrator submap displays a graphical representation of an FDDI concentrator. For 8240 and 8244 concentrators, the submap is a direct representation of the concentrator. For other FDDI concentrators, the submap is a generic representation of an FDDI concentrator.

As part of the graphical representation of the concentrator, the FDDI Concentrator submap also represents the other managed elements of the concentrator, including the ports and the station interface cartridges that are contained in the concentrator. These elements of the concentrator are represented by icons, which you can use to access those elements.

The top portion of the graphical representation of the concentrator includes an icon that represents the media access control (MAC) for the concentrator. Select the MAC icon to access profile, configuration, and performance information about the MAC element of the concentrator.

Similarly, select the icon at the top right of the concentrator to access profile, configuration, and fault information for the concentrator's station management (SMT) component.

The station interface cartridges are represented by the horizontal modules below the top portion of the concentrator. An icon to the right of each cartridge represents that cartridge. Select a cartridge icon to access profile information for the cartridge.

Within each cartridge icons represent the ports inserted in the cartridge. The port label indicates whether the port is being used as an A, B, M, or S port. Select a port to access profile, configuration, and fault information for the port.

The submap for the IBM 8244 concentrator is also a graphical representation of the concentrator, with a row of ports represented by icons. Other FDDI concentrators are displayed with a generic graphical view of a concentrator. The generic graphical view represents the managed elements of the concentrator with icons placed on a representation of a generic concentrator. To access management windows for these elements, select the icons in the submap in the same way you do in the 8240 and 8244 submaps.

At the lower right of all FDDI Concentrator submaps, just outside of the concentrator, are icons that represent the concentrator's attachment, path, and path class. Access profile, configuration, and fault information for these components by selecting the icon and using the LAN pull-down or context menu.

For information about:	**Read:**
MAC	"Displaying MAC Information" on page 326
SMT	"Displaying SMT Information" on page 322
Cartridge	"Displaying a Cartridge Profile" on page 339
Ports	"Displaying Port Information" on page 330
Path	"Displaying Path Information" on page 333
Path class	"Displaying Path Information" on page 333
Attachment	"Displaying Attachment Information" on page 334

Displaying a Concentrator Profile

The Concentrator Profile window displays information about an FDDI concentrator. You can access identification information that describes the physical device, such as the serial number or the machine type. Information about the operation of the concentrator is also displayed and provides such details as the addressing scheme for the concentrator and the slots that are in use.

To display a concentrator profile, select the concentrator, then select **Profile** from either the LAN pull-down menu or the context menu.

To perform additional actions from the Concentrator Profile window, select one of the following menu choices from the Actions: pull-down menu.

For information about:	Read:
Save Configuration	“Saving Concentrator Configuration”
Soft Reset	“Performing a Soft Reset”

To navigate directly to the SMT Profile window, select **Profile** from the Navigation pull-down menu on the Concentrator Profile window.

Saving Concentrator Configuration

To save changes you make to the configuration parameters of an 8240 concentrator, use the **Save configuration** menu choice.

Performing a Soft Reset

To cause a concentrator to reload its microcode and reset itself, select **Soft reset** Concentrator Profile Actions pull-down menu. When you select **Soft reset**, the concentrator removes itself from the communications path and reloads its microcode. Configuration changes that were saved are activated after the microcode is reloaded.

Displaying a Cartridge Profile

The Cartridge Profile window displays information about the cartridge, such as the current status, the physical connection type, and the number of ports that are attached.

To display information about a specific cartridge in the graphical submap, select the icon of the cartridge, then select **Profile** from either the LAN pull-down menu or the context menu.

Chapter 40. Displaying FDDI Statistics

Table 30. FDDI MAC Fault Panel - FDDI_MAC_Fault

Mib Attribute Name	OID	Variable Names
snmpFddiMACFrameErrorRatio	1.3.6.1.2.1.10.15.2.2 1.24	Frame_error_ratio
fddimibMACFrameErrorRatio	1.3.6.1.2.1.10.15.73.2.2.1.27	Frame_error_ratio

Table 31. FDDI MAC Performance Panel - FDDI_MAC_Performance

Mib Attribute Name	OID	Variable Names
snmpFddiMACFrameCts	1.3.6.1.2.1.10.15.2.2.1.20	Frames
fddimibMACFrameCts	1.3.6.1.2.1.10.15.73.2.2.1.21	Frames
fddimibMACCopiedCts	1.3.6.1.2.1.10.15.73.2.2.1.22	Receveid_frames
fddimibMACTransmitCts	1.3.6.1.2.1.10.15.73.2.2.1.23	Transmitted_frames
fddimibMACTokenCts	1.3.6.1.2.1.10.15.73.3.1.1.1	Tokens_receveid

Table 32. FDDI Port Fault - Link Errors Panel - FDDI_Port_Fault_Link Errors

Mib Attribute Name	OID	Variable Names
snmpFddiPORTLemRejectsCts	1.3.6.1.2.1.10.15.4.2.1.16	Link_error_rejection
snmpFddiPORTLemCts	1.3.6.1.2.1.10.15.4.2.1.17	Aggregate_link_error_count
fddimibPORTLemRejctsCts	1.3.6.1.2.1.10.15.73.5.2.1.16	Link_error_rejection
fddimibPORTLemCts	1.3.6.1.2.1.10.15.73.5.2.1.17	Aggregate_link_error_count

Table 33. FDDI Port Fault Panel - FDDI_Port_Fault

Mib Attribute Name	OID	Variable Names
snmpFddiPORTLCTFailCts	1.3.6.1.2.1.10.15.4.2.1.14	Confidence_test_failure
fddimibPORTLCTFailCts	1.3.6.1.2.1.10.15.73.5.2.1.14	Confidence_test_failure

Table 34. FDDI MAC Fault - Error Counters Panel - FDDI_MAC_Fault_Errors_Counters

Mib Attribute Name	OID	Variable Names
snmpFddiMACErrorCts	1.3.6.1.2.1.10.15.2.2.1.21	Error
snmpFddiMACLostCts	1.3.6.1.2.1.10.15.2.2.1.22	Lost
fddimibMACErrorCts	1.3.6.1.2.1.10.15.73.2.2.1.24	Error
fddimibMACLostCts	1.3.6.1.2.1.10.15.73.2.2.1.25	Lost
fddimibMACTvxExpiredCts	1.3.6.1.2.1.10.15.73.3.1.1.2	Tvx_expired
fddimibMACNotCopiedCts	1.3.6.1.2.1.10.15.73.3.1.1.3	Copy_failure
fddimibMACLateCts	1.3.6.1.2.1.10.15.73.3.1.1.4	Late
fddimibMACRingOpCts	1.3.6.1.2.1.10.15.73.3.1.1.5	Ring_opeartional_count

Table 35. FDDI MAC - Copy Failure Counters Panel - FDDI_MAC_Copy_Failure_Counters

Mib Attribute Name	OID	Variable Names
fddimibMACNotCopiedRatio	1.3.6.1.2.1.10.15.73.3.1.1.6	Not_copied_ratio

Traps

For information on traps, refer to “Chapter 28. Traps” on page 255

Part 8. Understanding Messages

Chapter 41. Files and Daemons

This chapter explains where the LAN Network Manager files are installed during the installation process and describes the daemons that begin running when you start LAN Network Manager.

LAN Network Manager Files

When the installation process is complete, the LAN Network Manager product files are installed in the following directories:

Directory
Type of Files

/usr/lpp/cml
This directory contains all the files needed to install and to handle SMIT configuration.

/usr/CML/app-defaults/C
Application default X resource definitions

/usr/CML/backgrounds
Device-specific background maps

/usr/CML/bin
Executable files

/usr/CML/bitmaps/C
LAN Network Manager icons

/usr/CML/conf
Configuration files

/usr/CML/data

/usr/CML/databases
Databases or data flat files

/usr/CML/help
Help text

/usr/CML/fields
LAN Network Manager fields

/usr/CML/filters
Filter strings

/usr/CML/gifs
GIF files

/usr/CML/man
Manual page entries

/usr/CML/nls
Message catalogs

/usr/CML/registration
Registration files

/usr/CML/reports
Files related to report generation, including history files

/usr/CML/sockets
Sockets for interprocess communication

/usr/CML/symbols/C
Symbol files

LAN Network Manager Files Installed in NetView for AIX Directories

LAN Network Manager product files are also linked in the following NetView for AIX directories:

Directory	Type of Files
/usr/OV/bitmaps/C	LAN Network Manager bitmaps used by OVW
/usr/OV/backgrounds	LAN Network Manager backgrounds used by OVW
/usr/OV/conf/C	Contains the lnm.oid_to_sym file modified by LAN Network Manager
/usr/OV/fields/C	LAN Network Manager fields used by OVW
/usr/OV/filters	LAN Network Manager filters used by OVW
/usr/OV/registration/C	LAN Network Manager registration files
/usr/OV/snmp_mibs	LAN Network Manager SNMP MIB definitions
/usr/OV/symbols/C	LAN Network Manager symbols used by OVW
/usr/OV/help/C/lnm	LAN Network Manager help files

LAN Network Manager Daemons and Executables

The LAN Network Manager component invokes several daemons and executables (shell scripts and compiled programs). These daemons and executables are stored in the `/usr/CML/bin` directory. The following list briefly describes the daemons and executables. For more detailed information, refer to the online man page for the specific daemon or executable. To display a man page, type:

```
man topic
```

Where topic is the name of the daemon or executable for which you want more information.

Process Name	Description
nvot_server	Maintains Nways Manager-LAN topology database.
cmld	Manages lnmtopod and the monitoring applications that are part of

LAN Network Manager and provides a communication channel for the LAN Network Manager command line interface.

cml_agent_found
Initiates the discovery of a specified agent.

cml_agent_remove
Stops monitoring an agent.

lnmexport Converts current week performance data collected by the OS/2 agent to a spreadsheet-readable delimited format.

lnmfddimgr Manages the LAN Network Manager FDDI application.

lnmfddimon FDDI SNMP Proxy Agent monitor process.

lnmlnmeint Manages the sending of run command requests to the LNM OS/2 Agents from LAN Network Manager and the receiving of the run command responses from the LNM OS/2 Agents by LAN Network Manager.

lnmlnmemgr Manages the LAN Network Manager LLC token-ring application.

lnmlnmemon OS/2 agent monitor process.

cmlstart Starts a specific daemon.

cmlstop Stops a specific daemon.

cmlsm Contains the Symbols Manager files (see the online book **User Interface** for more information).

cmlstatus Displays the status of the LAN Network Manager daemon processes.

lnmtopod Provide monitoring and management support by integrating multiprotocol networks into a single LAN interconnect topology hierarchy.

lnmbrmon SNMP Bridge monitor process.

lnmbrmgr Manages the LAN Network Manager SNMP bridge application.

lnmtrmon SNMP token-ring monitor process.

lnmtrmgr Manages the LAN Network Manager SNMP token-ring application.

lnmhubint Communicates with the Hub Manager iubd daemon to manage the LAN Network Manager Hub Manager integration function.

Note: If the **nvot_server** daemon stops, ensure that the **/var** directory is not more than 70% full.

LAN Network Manager Performance Data Files

The files used for segment and bridge performance data are stored in the `/usr/CML/reports/lnmlnmemon/dir_name` directory, where `dir_name` is the IP address of the OS/2 agent that manages the segment that is collecting the data.

There are two types of files used to store segment and bridge performance data, each with the following naming structure:

```
yyyxxx.history.nn
```

Where `yyy` is either `seg` or `brg`, `xxx` is either the number of the segment or the symbolic name of the bridge, and `nn` is either `01` or `02`. The extension `01` is used to store data that is currently being collected. The extension `02` is used to store data from the data collection period that has most recently completed.

For example, the file `seg005.history.01` stores performance data for segment 005 from a collection period that is currently active. When this collection period ends, the file is renamed `seg005.history.02`, replacing the file currently using that name, if necessary.

If you display a segment or bridge performance graph using the **Graph History** push button on the Segment Performance or the Bridge Performance Graphing window, the data from the `01` file is displayed, unless the `01` file does not exist, in which case the historical data in the `02` file is displayed. If data has never been collected for a segment or bridge and neither file exists, the LAN Network Manager program cannot display a performance graph.

Chapter 42. Problem Determination

This chapter describes problems you might experience while using the LAN Network Manager program and suggests how to resolve these problems. Refer to the `/usr/CML/lpp.README` file for additional information that might help you resolve problems.

If you experience problems with the LAN Network Manager program, first attempt to identify and solve the problem yourself. The "Gathering Problem Information" section describes tools you can use to help you obtain more information about the status of the LAN Network Manager program and the events that occur while you are using the program. The sections that follow describe specific problems and suggest how to resolve them. Specifically, this chapter includes the following topics:

If you cannot solve a problem with the information in this chapter, call the IBM Technical Support Center in the United States. The phone number is **1 (800) 237-5511**. Customers outside of the United States should contact their country's support center. When you call, be prepared with your customer number, your LAN Network Manager for AIX component ID, and a description of the problem. You can use the worksheet in "Problem Documentation Worksheet" on page 364 to help you gather the necessary information. It is helpful if you can recreate the problem; otherwise, the Technical Support Center personnel will attempt to do so.

Gathering Problem Information

If you experience problems with the LAN Network Manager program, the following tools might help you or IBM Technical Support Center personnel identify the problem:

- cmlstatus command
- nettl log
- kill -31 command
- Clearing the LAN Network Manager databases

Displaying LAN Network Manager Status Information

The **cmlstatus** command reports the status of each LAN Network Manager daemon configured to operate. You can use the **cmlstatus** command to determine the current status of the LAN Network Manager daemons, their process identifiers (PIDs), and their exit statuses. For specific information about the possible exit statuses that can be returned by the **cmlstatus** command, refer to the man page.

Checking the nettl Log

If a change that you did not expect takes place on the graphical interface or conversely if an expected change fails to take place, consult the nettl log to determine what might have happened with the resources and applications involved.

It is recommended that you use nettl logging whenever you are operating the LAN Network Manager program.

For example, if you attempt to manually discover an LNM OS/2 agent but no icon is created on the LAN Network submap, it is possible that you have not created a configuration file for that agent. If this is the case, the nettl log will contain an entry identifying the agent by its internet address and explaining the cause of the error. Knowing this, you can then create a configuration file with SMIT and rediscover the agent.

For more information about the format of the nettl log and how to view its contents, refer to “Chapter 43. Using NetView for AIX Logs” on page 367.

Clearing LAN Network Manager Databases

Clearing the LAN Network Manager databases is necessary to resolve certain problems. However, before you clear the LAN Network Manager databases:

- Stop all LAN Network Manager applications with the **ovstop cmld** command.
- Ensure the nvot_server and ovwdb processes are running.

Clear the LAN Network Manager databases in the following situations:

- If there is an abnormal termination of the lnmtopod process.
- If there is an abnormal termination of the nvot_server or ovwdb processes. If one of these processes is abnormally terminated, follow these steps before clearing the databases:
  1. Stop the NetView for AIX graphical interface.
  2. Issue the **ovstop** command.
  3. Issue the **ovstart** command.

  If any of the other NetView for AIX processes are abnormally terminated, it is also recommended that you follow the previous steps before clearing the databases.

General LAN Network Manager Problems

This section lists problems you might encounter using the LAN Network Manager program that are not obviously associated with a specific LAN Network Manager application. For information about problems that are clearly associated with a specific LAN Network Manager application, see later sections in this chapter.

Agent Discovery

If you attempt to manually discover an agent but an icon representing the subnet that the agent manages does not appear on the LAN submap, or the icon that represents the agent is blue, look in the nettl log for information about the problem, and ensure that the agent program is running.

Not Receiving Traps

If you are not receiving traps from an agent program in your network, begin by looking for a mismatch between community names and ensure you have activated the LAN Network Manager filter.

Mismatched Community Names

For LAN Network Manager to receive traps properly, the community name specified at the agent workstation must match the community name defined for that agent in NetView for AIX. To ensure that trap authentication is correctly configured check the following:

- Verify that the community name on the agent workstation matches that on NetView for AIX.

  If they do not match, you can change the agent community name to match the default community name defined in NetView for AIX, or you can define a node-specific community name for the agent on the SNMP Configuration window in NetView for AIX.
- Verify that the SNMP password file exists on the agent workstation.

Inactive Filter

If you are receiving agent traps but they are not being displayed in the NetView for AIX event display, you may need to activate the LAN Network Manager filter file. This filter specifies which LAN Network Manager traps are to be displayed in the event display.

To activate the LAN Network Manager filter, follow these steps:

1. Select **Filter control** from the Operations pull-down menu on the NetView for AIX event card display. The Filter Control window is displayed.
2. Select the **File List** push button. The File Selection window is displayed.
3. Select **/usr/OV/filters/lnm.filter** from the Files list and select the **OK** push button. When you are returned to the Filter Control window, the lnmCustomer filter is listed in the Available Filters in File list box.

4. Select **lnmCustomer** from the list and then select the **Activate** push button. The lnmCustomer filter is moved to the Active Filters List and is immediately activated.
5. Select the **Close** push button to close the window and apply the changes.

You can deactivate the filter by selecting the filter on the Filter Control window and selecting the **Deactivate** push button.

LAN Icon is Not Displayed in Root Submap

If the LAN icon does not appear on the Root submap, verify the following conditions:

- The **ovwdb** and **iubmap** and **nvot_server** processes are running.
- The **ovwdb** and **nvot_server** processes are attached to the **ovspmd** process.
- The **lnmtopod** process is running.

If these conditions are true and the LAN icon still does not appear in the Root submap, clear the LAN Network Manager databases.

Icons of SNMP Bridges in LAN Subnet Submaps Are Blue

If the icons of SNMP bridges in LAN Subnet submaps are blue (unknown), check the status of the lnmbrmon daemon by entering the command:

```
/usr/CML/bin/cmlstatus lnmbrmon
```

If lnmbrmon is not running, restart it by entering:

```
/usr/CML/bin/cmlstart lnmbrmon
```

Adapter Problems

Protocol switching is disabled for duplicate MAC addresses within the LAN Network Manager domain.

OS/2 Agent Application Problems

If you experience problems that seem to be associated with the OS/2 agent application, first follow the general problem determination suggestions in “Gathering Problem Information” on page 349. Other sources of information that may be helpful include the following:

Verify the connection

Use xnmbrowser of the NetView for AIX platform to query the SNMP agent on the LNM OS/2 agent workstation. In addition to defining the trap destination on the LNM OS/2 workstation, the COMMUNITYNAME must be set in CONFIG.SYS for traps to be forwarded to a NetView AIX workstation. Use `netstat -s` on the LNM OS/2 workstation to verify port assignment.

nettl log (see “Checking the nettl Log” on page 350)

Trap numbers for OS/2 agent-initiated traps correspond to DFI message numbers. Use the LAN Network Manager for OS/2 Version 2.0 documentation to resolve errors reported by traps. You will have to read the trap description to distinguish between traps with the same trap number.

Run command return codes written to the nettl log by the OS/2 agent monitor program (lnmlnmemon) usually correspond to DFI messages numbers in the LAN Network Manager for OS/2 Version 2.0 documentation. Exceptions are noted in the documentation for message 610 in “Chapter 44. Messages” on page 369.

A “1” has been appended to the DFI message number for the messages displayed by the LNM OS/2 Agent application if there is a matching DFI number.

Execute cmlstatus to determine the state of the OS/2 agent monitor program. Refer to the man page for cmlstatus for a description of the exit statuses provided by cmlstatus.

Save formatted nettl logs and the trapd.log.

Save the core image or output from the dbx command.

Execute `ps -ef | grep lnm` to ensure that the following conditions exist:

– lnmlnmemon is running and is the parent of an instance of lnmBaseTimer and lnmlnmeint. *lnmlnmemon* must be a child of cmld. If it is not, refer to messages 613 and 635 in “Chapter 44. Messages” on page 369.

– lnmlnmeint is running and is the parent of an instance of lnmBaseTimer. If it is not, refer to message 820 in “Chapter 44. Messages” on page 369.

– lnmlnmemgr is running. Attempting to bring up a window will restart lnmlnmemgr.

– lnmtopod is running. The OS/2 agent application fails if lnmtopod is not running.

– No LAN Network Manager processes should be direct children of the init process

If the problem is repeatable, tracing files are extremely useful. You can start tracing on both the lnmlnmeint and lnmlnmemon daemons.

– Start tracing on lnmlnmeint to log the command flow between LAN Network Manager and the OS/2 agent program.

– If you start tracing on lnmlnmemon you will log data which in conjunction with the log from lnmlnmeint should help resolve problems when the call stack from the core dump is not enough.

  Before starting tracing on lnmlnmemon, ensure that lnmlnmemon has started the lnmlnmeint and lnmBaseTimer processes by entering:

  ```
  ps -ef | grep lnm
  ```

  To obtain a complete log, turn off automatic agent discovery and execute cml_agent_found after executing the **kill -31** command.

Agent Discovery

If you have defined the agent program in SMIT and created a configuration file for the agent, but the configuration file is not found, the following message is added to the nettl.log file:

```
Error Cannot open file = /usr/CML/conf/lnmlnmemon/<IP address of
agent>.conf
```

In order to correctly discover LAN devices:

- LNM OS/2 agents must use PTF UN64092 for TCP/IP OS/2 Version 2.
- LNM OS/2 agents must be configured for a NetView for AIX connection. The default is `no connection`.
- The resync parameter of LNM OS/2 agents must be set to a value greater than the amount of time you expect LAN Network Manager to take to complete the agent discovery. If the LNM OS/2 agent informs LAN Network Manager that it is resynchronizing while LAN Network Manager is discovering the agent's domain, LAN Network Manager stops the discovery and restarts only after the LNM OS/2 agent has completed resynchronization. If the LNM OS/2 agent resync interval is too small, there is not sufficient time for LAN Network Manager to successfully discover the agent.
- If you have overlapping LNM OS/2 agents, protocol switching will not work for adapters known to both agents. Protocol switching is a function of NetView for AIX and has the restriction that the protocol-MAC pair must be unique. Overlapping LNM OS/2 agents violate this restriction.

Congested Adapters

An adapter may show incorrect status if its status is marginal and the segment to which it is attached is resynchronized. When a segment is resynchronized, the status of congested adapters is reset to normal. Therefore, whenever a segment is automatically or manually resynchronized, any adapters that show a marginal status (yellow) are reset to normal status (green) after the segment is successfully resynchronized.

Monitored Adapters

If you are monitoring an adapter and move it to another ring, the initial monitored adapter not responding trap will be processed against the adapter on the original ring. The monitor adapter responding clear trap will be processed on the new ring. A resync of the ring on which the adapter was previously located should reset the status of the adapter in the old location to unknown. Alternatively, if you know you are going to move a monitored adapter, you can set monitoring off before you move the adapter and set it back on after the adapter has been relocated.

Inactive Adapters

No connections are displayed for inactive stations.

Remote Program Update for 8230 Models 1 and 2

Twenty minutes have been added to the normal time-out value for this request. Successful completion of the request is recorded in /usr/OV/log/trapd.log as trap 465. Trap 465 is defined as LOGONLY. It will not display in the event window. Possible error

conditions (traps 464, 466, 468, 439) will display in the event window. If the execution of the load takes more than allotted time-out value, you may receive a false time-out message.

Multiport Bridges

Until a bridge has been linked, the LNM OS/2 agent does not know if the bridge has the potential to be a multiport bridge. LAN Network Manager will place a symbol on the agent submap for each undefined bridge. If it is later determined that the bridge has the potential to be a multiport bridge, LAN Network Manager will delete the symbol from the agent submap.

Resource Status

The status for a resource displayed by the OS/2 agent on the OS/2 agent workstation may differ from the status displayed for the resource by LAN Network Manager. For example:

- A concentrator may have a normal status but is not within the OS/2 agent managed domain. It will be displayed as unknown by LAN Network Manager.
- A segment may have a normal status but there is no configuration information available. The segment will be displayed as unknown by LAN Network Manager. One place this occurs is when a CISCO router is acting as a bridge but CRS is turned off.
- A bridge adapter defined to the OS/2 agent will show an unknown status by LAN Network Manager if the bridge is not linked, even though the status of the adapter itself may be active.

Permanent Hourglass on OS/2 Agent Windows

If a window displays a permanent hourglass symbol, cancel the window from the system menu, then repeat the operation. If the window hangs again, cancel the window and terminate the process lnmlnmemgr. Retrying the operation will restart lnmlnmemgr. In most cases this should resolve the problem.

If commands are flowing from LAN Network Manager to an OS/2 agent and back successfully, requests will time out in the normal course of events if the OS/2 agent does not respond within the allotted time. The allotted time is determined by the number of commands already sent to the OS/2 agent for which no response has yet been received multiplied by the sum of the timeout values for LAN Network Manager and for the OS/2 agent. If a problem develops and the OS/2 agent is unable to respond, the application generates a trap stating that the OS/2 agent is not responding. If this problem continues for a long time, eventually the maximum number of requests which can be sent to the agent until a response is received will be reached. An external symptom of this problem is a permanent hourglass. Close the window using the System menu and restart the OS/2 agent that is not functioning.

Deleting LNM OS/2 Agents

If you delete an agent from SMIT or use cml_agent_remove, open management windows for that agent remain open. Close the windows that are associated with the deleted agent.

Managing the Same Segment Using LNM OS/2 and SNMP Token-Ring Agents

If you manage the same segment using an LNM OS/2 agent and an SNMP token-ring agent, both management applications in LAN Network Manager will respond to window requests.

Also, if you have an 8230 Model 003 or Model 013 on the ring, you may loose the capability to manage the 8230 Model 003 or Model 013 as a concentrator.

Trap Correlation

Traps generated from a token-ring segment on the other side of a transparent bridge lose their routing information at the transparent bridge. If the monitor program receives a trap from the agent that does not have the correct routing information, it will be correlated to the agent submap.

Traps received while the agent is in an unknown state may not be correlated since the view will be refreshed when the agent can be rediscovered.

Traps generated by the LNM OS/2 agent for a bridge that the LNM OS/2 Version 2 classifies as a multiport bridge when it responds to LAN BRG QUERY NAME=<bridge name> ATTR=RPT will be correlated to the agent submap and no other action will be performed.

Message 610 - Return Code 500

If message 610 with return code 500 is in the nettl log for SEGMENT UTIL with the agent IP address but no segment number (for example, 9.67.167.11), the agent configuration file is corrupted. Delete the agent using the Delete LNM OS/2 Agent option in SMIT, then add the agent using SMIT and rediscover it.

Integration with 8250, 8260, and 8265 Device Manager

This function is not supported for token-ring segments managed by the LNM OS/2 agent.

SNMP Token-Ring Application Problems

If you experience problems that seem to be associated with the SNMP Token-Ring application, follow the general problem determination suggestions in “Gathering Problem Information” on page 349. Next, check the following sources of information:

nettl log (see “Checking the nettl Log” on page 350) and trapd log

Execute cmlstatus to determine the state of the SNMP Token-Ring monitor program. Refer to the man page for cmlstatus for a description of the exit statuses provided by cmlstatus.

Save formatted nettl logs and the trapd.log.

Save the core image or output from the dbx command.

Execute `ps -ef | grep lnm` to ensure that the following conditions exist:

– lnmtrmon is running and is a child of the cmld process.

– lnmtrmgr is running. Attempting to bring up a window will restart lnmtrmgr.

– lnmtopod is running. The SNMP Token-Ring application fails if lnmtopod is not running.

– LAN Network Manager processes are not direct children of the init process.

If the problem is repeatable, tracing files are extremely useful. You can start tracing on the lnmtrmon daemon.

Start tracing on lnmtrmon to log the command flow between LAN Network Manager and the SNMP Token-Ring agents.

Incorrect Display of a Token-Ring Segment with Multiple Agents

An SNMP token-ring segment or device may run any of the following agents:

- Token-ring surrogate agents
- Remote monitor (RMON) agents
- Concentrator agents

LAN Network Manager retrieves different configuration information and sends different management instructions depending on whether the agent manages a segment, station, or bridge. LAN Network Manager allows only one agent (called the *primary agent*) to manage a segment or device at a given time and merges the information received from the secondary and tertiary agents to provide a single view. The primary agent is selected in the following order according to the completeness of segment or device information provided:

1. Token-ring surrogate
2. RMON
3. Concentrator

An SNMP token-ring segment or device in LAN submaps may be incorrectly displayed for any of the following reasons:

- If the connection between LAN Network Manager and the primary agent is lost, the status of a token-ring segment changes to unknown and its color changes to blue in

LAN submaps. An age-out timer starts. When the age-out timer expires, the unknown segment is deleted from LAN submaps. The secondary agent then assumes management and updates LAN submaps with its own information.

To resolve the problem, delete the agent in one of the following ways before the age-out timer for the primary agent expires:

- Enter the command `/usr/CML/bin/cml_agent_delete <ip_address>` where `<ip_address>` is the IP address of the primary agent.
- In the LAN submap, delete the primary agent and re-configure it. Then use SMIT to re-discover the primary agent.

- The information provided by the agent in an SNMP-managed 8230 token-ring concentrator is successfully merged into the segment view provided by the token-ring surrogate or RMON agent managing the segment. The 8230 token-ring information is not, however, merged into the corresponding SNMP Bridge submap.

  You can resolve this problem for 8230 concentrators with microcode at Version 5.30 or higher by enabling the RMON agent in the concentrator so that the concentrator information is merged into the Bridge submap. To change the configuration of the RMON agent, use SMIT as described in the online book **Coupling and Autodiscovery**.
- If an RMON agent reports the MAC addresses of token-ring stations in canonical format, the information may not be merged in the Token-Ring Segment view. This is because LAN Network Manager requires MAC addresses reported in ringStationGroup by RMON agents to be in non-canonical format in order to merge the station information.

  To resolve this problem, use SMIT to reconfigure the RMON agent. To do so, enter `smit cml` to start SMIT and select **Configure -> Configure SNMP Token-Ring application -> Configure IBM SNMP proxy agent -> RMON proxy agent**.

Incorrect Display of a Token-Ring Segment with 8250 Bridge

The status of an SNMP token-ring segment with one or more 8250 bridges attached may be incorrectly displayed as marginal (yellow) when it really has normal (green) status. This is because the Token-Ring Management Module sometimes reports soft errors when the status of an 8250 bridge is normal. This is a known problem.

Token-Ring Segments Using Token-Ring Surrogates Are Not Discovered

Token-Ring segments using token-ring surrogate agents are not discovered by LAN Network Manager unless configReportServer (CRS) and ringErrorMonitor (REM) are running. When using token-ring surrogates to manage token-ring resources, ringParameterServer (RPS) is not required.

Incorrect Hourglass on SNMP Token-Ring Windows

If a window displays a permanent hourglass symbol, try to cancel the window from the system menu, then repeat the operation. If the program still hangs, stop and restart LAN Network Manager.

SNMP Configuration

If you change the IP address parameter of an SNMP token-ring agent using SMIT, the change is not taken into account by the SNMP Token-Ring application until you do one of the following:

Stop and restart the SNMP Token-Ring daemon

Delete the agent, then reconfigure and rediscover it using SMIT.

Managing the Same Segment Using SNMP Token-Ring and LNM OS/2 Agents

If you manage the same segment using an SNMP token-ring agent and an LNM OS/2 agent, both management applications in LAN Network Manager will respond to window requests.

Also, if you have an 8230 Model 003 or Model 013 on the ring, you may loose the capability to manage the 8230 Model 003 or Model 013 as a concentrator.

Activating Local Access Control for 8230 Concentrators

If the access control settings you defined for an individual 8230 concentrator are not active, make sure that the general access control settings defined for all token-ring segments are activated.

To activate access control for all token-ring segments, select **LAN -> Applications -> SNMP Token Ring -> Access Control Policy** from the NetView menu bar. Then set the Access Control parameter to **Active**.

For more information, see the section “Defining SNMP Token-Ring Access Control Parameters” in the online book **Managing SNMP Token-Ring Resources**.

SNMP Token-Ring Stations are Removed From Segment Submaps

If SNMP token-ring stations are periodically removed from Segment submaps, check to see if access control for all token-ring segments is active and if it has been set to override the access control settings of individual segments. This sometimes occurs when another network operator changes the global default settings.

To check access control for all token-ring segments, select **LAN -> Applications -> SNMP Token Ring -> Access Control Policy** from the NetView menu bar.

In the SNMP Token-Ring - Access Control Policy window, note the current settings of the Access Control and Overwrite Resource-specific parameters. If necessary, you can make either of the following changes:

- Reset the Access Control parameter to **Inactive**.
- Reset the Overwrite parameter to **No**.

For more information, see the section ″Defining SNMP Token-Ring Access Control Parameters″ in the online book **Managing SNMP Token-Ring Resources**.

SNMP Bridge Application Problems

If you experience problems that seem to be associated with the SNMP bridge application, follow the general problem determination suggestions in “Gathering Problem Information” on page 349. Next, check the following sources of information:

nettl log (see “Checking the nettl Log” on page 350) The errors logged in the nettl log for the SNMP bridge application include SNMP bridge agent errors that can indicate possible hardware and configuration problems.

Save the core image file

MIB browser dump of the MIB

To obtain MIB browser dump of the MIB, follow these steps:

1. Select **MIB browser: SNMP** from the NetView for AIX Tools pull-down menu.
2. Select **mgmt** from the Browse MIB window.
3. Enter the IP address and community name of the bridge.
4. Select **Start Query**.
5. Select **Save** to save the output of the dump.

If the problem is repeatable, tracing files are extremely useful. You can start tracing on the lnmbrmon daemons.

Start tracing on lnmbrmon to log the command flow between LAN Network Manager and the SNMP bridge agents.

SNMP Bridge Discovery Problem Determination

If you are experiencing problems related to the discovery of SNMP bridges, the following procedures might help:

Execute **cmlstatus** to ensure that lnmtopod and lnmbrmon are up and running.

Check the nettl log to see if there is a message with the IP address of the bridge and an explanation of the error.

If a bridge is in an undiscovered subnet, follow these steps:

– ping <ipAddress>

  You must have a network connection to the bridge before it can be discovered. If you cannot ping the bridge, the SNMP session to the bridge cannot be established.

– Use the MIB browser to get mgmt attributes 1.3.6.1.2.1(iso.org.dod.internet.mgmt).

  If you get a timeout, one of three things might be the problem:

  - Community name is incorrect.

    You can get a timeout if the wrong community name is specified. LNM for AIX gets the community name from NetView for AIX. To change the community name in NetView for AIX, select **SNMP Configuration** from the Options pull-down menu. If the SNMP bridge agent has a community name other than `public` you *must* define the IPAddress and the community name to NetView for AIX before LNM for AIX can discover the bridge. See the section

″Configuring General Parameters for SNMP Agents″ in the online book **Managing SNMP Token-Ring Resources and SNMP Bridges** for more information.

- It is possible that the network could be operating slowly. If this might be the case, specify the IPAddress with a greater timeout value and a greater retry interval. Most bridges have been able to work with the defaults with the exception of some OS/2 bridges. Once you get the problem resolved, be sure to set the retry and timeout values back to a normal timeout. If you keep the retry and timeout values with the maximum values, it will take half an hour to detect a bridge timeout condition.
- Bridge agent failure. If you can ping the bridge and the community name is correct you should be able to get mgmt attributes. If not, the agent in the bridge is not working properly. Check you bridge agent installation and configuration. You might also want to verify the microcode level in the bridge.

– Verify that you can get the RFC 1286 MIB attributes. 1.3.6.1.2.1.17(iso.org.dod.internet.mgmt.mib-2.dot1dBridge).

  If you can get these attributes, the bridge agent is working. If you cannot get bridge attributes, change you bridge installation (hardware, installation, microcode levels, configuration, etc..)

Ensure that RFC 1286 must be in 1.3.6.1.2.1.17. The SNMP Bridge application will not discover SNMP bridges that implement RFC 1286 in a private branch.

RouteXpander/2 Bridge Is Not Discovered

In order for a RouteXpander/2 bridge to be managed by LAN Network Manager, it must be configured with two IP addresses and the protocol must be configured in LAPS. For information on how to use LAPS to do this, refer to the RouteXpander/2 documentation.

Also, when using RouteXpander/2 bridges in your network, it is recommended that you increase the SNMP time-out parameter to 10 seconds or more. To change this value, select the SNMP Configuration option from the Options pull-down menu on the NetView for AIX menu bar.

Incorrect Display of 8227 Bridges

In order for an SNMP-managed 8227 bridge to be correctly displayed, the bridge must be Version 1.01 or higher.

Also, LAN Network Manager has a restriction that the Ethernet port is always drawn between the 10baseT port area and the AUI port. Full bridge port management is still available for the Ethernet port.

Incorrect Display of 8229 Bridges

In order for an SNMP-managed 8229 bridge to be correctly displayed, the bridge must be one of the following versions:

- Token-Ring/Token-Ring (STRT.X) - Version 1.00.12 or higher

- Token-Ring/Ethernet (STREE.X) - Version 2.01.04 or higher

Also, these versions of the 8229 bridge have a known problem that causes the ring utilization parameter to be always reported as 0.

Incorrect Display of 8271 Bridge Ports

The following limitations apply to the display of bridge ports and bridges attached to the 8271 Model 001 Switch:

- Because the 8271 Model 001 does not report interfaces correctly, all bridge ports in the Bridge submap appear to be assigned to the first interface. Full management of 8271 Model 001 Ethernet ports is available by double-clicking on the first interface and displaying the context menu. This is a known problem.
- Because 8271 Model 001 reports all bridge ports under one interface, the 8271 module does not display connections to other bridges on LAN submaps.
- 8271 bridge ports are not displayed if the IP address of the daughter card is different from the IP Address of the 8271 switch.

Incorrect Display of 8272 Bridge Ports

The following limitations apply to the display of bridge ports on the 8272 Switch:

- 8272 bridge ports are not displayed if the IP address of the daughter card is different from the IP Address of the 8272 switch.

Incorrect Display of 8281 Bridges

In submaps of 8281 bridges, LAN Network Manager has a restriction that the Ethernet AUI port is always drawn in the 10base-T port area. Full bridge port management is still available for the AUI port, but the icon is not placed above the AUI port on the submap.

Also, 8281 modules currently report the same sysOid as 8281 standalone bridges. As a result, LAN Network Manager discovers the 8281 module and displays it as a standalone bridge. This is a known problem.

Incorrect Display of Synoptics Bridges

LAN Network Manager currently has a problem obtaining correct values from the SNMP agent in SynOptics bridges (Model 3522 with microcode version 2.2 and boot code version 2.1).

LAN Network Manager issues a single get request with multiple OIDs, rather than multiple gets with a single OID. However, when LAN Network Manager makes a get request having more than one OID, the SynOptics bridge SNMP agent does not always return the correct values for the OIDs requested.

For example, when the LAN Network Manager issues a get request with the OIDs 1.3.6.1.2.1.17.2.15.1.9.1 and 1.3.6.1.2.1.17.2.15.1.9.2, one of the values that the SNMP

agent in the SynOptics bridge returns overwrites the other. This causes LAN Network Manager to incorrectly display the segment connectivity of the bridge.

FDDI Application Problems

If you experience problems that seem to be associated with the FDDI application, follow the general problem determination suggestions in “Gathering Problem Information” on page 349. Next, check the following sources of information:

nettl log (see “Checking the nettl Log” on page 350) and trapd log

Execute cmlstatus to determine the state of the FDDI application. Refer to the man page for cmlstatus for a description of the exit statuses provided by cmlstatus.

Save formatted nettl logs and the trapd.log.

Save the core image or output from the dbx command.

Execute `ps -ef | grep lnm` to ensure that the following conditions exist:

– lnmfddimon is running and is a child of the cmld process.
– lnmfddimgr is running. Attempting to bring up a window will restart lnmfddimgr.
– lnmtopod is running. The FDDI application fails if lnmtopod is not running.
– LAN Network Manager processes are not direct children of the init process.

MIB browser dump of the MIB. If a station does not show all of its sub-objects (for example, path, path class, attachment), look at a MIB browser dump of the MIB.

To obtain MIB browser dump of the MIB:

1. Select **MIB browser: SNMP** from the NetView for AIX Tools pull-down menu.
2. Select **mgmt** from the Browse MIB window.
3. Fill in the IP address and community name of the bridge.
4. Select **Start Query**.
5. Select **Save** to save the output of the dump.

FDDI Devices Are Not Discovered

When using the FDDI SNMP proxy agent in your network, it is recommended that you increase the SNMP time-out parameter to 10 seconds or more. To change this value, select the SNMP Configuration option from the Options pull-down menu on the NetView for AIX menu bar.

Also, the FDDI SNMP proxy agent Version 6.0 incorrectly reports `private.enterprises.ibm.ibmArchitecture.fddi.fddismt73ext.snmpFddiConfig` as `5.9` and LAN Network Manager displays this information.

Integration Problems with 8250, 8260, and 8265 Device Manager

If you experience problems integrating Hub Manager with LAN Network Manager, follow the general problem determination suggestions in “Gathering Problem Information” on page 349. Next, check the following sources of information:

Ensure that you have defined Hub Manager as an application to be started on the SMIT Applications to be Started When LNM for AIX Starts menu.

Verify that NetView for AIX has discovered the hub.

Ensure that lnmhubint is running using the **cmlstatus** command.

Ensure that iubd is running using the **ovstatus** command.

nettl log (see “Checking the nettl Log” on page 350) and trapd log.

Execute cmlstatus to determine the state of the 8250, 8260, and 8265 Device Manager application. Refer to the man page for cmlstatus for a description of the exit statuses provided by cmlstatus.

Save formatted nettl logs.

Save the core image or output from the dbx command.

Execute `ps -ef | grep lnm` to ensure that the following conditions exist:

– lnmhubint is running and is a child of the cmld process.
– lnmtopod is running. The Hub Manager integration fails if lnmtopod is not running.
– LAN Network Manager processes are not direct children of the init process.

Problem Documentation Worksheet

Use the following worksheet to gather information about a LAN Network Manager problem. If you call the IBM Technical Support Center for assistance, this information can be helpful.

Customer Information

Customer number
Nways Campus Manager LAN for AIX component ID
Problem symptoms

Software Version Levels and Applied PTFs on the LAN Network Manager Workstation

AIX operating system
Motif and X11
NetView for AIX
Nways Campus Manager LAN for AIX
Agent programs possibly involved in the problem

Hardware Configuration of the LAN Network Manager Workstation

Amount of memory (RAM) installed
Amount of paging space available
Amount of free space available in the file system that contains
`/usr/OV`

Amount of free space available in `/tmp`

AIX NetView/6000 Considerations

Which NetView for AIX applications were running at the time of the problem?

Which mode was NetView for AIX operating in at the time of the problem? ☐ Read ☐ Read-Write

What is the size of the network you are managing?

- Number of stations
- Number of bridges
- Number of concentrators
- Number of objects in the OVw database (use the command **ovobjprint | head**)
- Number of objects to hold in ovwdb cache

Additional Problem Information

Have the following information available when you call the IBM Technical Support center:

cmlstatus

Issue the **cmlstatus** command and direct the output to a file, which you can print and have available when working with the IBM Technical Support Center. To create the output file, enter the following command at an AIX command line:

```
cmlstatus > cmlstatus.output
```

You can then print the `cmlstatus.output` file.

See “Displaying LAN Network Manager Status Information” on page 350 for more information about the **cmlstatus** command.

Log Files

To ensure that you have a record of events that occurred when the problem arose, save the following log files:

– /usr/OV/log/trapd.log

– /usr/OV/log/nettl.log

See “Chapter 43. Using NetView for AIX Logs” on page 367 for more information about LAN Network Manager logging.

Core Image

A possible additional source of information about your problem is the core image that might have been created for an LAN Network Manager executable. Perform the following steps to locate and save the core image:

1. Check the root directory for the LAN Network Manager monitor core images.

2. Check the directory from which you started NetView for AIX for LAN Network Manager management application core images.
3. When you locate a core image, look at the file and determine if it seems reasonable that this core image is associated with your problem.
4. For each core image that you locate, determine the executable to which it belongs by issuing the following command from the directory in which the image is located and examining the output:

   ```
   /usr/bin/od -c core 3274 | head
   ```

5. Execute dbx using the **t** or **where** command and save the output, or save the core image.

Chapter 43. Using NetView for AIX Logs

In addition to graphically displaying the configuration and status of your LAN, LAN Network Manager uses the nettl and trapd logs provided by NetView for AIX to record notifications from the LAN Network Manager applications and agents. The nettl command is used to turn logging on and off. When nettl logging is turned on, errors encountered by NetView for AIX and the products that run with it, such as LAN Network Manager, are documented in the nettl log. The messages logged in the nettl log can indicate such conditions as an agent that cannot be discovered or an error that has occurred with a specific LAN Network Manager application.

NetView for AIX receives and logs all traps from the network and then forwards specific traps from LAN Network Manager agents to LAN Network Manager. LAN Network Manager processes these traps (with a few exceptions) and sends them back to NetView for AIX, where they are logged with the traps from other programs, such as Systems Monitor/6000. To improve your troubleshooting efficiency, LAN Network Manager provides correlated trap information to NetView for AIX.

This chapter describes how NetView for AIX logs are used by LAN Network Manager.

To help identify a problem with your network or with LAN Network Manager, use the information in the log file created by the NetView for AIX **nettl** command. To start logging, enter the **nettl** command, or use the nettl option in SMIT. A log file is created to record all abnormal conditions that occur when LAN Network Manager is operating. A variety of messages are stored in the log, which describes such situations as faulty communication between LAN Network Manager applications and problems connecting to remote agents.

Issue the **netfmt** command to view the nettl log. The following example illustrates a formatted log entry:

```
*****************************NetView/6000*************************0#%
 Timestamp           : Wed Jul 06 1994 15:18:02.816821
 Process ID          : 19915             Subsystem        : OVEXTERNAL
 User ID ( UID )     : 0                 Log Class        : ERROR
 Device ID           : -1                Path ID          : -1
 Connection ID       : -1                Log Instance     : 0

 Software            : /usr/CML/bin/lnmlnmeint
 Hostname            : aixidw01.raleigh.ibm.com
-------------------------------------------------------------------------


 803 Cannot connect to LNM OS/2 Agent with internet address: 9.67.164.24
```

The subsystem that NetView for AIX associates with LAN Network Manager is identified as `OVEXTERNAL` The Log Class field shows the logging category of the message, which corresponds to one of the logging options specified when the **nettl** command was issued. The Software field indicates the specific component within LAN Network Manager that generated the message.

Included with this statistical data is a text field that explains the reason the message was logged. In this example, LAN Network Manager was unable to establish a connection with one of its agents, which is identified by its internet address.

For more detailed information about using the **nettl** command, refer to *AIX SystemView NetView/6000 Problem Determination*.

Chapter 44. Messages

This chapter lists the LAN Network Manager messages you can receive when using LAN Network Manager. Messages are listed by message ID number and include an explanation of the message and suggested actions.

Messages with numbers between 1000 and 1999 are sent to LAN Network Manager from the OS/2 agent program. Refer to the documentation that is provided with the OS/2 agent for an explanation of the message and suggested actions to take to resolve the problem.

LAN Network Manager appends a “1” to the front of the message number that it receives from the OS/2 agent. Before consulting the OS/2 agent documentation, identify the appropriate message number for the OS/2 agent by removing the “1” from the number. For example, message number 1300 on LAN Network Manager corresponds to message number 300 on the OS/2 agent.

You can determine the process that generates a message by the software name given for the message in the formatted nettl log.

If you receive a message and are not able to find the message in this chapter, call IBM Service for more information. See “Chapter 42. Problem Determination” on page 349 for instructions on calling the IBM Technical Support center.

Messages 001 to 600

023 **Memory allocation error errno : <errnoValue> process id : <ProcessID>**

Meaning: The malloc() system call failed. The errnoValue indicates the particular error that malloc returned. The ProcessID indicates which application encountered the memory allocation error.

Action: If the errnoValue is 12 (ENOMEM), ensure memory storage space has not been exhausted. If the errnoValue is 22 (EINVAL), 0 bytes were being allocated by ProcessID, contact IBM Service for more information.

062 **Cannot exec the process: <Application>**

Meaning: The execl() system call failed.

Action: Verify the executable is in /usr/CML/bin. If it is not, reinstall LNM for AIX and retry the operation. If it is, exit the NetView for AIX graphical interface and then execute ovstop followed by ovstart. Verify all of the NetView for AIX daemons are running using ovstatus. Execute cmlstart.

072 **System call connect failed: Procedure <ProcedureName> File = <FileName>, Line = <LineNumber> Error <errornoValue>: <errornoText>**

Meaning: The connect() system call issued by a client in order to establish communication with a server has failed. This situation occurs if a client process attempts to connect with a server process and the server is not ready to accept the connection. The message is only important if attempts by the client application fail repeatedly.

Action: No action required. The application will attempt to recover. If this error becomes critical, the application will issue error messages that may be used to recover.

101 **Cannot open file = <file name> with access <access mode>**

Meaning: Cannot open the file with the filename and access requested.

Action: Ensure the file exists and has the correct access mode.

102 **Cannot search directory = <directory name>**

Meaning: Cannot open directory /usr/lpp/lnm/conf or one of its subdirectories.

Action: Verify that the directory exists and has the correct permissions.

104 **The number of records in file exceeds the limit = <maximum record size> passed in <configuration file> with record type value = <record type value>**

Meaning: The number of records added to the Configuration file for record type has been exceeded. Record types are:

- 1 - OS/2 agent Configuration Record
- 2 - OS/2 agent History Collection Segment Record
- 3 - OS/2 agent History Collection Bridge Record
- 4 - OS/2 agent Bridge Definition
- 5 - OS/2 agent Adapter Definition
- 6 - FDDI Agent Configuration Record
- 8 - SNMP Bridge Configuration Record
- 9 - SNMP Bridge Label Record

Action: Reduce the number of records entered into the configuration file for record type so that it does not exceed the limit.

201 **<Application name>: Cannot open LNM for AIX configuration file <Filename>**

Meaning: cmld could not open the cmld.conf file in /usr/CML/conf directory.

Action: Check the file for read access permission. If the file does not exist, either installation failed or the file has been deleted by accident. Reinstall LAN Network Manager.

202 **<Application name>: Syntax error in LNM for AIX configuration file <Filename>**

Meaning: The configuration file specified is corrupted.

Action: Reinstall LAN Network Manager.

203 **<Application name>: System call socket() failed**

Meaning: The system call socket() failed.

Action: After exiting the NetView for AIX graphical interface, stop LNM for AIX. Then execute ovstop followed by ovstart. Use ovstatus to verify the NetView for AIX daemons are running. Restart LNM for AIX.

204 **<Application name>: System call bind() failed**

Meaning: The system call bind() failed.

Action: After exiting the NetView for AIX graphical interface, stop LNM for AIX. Then execute ovstop followed by ovstart. Use ovstatus to verify the NetView for AIX daemons are running. Restart LNM for AIX.

205 **<Application name>: System call select() failed**

Meaning: The system call select() failed.

Action: After exiting the NetView for AIX graphical interface, stop LNM for AIX. Then execute ovstop followed by ovstart. Use ovstatus to verify the NetView for AIX daemons are running. Restart LNM for AIX.

206 **<Application name>: System call accept() failed**

Meaning: The system call accept() failed.

Action: After exiting the NetView for AIX graphical interface, stop LNM for AIX. Then execute ovstop followed by ovstart. Use ovstatus to verify the NetView for AIX daemons are running. Restart LNM for AIX.

207 **<Application name>: Invalid parameter**

Meaning: The parameter on the LNM for AIX service interface command is not valid.

Action: Correct and retry the command again.

208 **<Application name>: Invalid parameter count**

Meaning: Invalid number of parameters on the LNM for AIX service interface command.

Action: Correct and retry the command again.

209 **Host name size exceeded.**

Meaning: An invalid hostname was configured on the LNM for AIX service interface command (SMIT).

Action: Correct the hostname.

210 **<Application name>: cmld is not running, use ovstart cmld to start cmld**

Meaning: LNM for AIX daemon cmld is not running.

Action: Verify that the NetView for AIX daemons are running using ovstatus.

Use `ovstart cmld` to start cmld.

212 **<Application name>: Your trial period has expired. To order, please contact your IBM Representative.**

Meaning: The trial period for LNM for AIX has expired.

Action: To purchase an LNM for AIX license, please contact your IBM Representative.

216 **usage: cmlstart [clear]**

Meaning: The parameters on the `cmlstart` command are not valid.

Action: Refer to the man page for usage.

217 **usage: cml_agent_found [Object ID] [IP Address]**

Meaning: The parameters on the `cml_agent_found` command are not valid.

Action: Refer to the man page for usage.

218 **usage: cml_agent_remove [Object ID][IP Address]**

Meaning: The parameters on the `cml_agent_remove` command are not valid.

Action: Refer to the man page for usage.

219 **usage: cmlstop [clear]**

Meaning: The parameters on the `cmlstop` command are not valid.

Action: Refer to the man page for usage.

259 **<application> Timeout waiting for applications to start.**

Meaning: A cmlstart command was requested, but the application did not acknowledge the start.

Action: This may not be an error if the system is running slowly. Use the cmlstatus command to see the current status of the application.

260 **<application> Timeout waiting for agent to be found.**

Meaning: A cml_agent_found command was requested, but the agent did not respond before the timeout.

Action: This error is usually caused by a communication error with the agent. Verify the following:

1. You can ping the agent. If the ping does not work it usually indicates a physical error or a configuration error with the agent. Check cables, power, IP Addresses, hostnames, etc.
2. Bring up the mib browser (tools - Mib Browser: SNMP). Enter the IP Address or the hostname in the “Name or IP Address”. field. **Do not put anything in the community name field**. Click on “mgmt” and then select “Start Query”. A timeout it usually indicates one of the following:
   - The community name is wrong. Check the community name on the agent box and in the NetView for AIX Options pulldown “Options - SNMP Configuration”. Community names are CaSe SeNsiTiVe and must match *exactly*, including spaces as well as upper/lower case.
   - Session. LNM for AIX uses the SNMP session parameters on the “NetView for AIX Options - SNMP Configuration” pulldown. If you are getting timeouts and you can ping the box, and you have verified the community name, you may need to increase the “Timeout” and the “Retry Count” for that IP Address or Hostname.
   - Default Gateway. If everything else checks out, verify that the “Default Gateway” has been set correctly on the agent. Not all boxes have this

option, but some agents will not be able to route traffic back to the manager if this parameter is not set correctly.

3. If you have verified everything above, but you still cannot retrieve attributes in NetView for AIX's MIB browser, then contact a network specialist familiar with the box you are trying to establish a connection with. At this point you do not have a Nways Manager-LAN problem, but a problem communicating with the box.
4. In some cases it is possible to get attributes back from NetView for AIX and still have timeout errors. This is because the Mib Browser gets a single attribute at a time and Nways Manager-LAN gets multiple attributes at a time. In this case, increasing the "Timeout" or the "Retry Count" in the "Options - SNMP Configuration" should clear the problem.

---

261 <application> Timeout waiting for agent to be deleted.

Meaning: A cml_agent_delete command was requested, but the application did not respond before the timeout.

Action: This may not be an error if the system is running slowly. Use the cmlstatus command to see the current status of the application.

---

262 Topology initialization failed.

Meaning: lnmtopod failed to start.

Action: Verify that nvot_server is running by issuing the ovstatus command. If nvot_server is not running, issue the ovstart nvot_server command. If nvot_server fails to start, format the NetView for AIX nettl log and look for nvot_server error messages. See the NetView for AIX documentation for instructions on formatting the nettl log "/usr/OV/bin/netfmt -f /usr/OV/log/nettl.LOG00".

---

263 Discovery initialization failed.

Meaning: cmldiscd failed to start.

Action: No other daemons will start until the problems with the cmldiscd daemon are fixed. Format the nettl log and look for messages for the cmldisc daemon. The following command should format the NetView for AIX nettl log: "/usr/OV/bin/netfmt -f /usr/OV/log/nettl.LOG00". See the NetView for AIX documentation for information about formatting the nettl log.

---

264 <application> Timeout waiting for agent to be added.

Meaning: A cml_agent_add command was requested, but the agent did not respond before the timeout.

Action: This error is usually caused by a communication error with the agent. Verify the following:

1. You can ping the agent. If the ping does not work it usually indicates a physical error or a configuration error with the agent. Check cables, power, IP Addresses, hostnames, etc.
2. Bring up the mib browser (tools - Mib Browser: SNMP). Enter the IP Address or the hostname in the "Name or IP Address". field. **Do not put anything in the community name field**. Click on "mgmt" and then select "Start Query". A timeout it usually indicates one of the following:
   - The community name is wrong. Check the community name on the agent box and in the NetView for AIX Options pulldown "Options - SNMP Configuration". Community names are CaSe SeNsiTiVe and must match *exactly*, including spaces as well as upper/lower case.
   - Session. LNM for AIX uses the SNMP session parameters on the "NetView for AIX Options - SNMP Configuration" pulldown. If you are getting timeouts and you can ping the box, and you have verified the community name, you may need to increase the "Timeout" and the "Retry Count" for that IP Address or Hostname.
   - Default Gateway. If everything else checks out, verify that the "Default Gateway" has been set correctly on the agent. Not all boxes have this option, but some agents will not be able to route traffic back to the manager if this parameter is not set correctly.
3. If you have verified everything above but you still cannot retrieve attributes in NetView for AIX's MIB browser, then contact a network specialist familiar with the box you are trying to establish a connection with. At this point you do not have an Nways Manager-LAN problem, but a problem communicating with the box.
4. In some cases it is possible to get attributes back from NetView for AIX and still have timeout errors. This is because the Mib Browser gets a single attribute at a time and Nways Manager-LAN gets multiple attributes at a time. In this case, increasing the "Timeout" or the "Retry Count" in the "Options - SNMP Configuration" should clear the problem.

265 <agent> Timeout waiting for agent to be removed.

Meaning: A cml_agent_remove command was requested, but the application did not respond before the timeout.

Action: This may not be an error if the system is running slowly. Use the cmlstatus command to see the current status of the application.

266 <agent> There is no running capability interested in the agent_ID(s).

Meaning: An agent with an agent_ID (sysObjectID/MIB variable) was requested to be discovered, but there is no running application managing this type of agent.

Action: Make sure there is an application installed and running that manages this type of agent. Use the cmlstatus command to query the installed and running applications.

269 Discovery application is not running.

Meaning: The cmldiscd daemon is not running.

Action: Issue the ovstatus command to make sure all the NetView for AIX daemons are running properly. Once all the NetView for AIX daemons are running properly, issue the restart command to restart the desired applications. If applications do not start properly, format the nettl log and check for errors. The following command should format the NetView for AIX nettl log: "/usr/OV/bin/netfmt -f /usr/OV/log/nettl.LOG00". See the NetView for AIX documentation for information about formatting the nettl log.

270 Capability was not started because it depended on <application> capability.

Meaning: The requested application cannot be started until the required application is started.

Action: Start the required application.

271 nvot_server CONNECTION ERROR

Meaning: The nvot_server connection failed. Make sure nvot_server is running.

Action: Verify that nvot_server is running by issuing the ovstatus command. If nvot_server is not running, issue the ovstart nvot_server command. If nvot_server fails to start, format the NetView for AIX nettl log and look for nvot_server error messages. See the NetView for AIX doc for instructions on formatting the nettl log "/usr/OV/bin/netfmt -f /usr/OV/log/nettl.LOG00".

272 nvot_server DATABASE ERROR

Meaning: The nvot_server connection failed. Make sure nvot_server is running.

Action: Verify that nvot_server is running by issuing the ovstatus command. If nvot_server is not running, issue the ovstart nvot_server command. If nvot_server fails to start, format the NetView for AIX nettl log and look for nvot_server error messages. See the NetView for AIX documentation for instructions on formatting the nettl log "/usr/OV/bin/netfmt -f /usr/OV/log/nettl.LOG00".

273 Symbols Manager connection error.

Meaning: cmld could not connect to Symbols Manger. The device will not be changed to executable in the NetView for AIX maps.

Action: Restart ovw and check the nettl logs. Issue the following command to format the NetView for AIX nettl log: "/usr/OV/bin/netfmt -f /usr/OV/log/nettl.LOG00" See the NetView for AIX documentatio for information about formatting the nettl log.

275 Symbols Manager Server error.

Meaning:

cmld may have lost connection to the Symbols Manger. Some devices may not be changed to executable in the NetView for AIX maps.

Action: Restart ovw and check the nettl logs. The following command should format the NetView for AIX nettl log: "/usr/OV/bin/netfmt -f /usr/OV/log/nettl.LOG00" See the NetView for AIX documentation for information about formatting the nettl log.

276 Unexpected error on capability start: <application>.

Meaning: A cmlstart command was requested for the application and the application did not acknowledge the start.

Action: Use SMIT to verify that the requested application is installed. If the application is installed, use cmlstatus to determine the status of the application.

277 **Unexpected error on capability stop: <application>.**

Meaning: A cmlstop command was requested for the application and the application did not acknowledge the stop.

Action: Use SMIT to verify that the requested application is installed. If the application is installed, use the cmlstatus command to determine the status of the application.

301 **Change label request received for a non-existent resource. graph Protocol = <protocol> graph Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to change a label for a resource that is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

302 **Change label request received for a non-existent element. vertex Protocol = <protocol> vertex Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to change a label for a resource that is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

305 **Insert request received for a non-existent resource. graph Protocol = <protocol> graph Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to add a resource to a segment, but the resource is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

306 **Insert request received for a non-existent upstream neighbor. graph Protocol = <protocol> graph Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to add a resource downstream from a resource that is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

307 **Insert request received for a non-existent downstream neighbor.**

Meaning: An LAN Network Manager application has asked Topology Services to add a resource upstream from a resource that is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

308 **Associate request received for a non-existent device. Device Protocol = <protocol> Device Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to add an existing resource to a graph, but the resource is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

314 **Associate request received for a non-existent element. parent Protocol = <protocol> parent Name = <name> component Protocol = <protocol> component Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to add an existing element to a graph, but the resource is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

315 **Associate request received for a non-existent parent. parent Protocol = <protocol> parent Name = <name> component Protocol = <protocol> component Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to add a resource to a view that is not in the Topology Services cache. This means that a device or network has been has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

316 **Change extension request received for a non-existent resource. graph Protocol = <protocol> graph Name = <name>**

Meaning: Topology Services received a request for a resource that is not in its cache. That means that the resource has been discovered but is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

317 **Change extension request received for a non-existent element. vertex Protocol = <protocol> vertex Name = <name>**

Meaning: Topology Services received a request for an element that is not in its cache. That means that the resource has been discovered but is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

320 **Change status request received for a non-existent element. Element Protocol = <protocol> Element Name = <name>**

Meaning: Topology Services received a request for an element that is not in its cache. That means that the resource has been discovered but is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

322 **Change status request received for a non-existent arc. aEndpointName = <name> zEndpointName = <name>**

Meaning: Topology Services received a request for an arc that is not in its cache. That means that the arc has been discovered but is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

324 **Change status request received for a non-existent resource. Resource Protocol = <protocol> Resource Name = <name>**

Meaning: Topology Services received a request for a resource that is not in its cache. That means that the resource has been discovered but is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually

resynchronize the view if you know which one the resource should have been in.

326 **Change status request received for a non-existent view. graph Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to change a view that is not in the Topology Services cache. This means that a segment or network has been has been discovered that is not in any other view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

327 **Change status request received for a non-existent arcs in view. graph Protocol = <protocol> graph Name = <name>**

Meaning: Topology Services received a request for an arc that is not in its cache. That means that the arc has been discovered but is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

329 **Change contents request received for a non-existent view. View Protocol = <protocol> View Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services change a view that is not in the Topology Services cache. This means that a view has been discovered by the application but is not known to Topology Services.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

330 **Change contents request received for a non-existent device. Resource Protocol = <protocol> Resource Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services change a device that is not in the Topology Services cache. This means that a device has been discovered by the application but is not known to Topology Services.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

331 **Change type request received for a non-existent resource. graph Protocol = <protocol> graph Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services change a resource that is not in the Topology Services cache. This means that a resource has been discovered by the application but is not known to Topology Services.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

332 **Change type request received for a non-existent element. vertex Protocol = <protocol> vertex Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services change an element that is not in the Topology Services cache. This means that an element has been discovered by the application but is not known to Topology Services.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

339 **Create arc request received for a non-existent endpoints. aEndpointProtocol = <protocol> aEndpointName = <name> zEndpointProtocol = <protocol> zEndpointName = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to create an arc between endpoints that are not in the Topology Services cache. This means that the endpoints have been discovered but are not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

340 **Delete request received for a non-existent view. graph Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services to delete a view that is not in the Topology Services cache. This means that a segment or network has been has been discovered that is not in any other view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

341 **Delete request received for a non-existent arc. aEndpointName = <name> zEndpointName = <name>**

Meaning: Topology Services received a request for an arc that is not in its cache. That means that the arc has been discovered but is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

342 **Delete request received for a non-existent resource. graph Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services delete a resource that is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

343 **Delete request received for a non-existent element. vertexName = <name>**

Meaning: An LAN Network Manager application has asked Topology Services change an element that is not in the Topology Services cache. This means that an element has been discovered by the application but is not known to Topology Services.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

346 **Root not found when executing delete Protocol. Database is empty.**

Meaning: Topology Services cannot find the LAN Network Manager for AIX graph in the NetView for AIX database. Therefore, it cannot look for the children of that graph and delete the ones that match the requested protocol.

Action: None.

347 **Remove request received for a non-existent resource. graph Protocol = <protocol> graph Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services remove a resource that is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

348 **Remove request received for a non-existent downstream neighbor.**

Meaning: An LAN Network Manager application has asked Topology Services remove a resource from a

segment, but the downstream neighbor of the resource is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

---

349 **Remove request received for a non-existent upstream neighbor.**

Meaning: An LAN Network Manager for AIX application has asked Topology Services remove a resource from a segment, but the upstream neighbor of the resource is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

---

350 **Connection with Topology already established.**

Meaning: An LAN Network Manager for AIX application has attempted to establish communications with Topology Services, even though it has already successfully done so.

Action: No response is required.

---

351 **Connection with Topology was not established.**

Meaning: Topology Services tried to establish a connection with the cmld daemon, but was unsuccessful.

Action: After exiting the NetView for AIX graphical interface, stop LNM for AIX. Then execute ovstop followed by ovstart. Use ovstatus to verify the NetView for AIX daemons are running. Restart LNM for AIX.

---

386 **View not found when executing getPosition.**

Meaning: Topology Services cannot find the information it expects in its database.

Action: Go to the directory /usr/CML/databases. Verify that the files lnmTopoGraph.spec and lnmTopoVertex.spec are present and have not been changed since your last installation of LAN Network Manager for AIX. If they have been changed, reinstall LAN Network Manager. Otherwise, contact IBM Service for more information.

---

387 **Element not found when executing getPosition.**

Meaning: Topology Services cannot find information it expects in its database.

Action: Go to the directory /usr/CML/databases. Verify that the files lnmTopoGraph.spec and lnmTopoVertex.spec are present and have not been changed since your last installation of LAN Network Manager for AIX. If they have been changed, reinstall LAN Network Manager. Otherwise, contact IBM Service for more information.

---

388 **Port not found when executing getPosition.**

Meaning: Topology Services cannot find information it expects in its database.

Action: Go to the directory /usr/CML/databases. Verify that the files lnmTopoGraph.spec and lnmTopoVertex.spec are present and have not been changed since your last installation of LAN Network Manager for AIX. If they have been changed, reinstall LAN Network Manager. Otherwise, contact IBM Service for more information.

---

389 **Device not found when executing getPosition.**

Meaning: Topology Services cannot find information it expects in its database.

Action: Go to the directory /usr/CML/databases. Verify that the files lnmTopoGraph.spec and lnmTopoVertex.spec are present and have not been changed since your last installation of LAN Network Manager for AIX. If they have been changed, reinstall LAN Network Manager. Otherwise, contact IBM Service for more information.

---

393 **Root not found when executing timeoutReceived. Database is empty.**

Meaning: Topology Services was unable to retrieve its top-level view from the NetView for AIX Generic Topology Database.

Action: Shut down LAN Network Manager for AIX. Use SMIT to clear the database. (Maintain...Clear LNM for AIX databases). Restart LAN Network Manager for AIX.

If the problem persists, contact IBM Service for more information.

394 Trap send error when executing changeMemberPosition. graph Name = <name> Reason Code = <code>

Meaning: There was a problem with a message sent by Topology Services to NetView for AIX.

Action: Ensure the NetView for AIX daemons nvot_server or ovwdb are still running, using the `ovstatus` command. If they are not, restart them. If the problem persists, save the nettl log and contact IBM Service for more information.

395 Unknown message received by TopologyServer.

Meaning: An LAN Network Manager for AIX application sent Topology Services a request using a request identifier that is unsupported.

Action: None, although you may want to resynchronize any critical views since a message may have been corrupted and thus lost. If the problem persists, save the nettl log and contact IBM Service for more information.

396 Graph spec file was not opened.

Meaning: Topology Services cannot find information it expects in its database.

Action: Go to the directory /usr/CML/databases. Verify that the file lnmTopoGraph.spec is:

- Present
- Has the `read` permission turned on
- Has not been changed since your last installation of LAN Network Manager for AIX

Add the read permission if it is not there. If the file is missing or changed, reinstall LAN Network Manager.

397 Arc spec file was not opened.

Meaning: Topology Services cannot find information it expects in its database.

Action: Go to the directory /usr/CML/databases. Verify that the file lnmTopoArc.spec is:

- Present
- Has the `read` permission turned on
- Has not been changed since your last installation of LAN Network Manager for AIX

Add the read permission if it is not there. If the file is missing or changed, reinstall LAN Network Manager.

398 Vertex spec file was not opened.

Meaning: Topology Services cannot find information it expects in its database.

Action: Go to the directory /usr/CML/databases. Verify that the file lnmTopoVertex.spec is:

- Present
- Has the `read` permission turned on
- Has not been changed since your last installation of LAN Network Manager for AIX

Add the read permission if it is not there. If the file is missing or changed, reinstall LAN Network Manager.

399 getGraphType request received for a non-existent graph. graphName = <name>

Meaning: An LAN Network Manager application has asked Topology Services to act on a graph that is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

400 getVertexType request received for a non-existent vertex. vertexName = <name>

Meaning: An LAN Network Manager application has asked Topology Services to act on a graph that is not in the Topology Services cache. This means a resource has been discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

410 Error in initialization process (could not create root graph).

Meaning: There was a problem with a message sent by Topology Services to NetView for AIX.

Action: Ensure the NetView for AIX daemons nvot_server or ovwdb are still running, using the `ovstatus` command. If they are not, restart them. Stop any running LNM for AIX monitoring daemons. Restart LNM for AIX.

If the problem remains, stop any running LNM for AIX monitoring daemons. Use SMIT to clear the database. (Maintain...Clear LNM for AIX databases). Restart LNM for AIX. If the problem still persists, save the nettl log and contact IBM Service for more information.

---

418 **Topology config file not found, default values will be used.**

Meaning: The file that would contain any user-defined Topology Services customization was not found.

Action: None. This is an expected message, if no customization has been done of General Configuration Parameters using SMIT.

---

419 **Topology config file empty, default values will be used.**

Meaning: The file that would contain any user-defined Topology Services customization is empty.

Action: None. However, the General Configuration Parameters customization has been lost. Reenter it using SMIT.

---

424 **SNMP error -- OVsnmpErrno: <number>, nvSnmpErrno: <number>, nvSnmpSubsys: <subsystem>**

Meaning: Topology Services failed in an attempt to open a session with NetView for AIX to send a trap.

Action: Look at the man page for OVsnmpOpen. The error codes should help you determine the correct action to take. If they do not, then shut down and restart LAN Network Manager for AIX and NetView for AIX. If the problem persists, contact IBM Service for more information.

---

425 **Unable to close SNMP session -- OVsnmpErrno: <error number>**

Meaning: Topology Services failed in an attempt to close a trap session with NetView for AIX.

Action: Look at the man page for OVsnmpClose. The error number should help you determine the correct action to take. If it does not, then shut down and restart LAN Network Manager for AIX and NetView for AIX. If the problem persists, contact IBM Service for more information.

---

426 **Unable to create trap -- OVsnmpErrno: <error number>**

Meaning: Topology Services failed in an attempt to build a trap to send to NetView for AIX.

Action: Look at the man page for OVsnmpCreatePdu. The error number should help you determine the correct action to take. If it does not, then shut down and restart LAN Network Manager for AIX and NetView for AIX. If the problem persists, contact IBM Service for more information.

---

427 **Unable to send trap -- OVsnmpErrno: <error number>**

Meaning: Topology Services failed in an attempt to send a trap to NetView for AIX.

Action: Look at the man page for OVsnmpSend. The error number should help you determine the correct action to take. If it does not, then shut down and restart LAN Network Manager for AIX and NetView for AIX. If the problem persists, contact IBM Service for more information.

---

430 **Disassociate request received for a non-existent component. parent Protocol = <protocol> parent Name = <name> graph Protocol = <protocol> graph Name = <name>**

Meaning: Topology Services is trying to remove a resource from a graph, but the Topology Services cache has no record that the resource is in the graph.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

---

431 **Disassociate request received for a non-existent parent. parent Protocol = <protocol> parent Name = <name> graph Protocol = <protocol> graph Name = <name>**

Meaning: An LAN Network Manager for AIX application as asked Topology Services to remove a resource from a graph, but the Topology Services cache has no record of the graph. This means a resource has been

discovered that is not in any view.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

---

432 **Disassociate request received for a non-existent element. parent Protocol = <protocol> parent Name = <name> vertex Protocol = <protocol> vertex Name = <name>**

Meaning: An LAN Network Manager application has asked Topology Services change an element is not in the Topology Services cache. This means that an element has been discovered by the application but is not known to Topology Services.

Action: This problem should be resolved the next time the application resynchronizes a view that contains the resource. To resolve it more quickly, you can manually resynchronize the view if you know which one the resource should have been in.

---

435 **Cannot get ID for field <resource name> from OVw. OVw error is: <NV/6K error message>.**

Meaning: The Topology Services application was unable to get an object's resource ID from NetView/6000 database.

Action: Stop any LNM for AIX monitoring daemons. Exit the NetView for AIX graphical interface. Execute ovstop, then ovstart. Use ovstatus to verify that the NetView for AIX daemons are running. Restart LNM for AIX.

If the problem remains, stop any running LNM for AIX monitoring daemons. Use SMIT to clear the database. (Maintain...Clear LNM for AIX databases). Restart LNM for AIX. If the problem still persists, save the nettl log and contact IBM Service for more information.

---

436 **Cannot get value for field <field name> from OVw. OVw error is: <NetView/6000 error message>.**

Meaning: The Topology Services application was unable to get an object's field name from NetView/6000 database.

Action: Stop any LNM for AIX monitoring daemons. Exit the NetView for AIX graphical interface. Execute ovstop, then ovstart. Use ovstatus to verify that the NetView for AIX daemons are running. Restart LNM for AIX.

If the problem remains, stop any running LNM for AIX monitoring daemons. Use SMIT to clear the database. (Maintain...Clear LNM for AIX databases). Restart LNM for AIX. If the problem still persists, save the nettl log and contact IBM Service for more information.

---

446 **Topology clients failed to close socket at shutdown.**

Meaning: One or more LAN Network Manager application did not close the connection with topology at shut down.

Action: None.

---

448 **Topology index cache corrupted. file: <file name> line: <line number>**

Meaning: Internal topology database of LAN Network Manager has been corrupted.

Action: Clear the NetView for AIX databases using the NetView for AIX SMIT option (Maintain...Clear databases). Then stop LAN Network Manager using the clear option and restart.

---

452 **Cannot open Window Description File: < PDF filename >.**

Meaning:

The PDF file cannot be opened or does not exist.

Action: Verify that the .pdf files are installed in /usr/CML/databases directory and if the permissions are properly setup. If .pdf files are not installed, reinstall LAN Network Manager.

---

454 **OVw initialization error**

Meaning: During EUI Initialization, an OVw initialization error was returned.

Action: Verify that the AIX NetView/6000 graphical interface processes are running. Once all of these are running, retry accessing the management window. If the problem persists, contact IBM Service for more information.

455 **Error while registering action callback.**

Meaning: During EUI Initialization, an error occurred while registering the OVw action callbacks. The probable cause is that OVw actions which are being registered do not match the ones described in registration file.

Action: Verify that the AIX NetView/6000 graphical interface processes are running. Once all of these are running, retry accessing the management window. If the problem persists, contact IBM Service for more information.

456 **Error while registering termination callback.**

Meaning: During EUI Initialization, an error occurred while registering the OVw termination callback.

Action: Verify that the AIX NetView/6000 graphical interface processes are running. Once all of these are running, retry accessing the management window. If the problem persists, contact IBM Service for more information.

469 **OVW not running.**

Meaning: EUI was initialized before starting OVw.

Action:

Start the AIX NetView/6000 graphical interface.

501 **Error <errorCode> from agent in <routine>, RN=<resourceName>**

Meaning: An SNMP response was received in the specified routine with an unexpected SNMP error code while building the object with the given resource name.

Action: The following table describes the possible error codes and responses to them:

1 (tooBig)	This message should never occur. If it does, contact IBM service.
2 (noSuchName)	Ensure that the FDDI Proxy Agent software is running.
3 (badValue)	The value entered for a set is not valid. Enter a new value.
4 (readOnly)	A set was attempted to a read-only variable. Due to the nature of the SMT 6.2 and 7.3 MIBs, sometimes a variable is read-write in a window when it is read-only in the MIB.
5 (genErr)	Verify that the FDDI Proxy Agent software is running. If the software is running, then the device which is currently being interrogated may not support SMT properly.

502 **Segment resynchronized due to timeout in <routine>, RN=<resourceName>**

Meaning: An SNMP response was not received in the specified routine within the time specified in the NetView for AIX SNMP configuration while building the object with the given resource name. This could be caused by a network connection problem, or a device problem.

Action: If this message persists, physically verify that the device in question is functional. If so, extend the timeout value in the NetView for AIX SNMP Configuration window.

503 **Segment resynchronized due to trap <trapName> in <routine>**

Meaning: The following FDDI traps can cause a segment to be resynchronized:

- macDuplicateAddressResolved
- configUNAChange, if configurationReporting was previously determined to be off
- fddiProxyAgentReady

Also, the following generic traps will cause a resync:

- coldStart
- warmStart
- linkUp

This message indicates that the specified trap was received in the given routine.

Action: None.

504 **SNMP retry count exceeded in <routine>, RN=<resourceName>**

Meaning: This message is generated when more than 10 timeouts are received while attempting to issue SNMP requests against an FDDI object with the given resource name in the specified routine.

Action: If this message persists, physically verify that the device in question is functional. If so, increase the timeout value in the NetView for AIX SNMP Configuration window.

505 Error <errorNumber> from topology in <routine>, RN=<resourceName>

Meaning: Error errorNumber occurred while communicating with lnmtopod in routine while building an object with the given resource name.

Action: Issue the cmlstatus command to verify that lnmtopod is running. If it is not, check the nettl log to determine the cause of the error. Then reissue cmlstart to restart the application.

507 Memory allocation failed in <routine> getting <dataType>

Meaning: A memory allocation error has occurred in routine while trying to allocate memory for the given data type. This usually indicates a shortage of hardware resources.

Action: In the short term, shut down some other applications, then restart LAN Network Manager. In the long term, obtain more memory.

508 The Socket to <application> failed in <routine> with rc = <returnCode>

Meaning: A socket failure has occurred in the specified routine while communicating with one of the applications listed below.

Action:

Application	Action
CP	Consult the nettl log for messages associated with the failure of cmld and lnmtopod daemons. Then restart LAN Network Manager.
Topology	Verify that lnmtopod is running (see message number 505)
SNMP Trap	Verify that NetView for AIX is running properly. Then restart LAN Network Manager.
lnmfddimgr	Restart lnmfddimgr by selecting a FDDI object and requesting a window.

509 Unexpected Case in <routine>. Case number = <value>, RN = <resourceName>

Meaning: While building the object specified by resource name, in the specified routine, an unexpected value was encountered.

This can occur in an <object>::processingResponse method. In these cases, this indicates a device that may not support SMT properly.

In any other situation, this probably represents a programming error.

Action: If this falls under the `programming error` category, contact IBM service.

512 No <object> Found in <routine>, RN = <resourceName>, type = <type>

Meaning: This message indicates failure to find an object.

Action: None. If the problem persists, contact IBM service.

515 Frame error unknown in <routine>, value = <frameErrorFlagValue>, RN = <resourceName>

Meaning: The macFrameErrorFlag value received in routine while building object resourceName is unexpected. This could indicate the following condition:

- The device in question does not properly support the macFrameError attribute

Action: None.

516 Validity flag false for <variable> in <routine>, RN = <resourceName>

Meaning: While processing the specified variable for object resourceName, a validity flag with value false was received.

Action: None.

517 Configuration file missing. IPAddress = <ipAddress>

Meaning: There is no configuration file for the agent with this IP address.

Action: If desired, create a configuration file using SMIT CML.

518 **Panel requested resynch. IPAddress = <ipAddress>**

Meaning: A resynchronize request was received from lnmfddimgr for the agent with the specified IP address.

Action: None.

519 **Trap Correlation failed. rc = <returnCode>, OVsnmpErrno = <errorNumber>, Error String = <errorString>, Specific = <specificTrapNumber>, Generic = <genericTrapNumber>**

Meaning: An error occurred while trying to send a correlation trap to NetView for AIX.

Action: Issue ovstart to ensure that all NetView for AIX processes are running.

520 **Unexpected Trap in <routine>. Generic number = <genericTrapNumber>, specific Number = <specificTrapNumber>, RN = <resourceName>**

Meaning: A generic trap other than warmStart, coldStart, or linkUp was received from an FDDI Proxy Agent station.

Action: None.

521 **The Control program has terminated. The FDDI application will terminate. <routine>**

Meaning: The cmld daemon is required for LAN Network Manager to run.

Action: Restart LAN Network Manager using the cmlstart command.

522 **The Management Application has terminated. <routine>**

Meaning: lnmfddimgr has terminated.

Action: Restart it by selecting a FDDI object and requesting a window.

523 **Agent in Agent Found already exists: <ipAddress>**

Meaning: A duplicate agent found message was received.

Action: None.

524 **FDDI discovery application terminated**

Meaning: lnmfddimon terminated.

Action: Restart with cmlstart. If problem persists, contact IBM Service for more information.

527 **Agent in Agent Delete does not exist: <ipAddress>**

Meaning: The agent to be deleted cannot be found.

Action: None.

551 **<objectType> action FAILED due to <snmpFailureReasonText>.**

Meaning: An SNMP action for objectType failed for the reason given in the SNMP error text.

Action: The following table describes the possible error codes and responses to them:

1 (tooBig)
This message should never occur. If it does, contact IBM service.

2 (noSuchName)
Ensure that the FDDI Proxy Agent software is running.

3 (badValue)
The value entered for a set is not valid. Enter a new value.

4 (readOnly)
A set was attempted to a read-only variable. Due to the nature of the SMT 6.2 and 7.3 MIBs, sometimes a variable is read-write in a window when it is read-only in the MIB.

5 (genErr)
Verify that the FDDI Proxy Agent software is running. If the software is running, then the device which is currently being interrogated may not support SMT properly.

552 **<objectType> action completed successfully.**

Meaning: Command completed successfully.

Action: None.

553 Add Window failed. rc = <returnCode> in <routine>.

Meaning: An error occurred while creating a new window.

Action: This is an out-of-resources error. Close one or more windows and retry the operation.

556 Error accessing config file.

Meaning: An error occurred trying to access the config file.

Action: This probably indicates that NetView for AIX was started without root privileges. Restart NetView for AIX with root privileges.

557 Unexpected Case in <routine>. Case number = <receivedValue>, Instance = <panelID>.

Meaning: While building the window specified by the instance, in the specified routine, an unexpected value was encountered.

Action: This can indicate one of two things:

- An unexpected response was received from an SMT device. This case often implies that an SMT attribute is not supported by the device in question.
- A programming error. If the method is not of the form <object>::processingResponse(), this is probably a programming error. Contact IBM service.

558 lnmfddimon is not running.

Meaning: The LAN Network Manager FDDI discovery application is not running.

Action: Restart LAN Network Manager.

559 lnmfddimon socket is inactive.

Meaning: The socket used for communication between the FDDI discovery and management applications is not active, probably because lnmfddimon has not been started.

Action: Restart LAN Network Manager.

560 lnmfddimon socket has failed.

Meaning: The socket used for communication between the FDDI discovery and management applications has become inactive, probably because lnmfddimon has stopped.

Action: Restart LAN Network Manager.

561 Error <returnCode> from euiInit in <routine>.

Meaning: An error occurred while initializing the EUI library.

Action: Retry the operation. Consult the nettl log for a message corresponding to the return code. If the error persists, contact IBM service.

562 Set attribute failed in <routine> with rc = <returnCode>.

Meaning: An error occurred trying to directly set a window attribute, outside the normal get/set operation scope.

Action: Consult the nettl log for a message corresponding to the return code. If the error persists, contact IBM service.

563 Agent indices reassigned - panels may no longer correspond to expected objects. It is suggested that all open windows be closed and reopened.

Meaning: Due to an `index reassigned` trap from the FDDI agent, the indices of the SMT objects have been reassigned. Consequently, the currently open windows may no longer correspond to the objects they were opened against.

Action: Close and reopen all currently open windows.

564 Invalid panel. id = <panelID> in <routine>.

Meaning: A callback was received from OVw for which there is no corresponding window. This could indicate that the registration file has been altered.

Action: Reinstall LAN Network Manager. If the problem persists, contact IBM service.

565 Memory allocation failed in <routine>.

Meaning: A fault occurred when the application tried to allocate memory.

Action: Free resources by terminating unneeded

applications. Alternatively, install more memory in the affected workstation.

569 **Resynchronize performed - panels may no longer correspond to expected objects. It is suggested that all open windows be closed and reopened.**

Meaning: Due to resynchronize (due either to a request or timer pop), the indices of the SMT objects have been reassigned. Consequently, the currently open windows may no longer correspond to the objects they were opened against.

Action: Close and reopen all currently open windows.

570 **Resynchronize request has been sent to lnmfddimon.**

Meaning: The resynchronize request has been transmitted to lnmfddimon.

Action: None.

573 **The Socket to <applicationName> failed in <routine> with rc = <returnCode>.**

Meaning: The socket used for communication between the FDDI discovery and management applications has become inactive, probably because lnmfddimon has stopped.

Action: Restart lnmfddimon using the cmlstart command.

574 **Stopping lnmfddimgr.**

Meaning: lnmfddimgr is stopping due to stoppage of OVw.

Action: None.

Messages 601 to 2000

601 **Unexpected value <value> in switch statement in procedure <procedure name> Buffer contents = <buffer contents>**

Meaning: The data does not conform to the expected set.

Action: In general this indicates a programming error. If it does not reoccur it can be due to a failure in the transmission of data on the socket. If it reoccurs, contact IBM Service for more information.

602 **NAUN change processing failed on segment <segment number> for station <adapter address> NAUN <adapter address>.**

Meaning: One or more NAUN change traps have been lost. The current trap does not fit the expected pattern for stations going offline or coming online.

Action: If this occurs for only one segment, manually resynchronize the segment. If it occurs for multiple segments for the same LNM OS/2 Agent, manually resynchronize the agent. This may occur in conjunction with message 613 for the OVsnmp Receiving session.

You may reduce the number of times this occurs by increasing the size of the receiving buffer for the TCP/UDP socket for trapd.

603 **Authentication failure for <IP address>.**

Meaning: An SNMP generic trap 4 was received.

Action: Verify that

- The community names match.
- The SNMP password file exists on the OS/2 workstation.

604 **Socket connection not yet established from <name of executable> to <name of executable>.**

Meaning: The LNM OS/2 Agent discovery application (lnmlnmemon) must be able to communicate with each of the following executables: lnmtopod, cmld, lnmBaseTimer, lnmlnmeint. If it cannot establish communications, it will continue to attempt to do so, writing this message to the log every two minutes. There may be additional messages which indicate why the socket connections cannot be established.

Action: The speed of the RISC and its workload may cause this situation to occur and be resolved without any action. If the log is being flooded with these messages, stop LNM for AIX. Use the nettl log and cmlstatus to determine why determine why one or more of the executables is not running. If possible correct the problem and restart LNM for AIX. Otherwise contact IBM

Service for more information.

605 View Built for resource <resource identifier>

Meaning: This message indicates that the LNM OS/2 Agent discovery application has completed discovery of the resource named in the message. The resource identifier will either be for an agent or a segment. This does not imply that all resources attached to the resource identified were successfully discovered. Only that the LNM OS/2 Agent discovery application is not attempting to determine the resource configuration at this time.

Action: None.

606 Duplicate start message received

Meaning: The LNM OS/2 Agent discovery application initially comes up and waits for the control program to tell it to run. This is done with a start message. If this occurs more than once, the additional requests are discarded but noted in the log.

Action: None.

607 Request for unknown resource <resource identifier>.

Meaning: The LNM OS/2 Agent discovery application expects to be able to match the resource requested to a resource known in its internal data storage.

Action: This message occurs if an attempt is made to remove an agent that is not currently known to the LNM OS/2 Agent discovery application. In this case, verify that the parameters entered with cml_agent_remove are correct. If they are correct, verify that the agent has been discovered during the current LNM for AIX session. It is not possible to remove the agent representation from the display using this command unless the agent was discovered during this session. If the intent is to remove the agent from the display, execute an cml_agent_found followed by cml_agent_remove.

This message also occurs if the LNM OS/2 Agent management application requests information about a resource not currently known to the LNM OS/2 Agent discovery application. This may occur if the request occurs during a resynchronize or if the request occurs and the agent was not discovered during this session. If the agent has not been discovered, execute an cml_agent_found and retry the request. If the resource is being resynchronized, retry the operation later.

609 Invalid data received for <a character string>.

Meaning: The LNM OS/2 Agent discovery application expected a character string which contained valid hex digits.

Action: Verify that data being returned in run command responses is valid. Adapter addresses, segment numbers and concentrator ids are expected to be valid hex digits. If they are not, restart the LNM OS/2 Agent. If the problem persists, contact IBM Service for more information.

610 Return code <value> for <run command key words> run command

Meaning: With the exception of messages 804, 805, 808, 809, 810 and 833, prefix the value with DFI for the corresponding LNM OS/2 Agent message number. The run command key words tell which run command returned the DFI value. For the set enumerated above:

- 804 - The interface component was unable to assemble the run command.
- 805 - LNM OS/2 Agent was not able to successfully complete the request to enable traps.
- 808 - The interface component did not recognize the run command requested.
- 809 - The run command has timed out.
- 810 - The run command response cannot be parsed by the interface component.
- 833 - The LNM OS/2 Agent is busy gathering its view of the network.

Action: The impact of the message is determined by the run command which generated the response and the value returned. For example, 488 indicates no adapters match the defined view. This is an acceptable response for a request for an adapter list for an unlinked segment which is connected by an unlinked bridge. In general, though this message will mean there is a loss of data and the representation of the network from LNM for AIX will be at best incomplete and possibly inaccurate. The explanation for the DFI messages is documented by the LNM OS/2 Agent. The following list addresses those return code values which do not correspond to a DFI message from LNM OS/2 Agent.

- 804 - The interface component was unable to assemble the run command. In general this indicates a programming error. If it does not reoccur it can be due to a failure in the transmission of data on the socket. If it persists, contact IBM Service for more information.

- 805 - LNM OS/2 Agent was not able to successfully complete the request to enable traps. If traps do not flow from the agent to LNM for AIX it will be necessary to resynchronize the LNM for AIX view of the agent more frequently. Each time a resynchronize is initiated, an attempt will be made to enable traps from the LNM OS/2 Agent. Verify the following:
  - You can ping from the OS/2 workstation to the RISC workstation and from the RISC workstation to the OS/2 workstation.
  - The community name in CONFIG.SYS matches the community name for the agent known to NetView for AIX.
  - There is an SNMP PW file on the OS/2 workstation.
  - SNMPTRAP.DST contains the IP address of LNM for AIX.
  - SNMPD is running on the OS/2 workstation.
  - There are no messages from the LNM OS/2 Agent on start up that indicate it cannot get the trap thread going.
  - The name in the HOST file in the TCP/IP directory on the OS/2 workstation matches the host name in CONFIG.SYS.
- 808 - The interface component did not recognize the run command requested. In general this indicates a programming error. If it does not reoccur, it can be due to a failure in the transmission of data on the socket. It is persists, contact IBM Service for more information.
- 809 - The run command has timed out. No response was received from the LNM OS/2 Agent. A run command response is expected to be received from the LNM OS/2 agent within a designated time period. This time period is the sum of the LNM for AIX response time (transmission time, network congestion, etc) and the LNM OS/2 Agent response time multiplied by the number of requests that are currently on the LNM OS/2 Agent queue from LNM for AIX. The response time components can be set from SMIT or from the LNM OS/2 Agent Configuration windows. Initially the response time out values may need to be adjusted to reflect the realities of the network. Once a successful set of values have been selected, the occurrence of a time-out may indicate increased network traffic or that the agent is now located more hops away from LNM for AIX and the LNM for AIX response time needs to increase or it may indicate that the agent is unable to communicate with LNM for AIX but the socket connections have not gone down. DCAF or TELNET can be used to determine the state of the agent workstation if it is located remotely.
- 810 - The run command response cannot be parsed by the interface component. This indicates either that the run command response does not match the expected pattern because the agent malfunctioned, the transmission of the data introduced an error or there is a programming error. To verify that the agent is functioning correctly, attempt to execute the same run command from an OS/2 window. If the agent responds correctly, and it does not reoccur it can be due to a failure in the transmission of data on the socket. Otherwise it is a programming error, contact IBM Service for more information.
- 833 - The LNM OS/2 Agent is busy gathering its view of the network. To allow this to complete as quickly as possible, the LNM OS/2 Agent discovery application will not request any more information for 5 minutes. The LNM OS/2 Agent discovery application attempts to complete the request every five minutes until it is successful. Successful means that the LNM OS/2 Agent has completed establishing its view of the network. The length of delay is dependent on the size of the network the LNM OS/2 Agent is handling, the hardware the agent is running on and what is running on that hardware.

---

611 **Duplicate adapter <adapter address> on segment <segment number>.**

Meaning: An adapter address has been found more than once on the same segment. The additional occurrences of the adapter will not display. Any adapter specific traps will be correlated and applied to the first occurrence.

Action: If multiple Bridge link successful messages (OS/2 agent trap 458) come in at the same time for the same segment, ignore the warning. Otherwise, investigate the adapters on the segment to see if a duplicate exists. If so, change the locally administered address to make it unique.

---

612 **Unexpected value <value> in switch statement in procedure <procedure name>**

Meaning: The data does not conform to the expected set.

Action: In general this indicates a programming error. If it does not reoccur it can be due to a failure in the transmission of data on the socket. If it reoccurs, contact IBM Service for more information.

613 **Socket connection from <executable name> to <executable name/trap session> failed**

Meaning: The communications from the LNM OS/2 Agent discovery application to/from one of the other LNM for AIX components (cmld, lnmtopod, lnmlnmeint, lnmBaseTimer, lnmlnmemgr) or with NetView for AIX trap processing have been disrupted. There will be a loss of data.

Action: If communications failed with the OVsnmp Trap Receiving Session, traps coming from the LNM OS/2 Agents to LNM for AIX have probably been lost. It may be necessary to manually resynchronize the agents or one or more segments, to display an accurate representation of the network.

If communications failed with the OVsnmp Trap Sending Session, traps with the correlation data have probably been lost and will not reflect in the trapd log or, if applicable, the event cards. No action is required.

If communication fails with the Control program (cmld), the LNM OS/2 Agent components (lnmlnmemon, lnmlnmeint, lnmBaseTimer, and lnmlnmemgr) will terminate. Check the nettl log to see why communications failed. Correct the error indicated by the interprocess communication messages if possible. Try to restart the components using the command cmlstart. If this is unsuccessful, stop LNM for AIX and then restart LNM for AIX.

If communications fail with lnmtopod, the LNM OS/2 Agent discovery application components will terminate. Check the nettl log to see why communications failed. Correct the error indicated by the interprocess communication messages if possible. Try to restart the components using the command cmlstart. If this is unsuccessful, stop LNM for AIX and then restart LNM for AIX.

If communications fail with lnmlnmeint, there will be a disruption in the management but an attempt is made to recover. If it is possible to restart the interface component, the LNM OS/2 Agent discovery application will check the status of each known agent. If an agent was in the middle of a discovery cycle, the discovery process will be restarted. If an agent was in an idle state, connection will be reestablished.

If communications fails with lnmBaseTimer, an attempt is made to recover. Timed events are resubmitted but times are not recalculated. This will impact the accuracy of history collection times and scheduled resyncs.

If communication fails with the lnmlnmemgr, an attempt is made to recover. If lnmlnmemgr is not running, attempting to access an OS/2 agent management window will restart it.

615 **Duplicate resynchronize request for LNM OS/2 Agent <IP address> segment <segment number>**

Meaning: If a particular segment is being resynchronized and an additional request is received to resynchronize it, this message is written to the log and the request is discarded.

Action: None.

616 **Request for duplicate resource <IP address>**

Meaning: A request to discover a known agent has been received. It is discarded.

Action: None.

619 **Invalid ring interval found in file = <IP address.conf>**

Meaning: The ring utilization interval must be from 60 seconds to 86360 seconds (23 hours 59 minutes).

Action: Use the Segment Parameters window to correct the error.

620 **Invalid segment start/stop date found in file = <IP address.conf>**

Meaning: The start and stop date must be from 0 to 6 (Sunday through Saturday).

Action: Use the Segment Parameters window to correct the date in error.

621 **Invalid segment start/stop time found in file = <IP address.conf>**

Meaning: The start and stop time must be from 0 to 1439 minutes (0 hours and minutes to 23 hours and 59 minutes).

Action: Use the Segment Parameters window to correct the time in error.

622 **Invalid bridge start/stop date found in file = <IP address.conf>**

Meaning: The start and stop date must be from 0 to 6 (Sunday through Saturday).

Action: Use the Bridge Parameters window to correct the date in error.

---

623 **Invalid bridge start/stop time found in file = <IP address.conf>**

Meaning: The start and stop time must be from 0 to 1439 minutes (0 hours and minutes to 23 hours and 59 minutes).

Action: Use the Bridge Parameters window to correct the time in error.

---

628 **Could not set segment interval in file = <IP address.conf>**

Meaning: The attempt to retrieve the required record from the agent configuration file failed.

Action: Possible reasons for the failure are:

- The agent configuration file <IP address.conf> does not exist in the /usr/CML/conf/lnmlnmemon directory. Create the file using SMIT.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is locked. Exit the process locking the file.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is corrupted. The required record is missing. Delete the file and recreate it using SMIT. If you delete the file and were collecting history on any segments or bridges, you will need to re-enable collection on those segments and bridges and reset the collection window.

---

629 **Could not get segment interval in file = <IP address.conf>**

Meaning: The attempt to retrieve the required record from the agent configuration file failed.

Action: Possible reasons for the failure are:

- The agent configuration file <IP address.conf> does not exist in the /usr/CML/conf/lnmlnmemon directory. Create the file using SMIT.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is locked. Exit the process locking the file.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is corrupted. The required record is missing. Delete the file and recreate it using SMIT. If you delete the file and were collecting history on any segments or bridges, you will need to re-enable collection on those segments and bridges and reset the collection window.

---

630 **Could not set bridge interval in file = <IP address.conf>**

Meaning: The attempt to retrieve the required record from the agent configuration file failed.

Action: Possible reasons for the failure are:

- The agent configuration file <IP address.conf> does not exist in the /usr/CML/conf/lnmlnmemon directory. Create the file using SMIT.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is locked. Exit the process locking the file.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is corrupted. The required record is missing. Delete the file and recreate it using SMIT. If you delete the file and were collecting history on any segments or bridges, you will need to re-enable collection on those segments and bridges and reset the collection window.

---

631 **Could not get bridge interval in file = <IP address.conf>**

Meaning: The attempt to retrieve the required record from the agent configuration file failed.

Action: Possible reasons for the failure are:

- The agent configuration file <IP address.conf> does not exist in the /usr/CML/conf/lnmlnmemon directory. Create the file using SMIT.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is locked. Exit the process locking the file.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is corrupted. The required record is missing. Delete the file and recreate it using SMIT. If you delete the file and were collecting history on any segments or bridges, you will need to re-enable collection on those segments and bridges and reset the collection window.

---

632 **Could not get bridge graph lines in file = <IP address.conf>**

Meaning: The attempt to retrieve the required record from the agent configuration file failed. This information is used by the LNM OS/2 Agent management application to populate Bridge Performance Window with the last known choices.

Action: Possible reasons for the failure are:

- The agent configuration file <IP address.conf> does not exist in the /usr/CML/conf/lnmlnmemon directory. Create the file using SMIT.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is locked. Exit the process locking the file.
- The agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is corrupted. The required record is missing. Delete the file and recreate it using SMIT. If you delete the file and were collecting history on any segments or bridges, you will need to re-enable collection on those segments and bridges and reset the collection window.

---

633 **Cannot open history file = <history file name> with access = a+ Error <value>: <error description>**

Meaning: The file cannot be opened in append mode. This mode opens a file for writing at the end of the file, or creates a file for writing.

Action: Correct the error so that future collection will be successful. There will be a loss of data.

---

635 **lnmlnmemon exiting. Exit code <exit status>**

Meaning: lnmlnmemon is terminating for one of the following reasons:

- 0 - Normal termination
- 1 - Memory fault
- 2 - Socket connection error
- 3 - Socket information lost
- 6 - Program error
- 17 - Terminated after receiving SIGTERM signal
- 18 - Terminated from main
- 22 - Terminated after receiving SIGDANGER signal

Action: This message can be used in conjunction with the response from cmlstatus to understand why lnmlnmemon is no longer running. See the man page for cmlstatus for an explanation of the exit codes. If this message is not written to the log, lnmlnmemon was terminated using SIGKILL or terminated abnormally. If lnmlnmemon terminated abnormally, a core dump will probably be found in the root directory. You can determine the executable that generated a core dump by entering the following command while you are in the directory with the core image

```
od -c core 0x4850 | head
```

Record the information from executing dbx with the *where* subcommand or the *t* subcommand. Contact IBM Service for more information.

---

636 **Refresh of LNM OS/2 Agent <IP address> is in progress**

Meaning: If a particular agent is being refreshed and an additional request is received to refresh it, this message is written to the log and the request is discarded.

Action: None.

---

637 **LNM OS/2 Agent <IP address> is initializing or resyncing. Discovery of the agent topology will be retried in <n> minutes.**

Meaning: The LNM OS/2 Agent is busy gathering its view of the network. To allow this to complete as quickly as possible, the LNM OS/2 Agent discovery application will not request any more information for *n* minutes. The LNM OS/2 Agent discovery application will attempt to restart the discovery process for the agent, every *n* minutes until it is successful. Successful means that the LNM OS/2 Agent has completed establishing its view of the network. The length of delay is dependent on the size of the network the LNM OS/2 Agent is handling, the hardware the agent is running on and what is running on that hardware.

Action: None.

---

638 **Limits for loading the initial configuration for the LNM OS/2 agent <IP address> have been exceeded. There may be data loss.**

Meaning: The load of local configuration information is limited to 250 bridge definitions and 260 adapter definitions. In addition there can be no more than 250 bridge definitions or 255 segments currently known to the LNM OS/2 Agent. If the limits are exceeded a partial load will be carried out.

Action: Use the end user interface to complete the configuration process.

---

639 **The resource <resource name> is not within the LNM OS/2 Agent managed domain.**

Meaning: LNM for AIX received a trap 751 (new CAU) from an LNM OS/2 Agent. The segment in the trap is not

within the LNM OS/2 Agent domain. Therefore the segment and CAU will not be added to the graphical display.

Action: If the intent is to manage the segment, add a CAU qualifier for the segment or link a bridge which handles the segment. Otherwise no action is required.

---

641 **Cannot process response for LNM OS/2 Agent <IP address> adapter <adapter address>. Procedure = <procedure name> File = <file name>, Line = <line number>**

Meaning: The initial configuration processing has received a run command response for which it does not have a matching request.

Action: This is not expected to occur. It is unlikely that the configuration and discovery of the LNM OS/2 Agent will complete successfully. If this messages occurs, remove the LNM OS/2 Agent and retry the operation. If it does not reoccur it could be caused by corruption of the transmitted data. If it reoccurs, contact IBM Service for more information.

---

642 **Bridge <bridge name> is a multiport bridge. Procedure = <procedure name> File = <file name>, Line = <line number>**

Meaning: If an icon has been created for a bridge that the LNM OS/2 agent classifies as a multiport bridge when it responds to LAN BRG QUERY NAME=<bridge name> ATTR=RPT, the bridge is no longer manageable from the LNM OS/2 component of LNM for AIX. The icon is deleted from the LAN submap.

Action: None.

---

643 **Unexpected segment type <segment type> Procedure = <procedure name> File = <file name>, Line = <line number>**

Meaning: There is an inconsistency in the expected data and the data received.

Action: If the problem persists, collect trace files for the processes *lnmlnmemon* and *lnmlnmeint*. Contact IBM Service for more information.

---

644 **Received AGENT_FOUND message from <process>, IP=<IP address>.**

Meaning: This message is written to the log if the agent is included in the set of agents managed by the LNM OS/2 component.

Action: None.

---

645 **Received AGENT_REMOVE message from <process>, IP=<IP address>.**

Meaning: This message is written to the log if the agent is removed from the set of agents managed by the LNM OS/2 component.

Action: None.

---

702 **Starting lnmlnmemgr.**

Meaning: This message is written to the log when lnmlnmemgr is invoked.

Action: None.

---

703 **Stopping lnmlnmemgr.**

Meaning: This message is written to the log when lnmlnmemgr terminates normally.

Action: None.

---

706 **No history data exists for segment <segment number>.**

Meaning: There are no files in /usr/CML/reports/lnmlnmemon/<IP address> for the segment requested. The current file is seg<segment number>.history.01 and the file for the previous period is seg<segment number>.history.02.

Action: If data was expected for the current period, verify that history collection is enabled for the segment and that the current period's interval spans the time during which the request was made. Check the log to ensure that ring utilization data is available for this segment. No file is created until there is data to put in it. There will not be a ...history.02 file until the collection window expires for the first time and a ...history.01 had been created.

---

707 **No history data exists for bridge <bridge name>.**

Meaning: There are no files in /usr/CML/reports/lnmlnmemon/<IP address> for the

bridge requested. The current file is brg<bridge name>.history.01 and the file for the previous period is brg<bridge name>.history.02.

Action: If data was expected for the current period, verify that history collection is enabled for the bridge and that the current period's interval spans the time during which the request was made. Check the bridge performance window to ensure the performance notification interval is greater than 0. Check the trapd.log to ensure that trap 801 is being received from the bridge. No file is created until there is data to put in it. There will not be a ...history.02 file until the collection window expires for the first time and a ...history.01 had been created.

---

709 A graph for segment <segment number> already exists.

Meaning: A graph window is currently open for this segment.

Action: Close the open graph window for this segment and retry.

---

710 A graph for bridge <bridge name> already exists.

Meaning: A graph window is currently open for this bridge.

Action: Close the open graph window for this bridge and retry.

---

712 Selecting OK would enable the Module.

Meaning: The selected action will generate a run command request for the LNM OS/2 Agent to have the module enabled.

Action: Select OK or Cancel.

---

713 Selecting OK would disable the Module.

Meaning: The selected action will generate a run command request for the LNM OS/2 Agent to have the module disabled.

Action: Select OK or Cancel.

---

714 Selecting OK would enable the lobe.

Meaning: The selected action will generate a run command request for the LNM OS/2 Agent to have the lobe enabled.

Action: Select OK or Cancel.

---

715 Selecting OK would disable the lobe.

Meaning: The selected action will generate a run command request for the LNM OS/2 Agent to have the lobe disabled.

Action: Select OK or Cancel.

---

716 <executable> terminated.

Meaning: The named executable has terminated.

Action: If you have selected to stop LNM for AIX, this is only information. However, if you have not, this indicates that the executable in question has dropped the socket connection with lnmlnmemgr. Check the nettl log and execute cmlstatus for additional information on why the executable terminated. If lnmlnmeint terminates and lnmlnmemon does not, lnmlnmemon will attempt to restart lnmlnmeint.

---

717 Communication Error - Socket cannot be opened.

Meaning: Socket communications could not be established with lnmlnmemon or lnmlnmeint.

Action: Check the nettl log to determine why the attempt to establish communications failed.

---

719 You are about to remove the adapter from the network.

Meaning: Once removed, the adapter will no longer be able to communicate with the network in any way. Manual intervention at the workstation will probably be required to restore the adapter's ability to communicate with the network. Note that the removal of an adapter may adversely effect the operation of a ring.

Action: To proceed, select OK. To cancel the request, select Cancel.

---

721 Request could not be deleted from the list.

Meaning: An attempt to delete an entry from the list of outstanding requests failed.

Action: None.

---

725 **Receive system call failed.**

Meaning: The read call on the socket failed.

Action: Check the nettl log to determine why the call failed.

---

726 **Syntax Error reported by the LNM OS/2 Agent.**

Meaning: The run command contained a syntax error.

Action: In general this indicates a programming error. Retry the operation. If it does not reoccur, it can be due to a failure in the transmission of data on the socket. If it reoccurs, contact IBM Service for more information.

---

727 **Missing Station definition parameters. Adapter Address and Adapter Name are required to define a station.**

Meaning: The adapter name and address are required for a station definition.

Action: Enter the missing information and retry the operation.

---

728 **Missing Bridge definition parameters. Bridge Name, Adapter1 Address and Adapter2 Address are required to define a bridge.**

Meaning: The bridge name and two adapter addresses are required for a bridge definition.

Action: Enter the missing information and retry the operation.

---

729 **Missing Concentrator definition parameter. Concentrator ID is required to define a Concentrator.**

Meaning: The concentrator name is required for a Concentrator definition.

Action: Enter the missing information and retry the operation.

---

730 **Missing Concentrator Qualifier definition parameter. Segment Number is required to define a Concentrator Qualifier.**

Meaning: A segment number is required for a Concentrator Qualifier definition.

Action: Enter the missing information and retry the operation.

---

731 **You are about to delete the definition of the bridge. Select OK to delete the definition, Cancel to Abort.**

Meaning: The action you have selected will request the LNM OS/2 Agent to delete the bridge definition from its database.

Action: Select Enter or Cancel.

---

732 **You are about to delete the definition of the Concentrator. Select OK to delete the definition, Cancel to Abort.**

Meaning: The action you have selected will request the LNM OS/2 Agent to delete the concentrator definition from its database.

Action: Select Enter or Cancel.

---

733 **Missing Mapped Address parameters. Token Ring and Ethernet Addresses are required to add a mapped entry.**

Meaning: The Token Ring and Ethernet adapter addresses are required to add a mapped entry.

Action: Enter the missing information and retry the operation.

---

734 **You are about to restart the Concentrator. Select OK to restart, Cancel to Abort**

Meaning: The action you have selected will request the LNM OS/2 Agent to restart the concentrator.

Action: Select OK or Cancel.

---

735 **Communication Error - NO Data.**

Meaning: An error occurred when lnmlnmemgr tried to send a request to initially populate a window to either lnmlnmeint or lnmlnmemgr.

Action: Verify that lnmlnmeint and lnmlnmemon are running. Retry the operation.

736 Communication Error - OLD Data.

Meaning: An error occurred when lnmlnmemgr tried to send a request to refresh a window to either lnmlnmeint or lnmlnmemgr.

Action: Verify that lnmlnmeint and lnmlnmemon are running. Retry the operation.

737 Error while waiting for responses.

Meaning: One or more of the fields on the window cannot be populated for the following reasons:

- The LNM OS/2 Agent cannot execute the LAN program.
- The connection with the LNM OS/2 Agent is down.
- The connection with the LNM OS/2 Agent has not been established.
- The response from the LNM OS/2 Agent is not formatted as expected.
- The run command is not one of those expected by the interface component.

Action: Check the nettl log to determine the cause of the problem.

- If the LNM OS/2 Agent cannot execute the LAN program, restart the LNM OS/2 Agent. If this symptom persists, contact IBM Service for more information.
- If the connection with the LNM OS/2 Agent is down, see if restarting the LNM OS/2 Agent will bring it up.
- If the connection with the LNM OS/2 Agent has not been established, discover the agent using the SMIT windows or the command line script cml_agent_found.
- If an unexpected command or unexpected response format occurs, retry the operation. If it does not reoccur the error could be due to a failure in the transmission of data on the socket. If it reoccurs, contact IBM Service for more information.

738 Missing Remote Program Update definition parameter. File name is required to update the Remote Program.

Meaning: The file name is required for Remote program update.

Action: Enter the missing information and retry the operation.

739 The NLS catalog file <filename> was not found.

Meaning: The named catalog file was not found.

Action: Verify there were no errors during installation.

Verify the environment variable LANG is set to a language installed on your workstation.

Verify that the correct locale is installed on your workstation using the `locale` and `locale -a` commands. locale will display whether the LC_MESSAGES field is the same as the LANG field. If not, try typing `locale -a` to display all the locales installed on your workstation. If the proper one is not loaded for your country you need to have it installed.

Verify that the following conditions are true:

- /usr/CML/databases contains lnmlnmemgr.pdf
- /usr/lib/nls/msg/<lang> contains a symbolic link to /usr/CML/nls/<lang>/lnmeapp.cat
- /usr/lib/nls/msg/<lang> contains a symbolic link to /usr/CML/nls/<lang>/lnmlnmemgr_dfi.cat

If everything is correctly set, contact IBM Service for more information.

740 Fatal Error. RC=<value>

Meaning: The LNM OS/2 Agent management application cannot run. In general an error message will be found in the log with the same number as the RC value.

This is not true if an error occurred when trying to establish the socket connection with lnmlnmemon or lnmlnmeint. However there should be messages in the nettl log that indicate a socket call failure. The value returned indicates one of the following

- 151 - Other
- 152 - Connect call failed
- 153 - Connection timed out
- 154 - Insufficient resources
- 155 - File descriptor table full
- 156 - Connection refused

Action: Check the nettl log for message 703 which indicates that lnmlnmemgr has terminated. Look back through the log for additional messages that indicate why lnmlnmemgr cannot run.

741 Resync failed on segment <segment number>.

Meaning: This error is displayed if the selected segment is not a Token Ring segment or the DFI message returned by the LNM OS/2 Agent for the request is not 999.

Action: If the selected segment is a Token Ring segment, check the nettl log for why the resynchronize request failed.

742 Invalid range of the attribute Please try again.

Meaning: The value entered is not valid.

Action: Enter a value within the attribute's range.

744 Unable to get data for this attribute.

Meaning: The LNM OS/2 Agent discovery application was unable to retrieve the data necessary for the LNM for AIX management application to populate the window. Either the LNM OS/2 Agent has not been discovered during this session or the agent configuration file is corrupted.

Action: If the connection with the LNM OS/2 Agent has not been established, discover the agent using the SMIT windows or the command line script cml_agent_found.

If the agent configuration file <IP address.conf> in the /usr/CML/conf/lnmlnmemon directory is corrupted, delete the file and recreate it using SMIT. If you delete the file and were collecting history on any segments or bridges, you will need to re-enable collection on those segments and bridges and reset the collection window.

745 Could not connect to <executable>.

Meaning: The LNM for AIX management application is unable to establish a connection with the named executable.

Action: Use the nettl log and cmlstatus to determine why the executable is not running.

747 Could not connect to <executable> and <executable>.

Meaning: The LNM for AIX management application is unable to establish a connection with the named executables.

Action: Use the nettl log and cmlstatus to determine why the executables are not running.

748 Interval cannot be less than 1 minute.

Meaning: The minimum value for the history collection interval for ring utilization is 1 minute.

Action: Choose a value of 1 or more. If you do not want history collected for the segment, disable collection for the segment.

749 Unable to communicate with adapter. Last known data is displayed.

Meaning: You specified an adapter that is not active on the specified LAN segment at the time of the request. The information shown is from the data in the LNM OS/2 Agent database.

Action: None.

750 Segment test for segment <segment number> completed successfully.

Meaning: The LNM OS/2 Agent successfully tested the named segment's data-transfer capability.

Action: None.

751 Resync completed successfully on segment <segment number>.

Meaning: The LNM OS/2 Agent was able to successfully complete the request to resynchronize the segment. The LNM for AIX view is being refreshed.

Action: None.

752 Resync started on segment <segment number>.

Meaning: A message has been sent to the LNM OS/2 Agent discovery application to initiate a resynchronize for the named segment.

Action: None.

753 You are about to restart the LNM OS/2 Agent <IP address>. Select OK to restart, Cancel to Abort

Meaning: You have selected an action to request that the LNM OS/2 Agent be restarted. This action will fail if the agent is not currently within the LNM for AIX managed domain or LNM for AIX cannot communicate

with LNM OS/2 Agent. If this action succeeds management of the LNM OS/2 Agent will be temporarily disrupted.

Action: Select OK or Cancel.

754 **Submitted request for LNM OS/2 Agent <IP address> to be restarted.**

Meaning: A message has been sent to the interface component to inform the LNM OS/2 Agent to restart. The agent must be currently being managed by LNM for AIX for this request to be processed.

Action: None.

755 **Timeout occurred while waiting for a response.**

Meaning: A run command has timed out.

Action: No response was received from the LNM OS/2 Agent. A run command response is expected to be received from the LNM OS/2 Agent within a designated time period. This time period is the sum of the LNM for AIX response time (transmission time, network congestion, etc) and the LNM OS/2 Agent response time multiplied by the number of requests that are currently on the LNM OS/2 Agent queue from LNM for AIX. The response time components can be set from SMIT or from the LNM OS/2 Agent Configuration windows. Initially the response time out values may need to be adjusted to reflect the realities of the network. Once a successful set of values have been selected, the occurrence of a time-out may indicate increased network traffic or that the agent is now located more hops away from LNM for AIX and the LNM for AIX response time needs to increase or it may indicate that the agent is unable to communicate with LNM for AIX but the socket connections have not gone down. DCAF or TELNET can be used to determine the state of the agent workstation if it is located remotely.

756 **You are about to delete the definition of the selected bridge(s). Select OK to delete the definition(s), Cancel to Abort**

Meaning: Delete requests will be transmitted to the LNM OS/2 Agent. A message box will be displayed for each request that fails. You will need to refresh the list to determine the request that failed.

Action: To proceed, select OK. To cancel the request, select Cancel.

757 **You are about to delete the definition of the selected Concentrators(s). Select OK to delete the definition(s), Cancel to Abort**

Meaning: Delete requests will be transmitted to the LNM OS/2 Agent. A message box will be displayed for each request that fails. You will need to refresh the list to determine the request that failed.

Action: To proceed, select OK. To cancel the request, select Cancel.

758 **You are about to delete the definition of the selected adapter(s). Select OK to delete the definition(s), Cancel to Abort**

Meaning: Delete requests will be transmitted to the LNM OS/2 Agent. A message box will be displayed for each request that fails. You will need to refresh the list to determine the request that failed.

Action: To proceed, select OK. To cancel the request, select Cancel.

759 **You are about to remove the selected adapter(s) from the network.**

Meaning: Once removed, the adapter(s) will no longer be able to communicate with the network in any way. Manual intervention at the workstation will probably be required to restore an adapter's ability to communicate with the network. Note that the removal of an adapter may adversely effect the operation of a ring. Remove requests will be transmitted to the LNM OS/2 Agent. A message box will be displayed for each request that fails. You will need to refresh the list to determine the request that failed.

Action: To proceed, select OK. To cancel the request, select Cancel.

760 **You have modified the default reporting link. To ensure bridges using the default reporting link are reset, restart the LNM OS/2 Agent.**

Meaning: The default reporting link has changed.

Action: If the setting for the Automatic bridge relink parameter has been set to Active on the LNM OS/2 agent, the agent will unlink all bridges defined to use the default reporting link and then relink them according to the new reporting link value.

To verify the setting for Automatic bridge relink, telnet into the LNM OS/2 agent machine and enter the following command:

```
LAN SYSP QUERY ATTR=BRG
```

If Automatic bridge relink is set to Inactive, it is recommended that you restart the LNM OS/2 agent. If you prefer, you can manually unlink and relink each of the bridges that is defined to use the default reporting link.

On the LNM OS/2 agent, the default value for Automatic bridge relink is Inactive.

---

801 **Trying to remove a connection that is not connected: <IP address>**

Meaning: The interface component has received a request to close the connection between the interface component and the designated LNM OS/2 Agent. The interface component has no record of the designated LNM OS/2 Agent.

Action: In general this is not expected to occur. The exception case is when the socket connections have been disrupted between LNM for AIX and the LNM OS/2 Agent for an agent discovered during this session. Executing an cml_agent_remove or any action that causes lnmlnmemon to shutdown before an attempt is made by the LNM OS/2 Agent discovery application to have the connection reinstated could lead to this error. In all other cases, it would be a programming error.

If the problem occurs in any scenario other than that described above, contact IBM Service for more information.

---

802 **Trying to add a connection that is already connected: <IP address>**

Meaning: The interface component has received a request to establish a connection with an LNM OS/2 Agent with which it already has a connection.

Action: None.

---

803 **Cannot connect to LNM OS/2 Agent with Internet address: <IP address>**

Meaning: The interface component cannot establish a socket connection with the LNM OS/2 Agent.

Action: Verify the following:

- You can ping from the OS/2 workstation to the RISC workstation and from the RISC workstation to the OS/2 workstation.
- The LNM OS/2 Agent program is running on the OS/2 workstation.
- The port for the LNM OS/2 Agent in CONFIG.SYS matches the port in the agent configuration file on LNM for AIX. If there is no port defined in CONFIG.SYS, the port defined in the agent configuration file on LNM for AIX must be 7605.
- The selected socket is not in use on the OS/2 workstation.
- The correct address is resolved from the host name on the OS/2 workstation.
- There are buffers available for TCP/IP on the OS/2 workstation.
- There are no errors when TCP/IP starts on the OS/2 workstation.
- Only one LNM for AIX can establish connection with the LNM OS2 agent at a time.
- After resolving all of the above items, if the problem persists shutdown the LNM OS/2 Agent workstation and restart it.

---

804 **No Internet address matches the destination of the run command: <IP address>**

Meaning: The interface component has received a request to transmit a run command to an unknown agent. This occurs if a request is sent from the LNM OS/2 Agent management application before an attempt to discover the agent by the LNM OS/2 Agent discovery application is made during this session or the agent is temporarily unavailable due to a RESTART request or failure of the socket from the interface component to the LNM OS/2 Agent.

Action: Review the nettl log to determine if a connection to the agent has not been established (message 803). If no cml_agent_found has been executed for the agent during this session, issue one. If a RESTART was requested, retry the operation later.

---

805 **The socket connection is broken from lnmlnmeint to one of its clients. Bytes received = <number of bytes read>**

Meaning: This message will be written when a socket connection is closed or fails between lnmlnmeint and lnmlnmemgr or lnmlnmemon. If bytes received if less than 0 a socket has closed, otherwise an error has occurred in the read system call.

Action: If an LNM OS/2 Agent has just been removed or a shutdown has been issued, it will be normal to see this message and bytes received should be zero. However, if communications do not seem to be functioning properly and this message is in the log, look for earlier indications in the log for why the interprocess communications are failing.

---

806 **Connection failure for LNM OS/2 Agent at: <IP address>**

Meaning: Either a send or receive on the Internet socket returned a socket error or indicated that the socket is closed.

Action: If the LNM OS/2 Agent was exited or the workstation was shutdown deliberately, no action is required. Otherwise, use the nettl log and trapd.log for an indication of why the connection to the LNM OS/2 Agent was dropped. DCAF or TELNET can be used to determine the state of the agent workstation if it is located remotely.

---

807 **Unidentified data received and ignored. Agent <IP address> Command Type <command mapping> Data = < dump of part of the buffer > File = <source file name>, Line = <line number>**

Meaning: Data returned to the interface component as a run command response did not match the expected response format. The first part of the response is written to the log. Only commands which return data in the response are mapped to a command type. The commands that return data in the response and are used by the LNM OS/2 Agent discovery and management applications are described in the following list:

Command type	Command
23006	LAN ADP LIST SEG=<segment number>
11011	LAN ADP QUERY ADP=<adapter address> SEG=<segment number>
11015	LAN ADP QUERY ADP=<adapter address> SEG=<segment number> ATTR=ATTACH
11016	LAN ADP QUERY ADP=<adapter address> SEG=<segment number> ATTR=PCINFO
33054	LAN BRG LIST ATTR=MSM
21020	LAN BRG QUERY NAME=<bridge name> ATTR=CONF
21023	LAN BRG QUERY NAME=<bridge name> ATTR=STATIC
21024	LAN BRG QUERY NAME=<bridge name> ATTR=MAPPED
21021	LAN BRG QUERY NAME=<bridge name> ATTR=PRF
21022	LAN BRG QUERY NAME=<bridge name> ATTR=RPT
21025	LAN BRG QUERY NAME=<bridge name> ATTR=DEFINE
43000	LAN CAU LIST
31063	LAN CAU QUERY UNIT=<unit id>
31096	LAN CAU QUERY UNIT=<unit id> ATTR=WRAP
31127	LAN CAU QUERY UNIT=<unit id> MOD=<module number>
31161	LAN CAU QUERY UNIT=<unit id> MOD=<module number> ATTR=LOBE
61000	LAN SYSP QUERY
61044	LAN SYSP QUERY ATTR=MIS
61049	LAN SYSP QUERY ATTR=ALL
49000	LAN NETWORK STATUS
49006	LAN NETWORK STATUS SEG=<segment number>
60006	LAN SEGMENT UTIL SEG=<segment number>
82052	LAN TRPFLTR SET ATTR=ENABLE
82053	LAN TRPFLTR SET ATTR=DISABLE
103000	LAN CAUQUAL LIST

Action: It is possible for this situation to occur if the data on the socket is corrupted. Verify the run command is returning a valid response by executing it in the OS/2 window. If the response is valid, retry the operation. If the problem persists, contact IBM Service for more information.

808 **Received more than maximum supported adapter entries. The excess entries are discarded. Agent <IP address> File = <source file name>, Line = <line number>**

Meaning: The LNM for AIX application supports a maximum of 500 adapters in the run command responses for any LAN ADP LIST, LAN BRG QUERY ATTR=MAPPED or LAN BRG QUERY ATTR=STATIC request.

Action: Remove unnecessary adapter definitions.

809 **Received more than maximum supported bridge entries. The excess entries are discarded. Agent <IP address> File = <source file name>, Line = <line number>**

Meaning: The LNM for AIX application supports a maximum of 500 bridges in any LAN BRG LIST run command response.

Action: Remove unnecessary bridge definitions.

810 **Received more than maximum supported Concentrator entries. The excess entries are discarded. Agent <IP address> File = <source file name>, Line = <line number>**

Meaning: The LNM for AIX application supports a maximum of 1000 concentrators in the LAN CAU LIST run command response.

Action: Remove unnecessary concentrator definitions.

811 **The LNM OS/2 Agent <IP address> cannot execute the LAN command. Error code = <value>, File = <source file name>, Line = <line number>**

Meaning: The LNM OS/2 Agent program is unable to process the run command.

Action: The action depends on the error code:

2: LNM OS/2 can not initialize the command line thread. Either end another OS/2 application(s) or increase the THREADS parameter in your CONFIG.SYS and reboot the workstation.

6: The command line queue was full. If the failure is in response to a request from a panel, retry the operation. If the failure occurred during discovery, discovery will be retried in 5 minutes. If the same message repeats, reboot the agent OS/2 machine.

7: An internal error in the agent occurred. If the failure is in response to a request from a panel, retry the operation. If the failure occurred during discovery, discovery will be retried in 5 minutes. If the same message repeats, reboot the agent OS/2 machine.

8: An internal error in the agent occurred. If the failure is in response to a request from a panel, retry the operation. If the failure occurred during discovery, discovery will be retried in 5 minutes. If the same message repeats, reboot the agent OS/2 machine.

812 **The LNM OS/2 Agent <IP address> cannot set the trap filter. File = <source file name>, Line = <line number>**

Meaning: The request to enable or disable traps failed. LNM for AIX will continue to process run commands but the status of the topology display will only be as current as the last refresh of the agent view on LNM for AIX.

Action: The action depends on the error code:

10: Verify the following:

- You can ping from the OS/2 machine to the RISC machine and from the RISC machine to the OS/2 machine.
- The community name in CONFIG.SYS matches the community name for the agent known to AIX NetView/6000.
- You have a current SNMP PW file on the OS/2 machine.
- SNMPTRAP.DST contains the IP address of LNM for AIX.
- SNMPD is running on the OS/2 machine.
- There are no messages from the LNM OS/2 Agent on start up that indicate it cannot get the trap thread going.
- The name in your HOST file in the TCP/IP directory on the OS/2 machine matches the host name in CONFIG.SYS.

11: LNM OS/2 can not initialize the trap thread. Either end another OS/2 application(s) or increase the THREADS parameter in your CONFIG.SYS and reboot the workstation.

813 **Unknown command received at the LNM OS/2 agent <IP address>. File = <source file name>, Line = <line number>**

Meaning: A run command request has been received by the interface component that is not within the set of commands it is set up to handle.

Action: It is possible for this situation to occur if the data on the socket is corrupted. Retry the operation. If the condition persists, contact IBM Service for more information.

814 **A timeout occurred on an LNM OS/2 Agent <IP address> correlator = <correlator>.**

Meaning: A run command has timed out.

Action: No response was received from the LNM OS/2 Agent. A run command response is expected to be received from the LNM OS/2 Agent within a designated time period. This time period is the sum of the LNM for AIX response time (transmission time, network congestion, etc) and the LNM OS/2 Agent response time multiplied by the number of requests that are currently on the LNM OS/2 Agent queue from LNM for AIX. The response time components can be set from SMIT or from the LNM OS/2 Agent Configuration windows. Initially the response time out values may need to be adjusted to reflect the realities of the network. Once a successful set of values have been selected, the occurrence of a time-out may indicate increased network traffic or that the agent is now located more hops away from LNM for AIX and the LNM for AIX response time needs to increase or it may indicate that the agent is unable to communicate with LNM for AIX but the socket connections have not gone down. DCAF or TELNET can be used to determine the state of the agent workstation if it is located remotely.

818 **Unexpected value <value> in switch statement in procedure <procedure name> File = <source file name>, Line = <line number>**

Meaning: The data does not conform to the expected set.

Action: In general this indicates a programming error. If it does not reoccur it can be due to a failure in the transmission of data on the socket. If it reoccurs, contact IBM Service for more information.

820 **Socket connection from lnmlnmeint to lnmBaseTimer failed**

Meaning: A communications error has been detected, an attempt is made to recover. Timed events are resubmitted but times are not recalculated.

Action: Check the nettl log to determine why communications failed.

821 **Received more than maximum supported concentrator qualifier entries. The excess entries are discarded. Agent <IP address> File = <source file name>, Line = <line number>**

Meaning: The LNM for AIX application supports a maximum of 256 concentrator qualifiers in the LAN CAUQUAL LIST run command response.

Action: Remove unnecessary concentrator qualifier definitions.

901 **SNMP error -- OVsnmpErrno: <error number>, nvSnmpErrno: <NetView error number> , nvSnmpSubsys: <NetView snmp subsystem>, File:<file name>, Line:<line number>**

Meaning: The trap processor failed in an attempt to open a session with NetView for AIX to send a trap.

Action: Look at the man page for OVsnmpOpen. The error codes should help you determine the correct action to take. If they do not, then shut down and restart LAN Network Manager for AIX and NetView for AIX. If the problem persists, contact IBM Service for more information.

902 **Unable to close SNMP session -- OVsnmpErrno: <error number> File: <file name>, Line: <line number>**

Meaning: The trap processor has failed in an attempt to close a trap session with NetView for AIX.

Action: Look at the man page for OVsnmpClose. The error code should help you determine the correct action if any to take to take. If traps are continuing to flow from AIX NetView/6000 to LNM for AIX and back for all monitored agents, no action additional action is necessary. If the trap flow does not recover, then shut down and restart LAN Network Manager for AIX and NetView for AIX. If trap processing cannot be recovered, contact IBM Service for more information.

903 **Unable to get filter from NetView for AIX, return code is <return code>. File: <file name>, Line: <line number>**

Meaning: The trap processor has failed in an attempt to retrieve a trap filter file.

Action: Look at the man page for nvFilterGet. The error code should help you determine the correct action to take. If it does not, then shut down and restart LAN Network Manager for AIX and NetView for AIX. Both applications must be started with root privileges. If the problem persists, contact IBM Service for more information.

905 **Attempt to delete unknown agent <agent name>. File: <file name>, Line: <line number>**

Meaning: An application is attempting to delete an agent that is unknown to the trap processor.

Action: None. If the problem persists, contact IBM Service for more information.

906 **Unable to create trap -- OVsnmpErrno: <error number>. File: <file name>, Line: <line number>**

Meaning: The trap processor failed in an attempt to build a trap to send to NetView for AIX.

Action: Look at the man page for OVsnmpCreatePdu. The error code should help you determine the correct action to take. If it does not, then shut down and restart LAN Network Manager for AIX and NetView for AIX. If the problem persists, contact IBM Service for more information.

907 **Unable to send trap -- OVsnmpErrno: <error number>. File: <file name>, Line: <line number>**

Meaning: The trap processor failed in an attempt to send a trap to NetView for AIX.

Action: Look at the man page for OVsnmpSend. The error code should help you determine the correct action to take. If it does not, then shut down and restart LAN Network Manager for AIX and NetView for AIX. If the problem persists, contact IBM Service for more information.

910 **Received invalid trap. File: <file name>, Line: <line number>**

Meaning: Validation failed on a trap sent from the agent to LAN Network Manager for AIX.

Action: None; the trap may have just be corrupted during transmission. If the problem persists, contact IBM Service for more information.

951 **LNM databases are already empty.**

Meaning: No LNM objects were found in the database.

Action: None.

952 **LNM databases will be cleared. Proceed Y/N ?**

Meaning: You have requested that all LNM objects be removed from the database.

Action: Type **Y** if you wish to continue; otherwise, type **N** to cancel the operation.

955 **Unable to send message number <message_number> to ATM topology. Return code was <return_code>.**

Meaning: A communication failure occurred between a ahmtopod and lnmtopod.

Action: Ensure ovstatus

956 **Started up ATM topology interface.**

Meaning: This message is written to the log when ahmtopod sends a start message to lnmtopod.

Action: None.

957 **Shutting down interface with ATM topology.**

Meaning: This message is written to the log when lnmtopod receives a shutdown message and there is a start message from ahmtopod during the same session.

Action: None.

960 **nvot_server connection was not established.**

Meaning: Topology Services was unable to connect to the nvot_server daemon.

Action: Use ovstatus to determine why the nvot_server daemon is not running. Use ovstart nvot_server to start the daemon. Restart LNM for AIX using ovstart cmld.

961 nvot_server connection already established.

Meaning: A connection with the nvot_server daemon was established already when another attempt to do so was made.

Action: None.

1000–1999 Message received from the OS/2 agent program.

Meaning: Messages with numbers between 1000 and 1999 are sent to LAN Network Manager from the OS/2 agent program.

Action: Refer to the documentation that is provided with the OS/2 agent for an explanation of the message and suggested actions to take to resolve the problem.

LAN Network Manager appends a 1 to the front of the message number that it receives from the OS/2 agent. Before consulting the agent documentation, identify the appropriate message number for the OS/2 agent by removing the 1 from the number. For example, message number 1300 on LAN Network Manager corresponds to message number 300 on the OS/2 agent.

Messages 2001 to 2505

2001 Starting lnmbrmgr.

Meaning: The bridge management application has started.

Action: None.

2002 Stopping lnmbrmgr.

Meaning: The bridge management application has terminated due to NetView for AIX terminating or because of an unexpected error.

Action: None.

2003 The NLS catalog file <filename> was not found.

Meaning: The bridge management application was unable to open the specified catalog file. Default text will be displayed in English.

Action: Ensure the environment variables LANG and NLSPATH are properly set for your AIX workstation. Also, be sure the correct locale is installed on your AIX workstation.

2004 lnmbrmon terminated.

Meaning: The bridge discovery application has terminated while the bridge management application had a socket connection with it.

Action: If you did not intend to stop the bridge discovery application, you can restart it with cmlstart.

2005 lnmbrmon socket has failed.

Meaning: The bridge management application was unable to communicate with the bridge discovery application because of a severe error.

Action: The bridge management application will shutdown immediately. Stop and restart LAN Network Manager.

2006 lnmbrmon is not running.

Meaning: The bridge management application was unable to communicate with the bridge discovery application because the bridge discovery application is not running.

Action: Stop and restart LAN Network Manager.

2007 Unable to open socket to lnmbrmon.

Meaning: The bridge management application was unable to communicate with the bridge discovery application because of a severe error.

Action: Stop and restart LAN Network Manager and NetView for AIX.

2008 SNMP timeout on request.

Meaning: An SNMP request timed out because the IP address is not valid or the community name is not valid.

Action: Verify that the IP address is correct.

Verify that the IP address exists on the network (ping the address).

Verify that the community name is correct using the NetView for AIX SNMP Configuration option.

Increase the timeout interval. If that fails, contact IBM Service for more information.

2010 SNMP noSuchName error. For a set, the value is read-only or the community name is not valid.

Meaning: The requested SNMP OID does not exist on the SNMP agent. If you are attempting to set a value, the value may be read-only or you may be using a community name that is not valid.

Action: If this SNMP OID is not supported by the SNMP agent, no value can be retrieved and displayed to the user. If a value is displayed and you are trying to change it, ensure you are using the proper community name. Check the SNMP Configuration from NetView for AIX and the SNMP community name on the agent that allows read/write authority.

2011 SNMP badValue error.

Meaning: An attempt to SET an SNMP OID has failed because the value is outside the allowable values.

Action: Check the value you are trying to set and ensure it is valid. Retry the operation.

2012 SNMP readOnly error.

Meaning: The SNMP OID you are trying to set is read only.

Action: Since this SNMP OID is read only on the SNMP agent you will not be allowed to set it.

2015 Memory allocation failed.

Meaning: The bridge management application was unable to allocate memory.

Action: In the short term, shut down some other applications, then restart LAN Network Manager. In the long term, obtain more memory.

2018 Cannot establish an SNMP session.

Meaning: The bridge management application was unable to open an SNMP session using the NetView for AIX API services.

Action: Close several windows and retry the operation. If the problem persists, stop and restart NetView for AIX and LAN Network Manager and retry the operation.

2022 This parameter is below the minimum value.

Meaning: The parameter you are attempting to set is below the minimum value.

Action: Increase the value so that it is equal to or greater than the minimum value and retry the operation.

2023 This parameter is above the maximum value.

Meaning: The parameter you are attempting to set is above the maximum value.

Action: Decrease the value so that it is equal to or less than the maximum value and retry the operation.

2024 Resync started for subnet <name>.

Meaning: The user has requested that a resynchronize be done for the specified subnet.

Action: None. The user will be notified when the resynchronize completes.

2025 Polling started for agent <name>.

Meaning: The user has requested that a poll be done for the specified agent.

Action: None. The user will be notified when the poll completes.

2026 Resync completed for subnet <name>.

Meaning: A user requested resynchronize has completed.

Action: None.

2027 **Polling completed for agent <name>.**

Meaning: A user requested poll has completed.

Action: None.

2028 **Resync in progress for subnet <name>.**

Meaning: The user requested to resynchronize the subnet but a resync is already in progress.

Action: Wait for the resynchronize to complete before requesting another.

2029 **Polling in progress for agent <name>.**

Meaning: The user requested to poll the agent but a poll is already in progress.

Action: Wait for the poll to complete before requesting another.

2030 **Unable to read the configuration file.**

Meaning: The bridge management application requested information from the bridge discovery application but the bridge discovery application was unable to read the information from the configuration file.

Action: Use SMIT to verify the bridge SNMP application bridge parameters are correct.

2031 **Unable to write to the configuration file.**

Meaning: The bridge management application requested for the bridge discovery application to save information but the bridge discovery application was unable to write the information to the configuration file.

Action: Use SMIT to verify the bridge SNMP application bridge parameters are correct. Try the same operation from the SMIT window. Also, verify that the user has write authority for the configuration file.

2032 **No SNMP data was collected.**

Meaning: This attribute is a combination of SNMP values. If any one of the SNMP values could not be collected, this message is used.

Action: Verify that the SNMP OIDs used in this calculation are valid for the SNMP agent by selecting the **Details** push button.

2033 **Starting the user definable device configuration program <filename>. Please read the documentation for more information about setting up this option.**

Meaning: The Device Configuration pushbutton on the Bridge Configuration window was selected and the specified script file has been executed. If you want to use other external configuration programs you can use this feature to invoke the programs from the bridge management application.

Action: For more information on setting up this option, please refer to *Using LAN Network Manager for AIX*.

2034 **Unable to run the device configuration program <filename>.**

Meaning: The specified program was unable to be executed. Either you do not have execute authority or the program does not exist.

Action: Verify that the program exists and you have the proper permissions to execute it.

2101 **Cannot open SNMP session for agent. IP Address = <IP address> errno = <error number> File = <filename>, Line = <line number>**

Meaning: The OVsnmpXOpen failed for the SNMP agent listed in the IP Address field.

Action: Use the NetView/6000 reference manual and follow the instructions for the error number.

2102 **SNMP get error for agent. IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: Error allocating the correlator for the SNMP get request.

Action: Try stopping and restarting LNM for AIX. Contact IBM Service for more information.

2103 **SNMP get response error for agent. IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: A get request for the SNMP agent with the IP Address failed.

Action: Verify that the SNMP agent is up by using the MIB browser and issuing get requests on the IP Address

specified in the message. If the agent is working, stop and restart LNM for AIX. If that does not solve the problem, contact IBM Service for more information.

2104 **Error: snmp unknown response IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: The SNMP bridge application received a NULL PDU from the agent. The bridge will be placed in the undiscovered subnet.

Action: If the bridge is responding properly, it should be rediscovered the next time a poll request is issued.

2105 **Error: Request ID failed in <function> IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: Error allocating the correlator for the SNMP get request.

Action: Try stopping and restarting LNM for AIX. If the error persists, contact IBM Service for more information.

2107 **Request for unknown resource <resource name> File = <filename>, Line = <line number>**

Meaning: A delete agent was received, but the agent is not currently being managed by the bridge application.

Action: The request is ignored.

2108 **Unexpected value in switch statement Procedure <name>. Switch value = <value> File = <filename>, Line = <line number>**

Meaning: This is a `catch all` message that dumps any unexpected values. The switch value will indicate the value that caused the error. The file can be used to determine the kind of problem that occurred.

Action:

1. EZVDGUTILITY.C

   The bridge application has received a signal that it does not process. The default action for the signal will be taken. Refer to AIX documentation for details.

   None.

2. EZVDGtrapCallback.C

   The bridge application received a trap from an agent that the bridge application does not support. The trap will be ignored. The IP Address identifies the bridge that is sending the traps.

   Verify that the bridge filter files are correct.

3. EZVDGtimerClient.C

   The bridge application is receiving timer messages that are not supported by the bridge application.

   Verify that automatic polling and resynchronize are working.

4. EZVDGsubnet.C

   There are several possibilities for subnet. The procedure will determine the cause of the error for subnet.C

   a. addBridge

      The bridge received an invalid response from the agent for the dot1dBaseType. The value returned is in switch value. Verify that this value maps to the value returned by the MIB browser.

      If the switch value matches the value returned by the MIB browser, the agent is not supporting RFC 1286 properly. Report the problem to the bridge vendor.

   b. handleTrap

      The bridge application received a trap from an agent that the bridge application does not support. The trap will be ignored. The IP Address identifies the bridge that is sending the traps.

      Verify that the bridge filter files are correct.

   c. handleTimerPop

      The bridge application is receiving timer messages that are not supported by the bridge application.

      Verify automatic resynchronize is working is still working.

5. EZVDGsegManager.C

   An invalid protocol was detected.

   The bridge application will use `other` as a default in this case. Verify that the bridge is properly setting the RFC 1231(MIB II) ifType correctly.

6. EZVDGport.C

   An invalid SNMP response was received. The bridge will be placed in the undiscovered subnet.

   Verify that the agent specified in the IP address is working correctly and then poll the agent. Verify that the SNMP agent is up by using the MIB browser and issuing get requests on the IP Address specified in the message. If the agent is working, stop and restart LNM for AIX. If that does not solve the problem, contact IBM Service for more information.

7. EZVDGcpClient.C

   The bridge discovery application received an invalid request from the control Program. This is a programming error.

   The bridge application will ignore the request.

8. EZVDGbridge.C

   An invalid SNMP response was received. The bridge will be placed in the undiscovered subnet.

   Verify that the agent specified in the IP address is working correctly and then poll the agent. Verify that the SNMP agent is up by using the MIB browser and issuing get requests on the IP Address specified in the message. If the agent is working, stop and restart LNM for AIX. If that does not solve the problem, contact IBM Service for more information.

9. EZVDGapplication.C

   There are several possibilities for application. The procedure will determine the cause of the error for application.C

   a. handleTimerResponsePop -

      The bridge application is receiving timer messages that are not supported by the bridge application.

      Verify automatic resynchronize and polling are working.

   b. recoverTimer

      The bridge application is attempting to recover from a timer socket failure and discovered invalid timer items. The bridge application should recover and continue processing.

      Verify automatic resynchronize and polling are working.

10. EZVDGagent.C

    There are several possibilities for agent. The procedure will determine the cause of the error for agent.C

    a. handleTimerResponsePop

       The bridge application is receiving timer messages that are not supported by the bridge application.

       Verify automatic polling is working is still working.

    b. snmpResponse

       An invalid SNMP response was received. The bridge will be placed in the undiscovered subnet.

       Verify that the agent specified in the IP address is working correctly and then poll the agent. Verify that the SNMP agent is up by using the MIB browser and issuing get requests on the IP Address specified in the message. If the agent is working, stop and restart LNM for AIX. If that does not solve the problem, contact IBM Service for more information.

11. StandAloneBridge.C

    The bridge received an invalid response from the agent for the dot1dBaseType. The value returned is in switch value. Verify that this value maps to the value returned by the MIB browser.

    If the switch value matches the value returned by the MIB browser, the agent is not supporting RFC 1286 properly. Report the problem to the bridge vendor.

2109 Socket connection from <executable> to <executable> failed in <function>. Return Code= <rc>, File = <filename>, Line = <line number>

Meaning: This is a `catch all` message for socket errors. The connection that failed is identified by the component that is connected to lnnbrmon. The following is the action taken depending on the failing component.

Action:

- cmld

  This is the control program. The bridge application will terminate when this socket connection fails.

  Fix the control program and then restart LNM for AIX

- lnmtopod

  The bridge application will terminate when its connection to topology fails. The status of the bridge icons may be incorrect after lnmbrmon terminates.

  Fix the topology failure and then restart the LNM for AIX

- lnmBaseTimer

  The bridge application will continually attempt to recreate the timer.

  None.

- lnmbrmgr

  The bridge application will recreate the socket and wait for the bridge window application to restart.

  None.

- OVsnmp Trap Session

  The bridge application will attempt to recreate the trap session.

  Verify that traps are still being received.

2111 **Request for duplicate resource <resource name>. File = <filename>, Line = <line number>**

Meaning: A duplicate agent found message has been detected. The duplicate request will be ignored.

Action: None.

2112 **Wrong response in <function>. type = <SNMP response>, IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: The bridge application issued a get or get-next request and it received an invalid SNMP response. The bridge will be placed in the undiscovered subnet.

Action: This should not happen. Verify that the agent in the IP Address field is functioning properly.

2113 **SNMP error in <function>. errorStatus = <number>, IP Address = <IP address>, errorIndex = <number> File = <filename>, Line = <line number>**

Meaning: The bridge application received an SNMP error back from a get or get-next request. This is most likely an agent error.

Action: Verify that the agent identified by IP the address works with the MIB browser. Verify that all MIB II(RFC 1213) and bridge(RFC 1286) attributes can be retrieved by the MIB browser.

If you see this message in SnmpBrPort::processingPortIfIndex, check that there is an ifIndex in MIB II that corresponds to the RFC 1286 basePortIfIndex. This is a common problem with OS/2 bridges that use TCP/IP. The following example shows two base ports that map back to MIB II inIndex 1 and 2. In this example the MIB II ifIndex is missing for ifIndex 2, so the bridge cannot be discovered.

```
MIB II
   ifType problems (OS/2 agents)
   ..ifTable.ifEntry.ifType.1 iso8802-tokenring

RFC 1286
   ..dot1dBasePortEntry.dot1dBasePortIfIndex.1 1
   ..dot1dBasePortEntry.dot1dBasePortIfIndex.2 2
```

2114 **Wrong OID returned in <function>. errorStatus = <number>, IP Address = <IP address>, errorIndex = <number>, OID = <object ID>, File = <filename>, Line = <line number>**

Meaning: The bridge application received an SNMP error back from a get or get-next request. This is most likely an agent error.

Action: Verify that the agent identify by the IP address works with MIB browser. Verify that all MIB II(RFC 1213) and bridge(RFC 1286) attributes can be retrieved by the MIB browser.

2115 **No Matching Base port for <port type> Port in <function>. IP Address = <IP address>, OID = <object ID>, value = <object value>, File = <filename>, Line = <line number>**

Meaning: The bridge application maps the RFC 1286 SR, TP, and STP tables to the RFC 1286 BasePort table. Multiple algorithms are used to try to perform this mapping. In this case, the bridge application cannot map RFC 1286 ports for this bridge.

Action: Dump the dot1dBridge attributes using the MIB browser verify that the number of SR, TP, STP, and base ports do not match.

SR and TP ports are ignored if they do not match a base port. In this case below, dot1dSRPort.3 does not match and the bridge application will not report the port as an SR port.

```
RFC 1286
   ..dot1dBasePortEntry.dot1dBasePortIfIndex.1 1
   ..dot1dBasePortEntry.dot1dBasePortIfIndex.2 2
   ..dotd1dSrPortEntry.dot1dSRPort.1 : 1
   ..dotd1dSrPortEntry.dot1dSRPort.2 : 2
   ..dotd1dSrPortEntry.dot1dSRPort.3 : 3
```

If STP ports cannot be mapped to the base ports, the discovery for that bridge is terminated and the bridge is placed in the undiscovered subnet.

```
RFC 1286
  ..dot1dBasePortEntry.dot1dBasePortIfIndex.1 1
  ..dot1dBasePortEntry.dot1dBasePortIfIndex.3 3
  ..dotdStpPortEntry.dot1dStpPort.1 : 1
  ..dotdStpPortEntry.dot1dStpPort.2 : 2
  ..dotdStpPortEntry.dot1dStpPort.3 : 3
```

2116 **Unknown Port Type in <Procedure> IP Address = <IP address>, MAC Address = <address>, IfIndex = <number> File = <filename>, Line = <line number>**

Meaning: The bridge application discovered a base port with the corresponding ifIndex that did not have a matching entry in the SR port table or the TP port table.

Action: The bridge application will continue processing. This is a possible bridge configuration error, or a non-standard bridge.

2117 **Wrong Interface Type in <function>. original interface type = <number> new interface type = <number> segment number = <number> desigBridge = <bridge>, desigPort = <port> File = <filename>, Line = <line number>**

Meaning: The bridge application discovered the same segment with a different ifType.

Action: Verify the bridge configuration.

2119 **Trap from invalid agent with OID = <object ID> received in <function>. File = <filename>, Line = <line number>**

Meaning: The bridge application received a trap from an agent that the bridge application does not support. The trap will be ignored. The IP Address identifies the bridge that is sending the traps.

Action: Verify that the bridge filter files are correct.

2120 **Cannot get text from the message catalog in <function>. Default text = <text> Text ID = <number> File = <filename>, Line = <line number>**

Meaning: The NLS catalog could not be open. This may be an installation problem. The bridge application will continue with default text in English.

Action: Ensure the environment variables LANG and NLSPATH are properly set for your AIX workstation. Also, be sure the correct locale is installed on your AIX workstation.

2121 **Error accessing the Bridge config file in = <function>. Return code = <number> fileName = <filename>, record = <record> File = <filename>, Line = <line number>**

Meaning: The bridge parameters window attempted to update the bridge configuration file `/usr/CML/conf/lnmbrmon/lnmbrmon.default.conf` The update failed.

Action: Verify that the access permissions and owner are correct.

2122 **Unexpected Trap in <function>. Generic number = <number>, specific Number = <number>, IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: The bridge application received a generic trap (RFC 1157).

Action: This is a warning message so that traps about the community name are logged.

2123 **Unexpected Bridge Configuration in <function>. IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: The number of unique ifIndices found for this bridge was 0.

Action: Verify the bridge configuration for the specified IP address.

2124 **SNMP Time out <function>. type = <number> IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: An SNMP timeout has occurred while attempting to discover or poll the bridge. The bridge will be placed in the undiscovered subnet.

Action: Verify that the agent is up and that you can retrieve attributes using the MIB browser. If so, attempt to poll the bridge. If you still receive timeout messages, change the SNMP timeout parameters in NetView/6000.

2125 **Socket connection from <executable> to <executable> failed in <function>. errno = <number> File = <filename>, Line = <line number>**

Meaning: The bridge application will recreate the socket and wait for the bridge window application to restart.

Action:

- cmld

  This is the control program. The bridge application will terminate when this socket connection fails.

  Fix the control program and then restart LNM for AIX

- lnmtopod

  The bridge application will terminate when its connection to topology fails. The status of the bridge icons may be incorrect after lnmbrmon terminates.

  Fix the topology failure and then restart the LNM for AIX

- lnmBaseTimer

  The bridge application will continually attempt to recreate the timer.

  None.

- lnmbrmgr

  The bridge application will recreate the socket and wait for the bridge window application to restart.

  None.

- OVsnmp Trap Session

  The bridge application will attempt to recreate the trap session.

  Verify that traps are still being received.

2126 **Error communicating with the <executable> application in <function>. Correlator = <number> Resource = <name> File = <filename>, Line = <line number>**

Meaning: The bridge application has encountered an error while attempting to communicate with the management application.

Action: This is a normal message if the management application terminates. The bridge application will continue processing.

2128 **Subnet could not be found for agent. IP Address = <IP address> Not found in <function> File = <filename>, Line = <line number>**

Meaning: The bridge application is receiving traps from an agent that it has not properly discovered.

Action: Poll the bridge and then resynchronize the subnet. If that fails to solve the problem, stop and restart LNM for AIX.

2129 **Parent with name = <name> not found for segment = in <function>. File = <filename>, Line = <line number>**

Meaning: The bridge application detected an error while cleaning up.

Action: Stop LAN Network Manager, use SMIT to clear the LAN Network Manager databases, then restart LAN Network Manager.

2130 **Error removing element from the list in <function>. File = <filename>, Line = <line number>**

Meaning: The bridge application detected an error while cleaning up.

Action: Stop LAN Network Manager, use SMIT to clear the LAN Network Manager databases, then restart LAN Network Manager.

2134 **Cannot discover agent due to an SNMP timeout. IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: An SNMP timeout has occurred while attempting to discover or poll the bridge. The bridge will be placed in the undiscovered subnet.

Action: Verify that the agent is up and that you can retrieve attributes using the MIB browser. If so, attempt to poll the bridge. If you still receive timeout messages, change the SNMP timeout parameters in NetView/6000.

2135 **Socket connection not yet established from <executable> to <executable>. File = <filename>, Line = <line number>**

Meaning: The timer has not started yet.

Action: The bridge application will wait 60 seconds and retry.

2137 **Bridges with same designated bridge and designated port, but with different segment numbers in <function>. resourceNames = <name> and <name>. File = <filename>, Line = <line number>**

Meaning: The bridge has detected a very unusual configuration. The IP Address of the bridges involved are located in the resource names. This may be a configuration error, or it could be caused by a bridge reporting invalid values.

Action: Verify your segment numbers in the bridge configuration.

2138 **Attempting to create the same bridge with different IP address. IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: Most bridges allow multiple IP Address to be configured for the same agent. The bridge application will verify the baseBridgeAddress to prevent the same bridge from being discover twice from two different IP addresses.

Action: Remove the duplicate agent IP address using SMIT.

2139 **Attempting to make another shutdown when the application is already in the shutdown state. File = <filename>, Line = <line number>**

Meaning: The bridge application will continue to shutdown. The request is ignored.

Action: None.

2141 **The trap session has been closed. IP Address = <IP address> File = <filename>, Line = <line number>**

Meaning: An error has been encountered with opening and closing the SNMP traps session.

Action: Verify that the NetView/6000 trap daemons are up. Stop and restart LNM for AIX.

2143 **Invalid spanning tree configuration in <name>, for resource=<name>, segment number=<value>, File=<file name>, line=<line number>**

Meaning: The bridge has detected a very unusual configuration. This may be a configuration error, or it could be caused by a bridge reporting some invalid values.

Action: Verify the spanning tree configuration for the ports connected to the segment with the specified segment number.

2144 **EUI resynchronize failed. Return Code=<value>, IP address=<IP address>**

Meaning: Resynchronize requested by the user failed

Action: If the problem persists, stop and restart LNM for AIX.

2201 **Topology Connection error, rc = <TopoReturnCode>**

Meaning: Application exits due a topology connection error.

Action: Run cmlstatus to verify whether lnmtopod is running. If it is running check the nettl log and correct any problems found. If it is not running, restart LNM for AIX. If the problem persists, contact IBM Service for more information.

2202 **Topology error changing station status, rc = <TopoReturnCode>, resource = <StationName>**

Meaning: An error occurred on changeResourceStatus topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2203 **Topology error changing station extension, rc = <TopoReturnCode>, resource = <StationName>**

Meaning: An error occurred on changeResourceExtension topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2204 **Topology error changing station label, rc = <TopoReturnCode>, resource = <StationName>**

Meaning: An error occurred on changeResourceLabel topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2205 **Topology error creating station, rc = <TopoReturnCode>, resource = <StationName>**

Meaning: An error occurred on createBoxGraph topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2206 **Topology error inserting station, rc = <TopoReturnCode>, resource = <StationName>**

Meaning: An error occurred on insertResource topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2207 **Topology error creating station (by trap), rc = <TopoReturnCode>, resource = <StationName>**

Meaning: An error occurred on createBoxGraph topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2208 **Topology error creating arc, rc = <TopoReturnCode>**

Meaning: An error occurred on createArc topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2209 **Topology error creating concentrator box rc = <TopoReturnCode>, resource = <ConcentratorName>**

Meaning: An error occurred on createBoxGraph topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2210 **Topology error changing concentrator status, rc = <TopoReturnCode>, resource = <ConcentratorName>**

Meaning: An error occurred on changeResourceStatus topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2211 **Topology error changing concentrator label, rc = <TopoReturnCode>, resource = <ConcentratorName>**

Meaning: An error occurred on changeResourceLabel topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2212 **Topology error changing concentrator extension, rc = <TopoReturnCode>, resource = <ConcentratorName>**

Meaning: An error occurred on changeResourceExtension topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2213 **Topology error deleting concentrator, rc = <TopoReturnCode>, resource = <ConcentratorName>**

Meaning: An error occurred on deleteResource topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2214 **Topology error removing concentrator, rc = <TopoReturnCode>, resource = <ConcentratorName>**

Meaning: An error occurred on removeResource topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2215 **Topology error changing segment contents, rc = <TopoReturnCode>, resource = <SegmentName>**

Meaning: An error occurred on changeViewContents topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2216 **Topology error deleting station, rc = <TopoReturnCode>, resource = <StationName>**

Meaning: An error occurred on deleteResource topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2217 **Topology error removing station, rc = <TopoReturnCode>, resource = <StationName>**

Meaning: An error occurred on removeResource topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2218 **Topology error resyncing segment, rc = <TopoReturnCode>, resource = <SegmentName>**

Meaning: An error occurred on a resynchronize topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2219 **Topology error changing segment status, rc = <TopoReturnCode>, resource = <SegmentName>**

Meaning: An error occurred on changeViewStatus topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2220 **Topology error changing segment label, rc = <TopoReturnCode>, resource = <SegmentName>**

Meaning: An error occurred on changeResourceLabel topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2221 **Topology error changing segment extension, rc = <TopoReturnCode>, resource = <SegmentName>**

Meaning: An error occurred on changeResourceExtension topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2222 **Topology error creating segment, rc = <TopoReturnCode>, resource = <SegmentName>**

Meaning: An error occurred on createView topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2223 **Topology error building segment, rc = <TopoReturnCode>, resource = <SegmentName>**

Meaning: An error occurred on viewBuilt topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2224 Topology error deleting segment, rc = <TopoReturnCode>, resource = <SegmentName>

Meaning: An error occurred on deleteView topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2225 Topology error deleting Surrogate segments, rc = <TopoReturnCode>

Meaning: An error occurred on topoDeleteProtocol topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2226 Topology error deleting RMON segments, rc = <TopoReturnCode>

Meaning: An error occurred on topoDeleteProtocol topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2227 Topology error deleting SNMP 8230 segments, rc = <TopoReturnCode>

Meaning: An error occurred on topoDeleteProtocol topology call.

Action: Take the following action depending on the <TopoReturnCode>:

-1 - Restart LNM for AIX.

-2 - Contact IBM Service for more information.

-3 - Contact IBM Service for more information.

-4 - Contact IBM Service for more information.

-5 - Restart LNM for AIX.

-6 - Contact IBM Service for more information.

If the problem persists, contact IBM Service for more information.

2228 Database internal error

Meaning: An error occurred on access of DBM. An open/read/write in the /usr/CML/databases/lnmTrsnmpData files failed.

Action: Check the nettl log and correct any problems found. Then, restart LNM for AIX. If the problem is not solved, delete the /usr/CML/databases/lnmTrsnmpData.* files.**Attention:** If you delete these files you will lose such information as labels, access control policy, resource monitoring definitions, and location definitions for the SNMP token-ring segments.

If the problem persists, contact IBM Service for more information.

2237 Database initialization error, rc = <DBMreturnCode>

Meaning: An error occurred on dbm_open call for one of the following reasons:

- -1 - Duplicate record
- -2 - Non-existent record
- -3 - Invalid record
- -4 - Invalid key

- -5 - Fetch failed

Action: Check the nettl log and correct any problems found. Then, restart LNM for AIX. If the problem is not solved, delete the /usr/CML/databases/lnmTrsnmpData.* files.

Warning: If you delete these files you will lose such information as labels, access control policy, resource monitoring definitions, and location definitions for the SNMP token-ring segments.

If the problem persists, record the <DBMreturnCode> and contact IBM Service for more information.

2254 Unsuccessful trap session open

Meaning: An error occurred when trying to open an snmp trap session. The application will retry to open the session.

Action: Verify the SNMP configuration file (community name, etc.)

2255 Trap received for a non-managed station, MAC = <Mac Address>

Meaning: The crsNaunChange trap was received but the related station (Mac Address) is not being managed.

Action: Manually resynchronize to update the AIX NetView/6000 submap. Verify that the MAC is present in the network.

2257 Oid undefined for this application, oid = <oid>

Meaning: The AGENT_FOUND message was received from cmld but the OID is not valid for this application. The message will be ignored.

Action: The cmld.conf file may be corrupted. Try to restore it by using `smit cml .. Configure .. LNM for AIX general configuration .. Applications to be started when LNM for AIX starts`. Then set SNMP Token-Ring to **No**, click on **Do**, set it back to **Yes** and click on **Do** again.

Then the cmld.conf file should be restored. Execute ovstop and then ovstart to restart cmld. Then restart LNM for AIX. If the problem persists, contact IBM Service for more information.

2258 SNMP get failed due timeout, IP = <Ip Address>

Meaning: A timeout PDU was received.

Action: Verify that the agent on which the problem occurred is running. If the agent is already running, increase the timeout value for the SNMP configuration using the SNMP configuration option in NetView for AIX menu bar.

2260 SNMP set error, Segment access control could not be done, segment = <SegmentName>

Meaning: An SNMP error occurred when trying to issue the remove command for a controlled station.

Action: Verify that the agent on which the problem occurred is running. If the agent is already running, use the SNMP configuration option in NetView for AIX menu bar and verify that you have set the correct community name to have write access permission. If the problem persists, contact IBM Service for more information.

2261 Surrogate station attachment error, status = <attachStatus>, MAC = <Mac Address>

Meaning: The rpsLastAttachedReportStationInRing trap was received. The status of the attachment process indicates an error. The station was not inserted in the ring.

Action: Verify that this MAC was correctly inserted in the network.

2262 The station should have been already created at this time, MAC = <Mac Address>

Meaning: An error occurred when processing a surrogate trap. A station should have been already created when an SNMP GET response is received from the surrogate.

Action: This is an unexpected condition. Resynchronizing the segment will update AIX NetView/6000. Verify that this MAC was correctly inserted in the network.

2263 REM and/or CRS functions not available for segment <SegmentName>.

Meaning: Informative.

Action: Verify whether the agent provides REM and CRS functions. Also, verify whether these functions are enabled by using the segment configuration window.

2267 SNMP GET/SET error, rc = <SNMP ErrorCode>, Segment = <segmentName>

Meaning: A GET/SET response was received with error for one the following reasons:

1 - Too big

2 - No such name

3 - Bad value

4 - Read only

5 - Generic

Action: Verify that the agent on which the problem occurred is running. If the agent is already running, use the SNMP configuration option in NetView for AIX menu bar, and verify if you have set the correct community name to have write access permission. If the problem persists, contact IBM Service for more information.

2268 SNMP get/set/get_next failed due timeout, Segment = <Segment Name>

Meaning: A timeout PDU was received.

Action: Verify that the agent on which the problem occurred is running. If the agent is already running, increase the timeout value for the SNMP configuration using the SNMP configuration option in NetView for AIX menu bar.

2269 Error sending snmp GET/SET, Segment = <Segment Name>

Meaning: A SNMP get or set request could not be sent

Action: Verify that the agent on which the problem occurred is running. If the agent is already running, try to ping it. If you can ping the agent and the problem persists, contact IBM Service for more information.

2270 Management application connection error

Meaning: The application cannot communicate with lnmtrmgr.

Action: Verify that lnmtrmgr is running. If it is not running, access any SNMP token-ring window and lnmtrmgr will be started. If it is running and the problem persists, contact IBM Service for more information.

2275 Application ended with error, rc = <ErrorCode>

Meaning: lnmtrmon process exits for one of the following reasons:

0 - Normal termination

1 - Memory fault

5 - cmld connection error

6 - Program error

17 - Terminated after receiving SIGTERM signal

19 - lnmtopod connection error

20 - Internal database initialization error

21 - Clear internal database error

22 - Terminated after receiving SIGDANGER signal

Action: This message can be used in conjunction with the response from cmlstatus to understand why lnmtrmon is no longer running. See the man page for cmlstatus for an explanation of the exit codes. If this message is not written in the log, lnmtrmon was terminated using SIGKILL or terminated abnormally. If lnmtrmon terminated abnormally, a core dump will probably be found in the root directory. You can determine the executable that generated a core dump by entering the following command while you are in the directory with the core image.

```
od -c core 0x4850 | head
```

Record the information from executing dbx with the *where* subcommand or *t* subcommand and contact IBM Service for more information.

2276 Application stopped due to cmld connection error

Meaning: There was a communication problem with cmld.

Action: Check the nettl log and correct any problems found. Then, restart LNM for AIX.

2277 Application stopped due to Topology connection error

Meaning: There was a communication problem with lnmtopod.

Action: Check the nettl log and correct any problems found. Then, restart LNM for AIX.

2278 Application stopped due to database initialization error.

Meaning: There was a problem during internal database initialization.

Action: Check the nettl log and correct any problems found. Then, restart LNM for AIX. If the problem is not solved, delete the /usr/CML/databases/lnmTrsnmpData.* files.

Warning: If you delete these files you will lose such information as labels, access control policy, resource monitoring definitions, and location definitions for the SNMP token-ring segments.

If the problem persists, contact IBM Service for more information.

2279 Application stopped due to database record deletion error.

Meaning: There was a problem during internal database operation.

Action: Check the nettl log and correct any problems found. Then, restart LNM for AIX. If the problem is not solved, delete the /usr/CML/databases/lnmTrsnmpData.* files.

Warning: If you delete these files you will lose such information as labels, access control policy, resource monitoring definitions, and location definitions for the SNMP token-ring segments.

If the problem persists, contact IBM Service for more information.

2281 Authentication failure, IP = <IP address>

Meaning: An SNMP generic trap 4 was received.

Action: Verify that the community names match.

2302 Connection with discovery not established.

Meaning: lnmtrmgr has an interface with lnmtrmon process, and setting some attributes requires that this interface is up.

Action: Restart LNM for AIX.

2303 OVW not running.

Meaning: If lnmtrmgr is started when NetView for AIX is not running this message is logged.

Action: Start NetView for AIX.

2308 Cannot match attribute <PDF attribute name> with an oid from MIB table.

Meaning: The Token Ring management application failed on trying to get an attribute from the MIB table.

Action: Verify if the directory /usr/CML/databases contains the following files with read permission:

- lnmTrClamMib.tbl
- lnmTrRmonMib.tbl
- lnmTrSurrMib.tbl

If the problem persists, contact IBM Service for more information.

2313 Cannot remove station. SNMP set operation failed.

Meaning: When the user tried to remove a station from a Ring with the Station Profile/Configuration window, a set operation error occurred.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing set requests to the agent on which the problem occurred. This problem generally happens when a community name does not have write permission, which is required for a set operation. Use the SNMP configuration option in NetView for AIX menu bar, and verify that you have set the correct community name to have write access permission. If the problem persists, contact IBM Service for more information.

2324 Unable to initialize SNMP session for resource <resource name>.

Meaning: The open function failed for the SNMP specific agent whose OID is included in the resource name.

Action: Verify that the SNMP agent is up using the MIB browser. Check the SNMP configuration option using the NetView for AIX menu bar. Retry the operation. If the problem persists, contact IBM Service for more information.

2325 Cannot open MIB table <MIB table name>.

Meaning: Token Ring Management Application failed on trying to open one of the MIB tables.

Action: Verify if the directory /usr/CML/databases contains the following files with read permission:

- lnmTrClamMib.tbl
- lnmTrRmonMib.tbl
- lnmTrSurrMib.tbl

If the problem persists, contact IBM Service for more information.

2326 Cannot find label in OVw DB.

Meaning: The Token Ring management application failed on getting the label from NetView for AIX.

Action: Exit from the AIX NetView/6000 graphical interface. Stop LNM for AIX. Clear the LNM databases using `SMIT .. LNM for AIX .. Maintain .. Clear LNM for AIX databases`. Restart LNM for AIX and AIX NetView/6000. If the problem persists, contact IBM Service for more information.

2327 There is no symbol associated to objectID: <OID>.

Meaning: The Token Ring management application failed on getting the symbol associated with the object described in the message field.

Action: Exit from the AIX NetView/6000 graphical interface. Stop LNM for AIX. Clear the LNM databases using `SMIT .. LNM for AIX .. Maintain .. Clear LNM for AIX databases`. Restart LNM for AIX and AIX NetView/6000. If the problem persists, contact IBM Service for more information.

2328 OVw map not opened.

Meaning: The Token Ring management application failed on getting the submapID associated with the object selected.

Action: Exit from the AIX NetView/6000 graphical interface. Stop LNM for AIX. Clear the LNM databases using `SMIT .. LNM for AIX .. Maintain .. Clear LNM for AIX databases`. Restart LNM for AIX and AIX NetView/6000. If the problem persists, contact IBM Service for more information.

2332 Error while deleting panel <Panel Name>.

Meaning: An internal error occurred when the Token Ring management application was deleting an open window.

Action: Stop LNM for AIX and restart it. If the problem persist, contact IBM Service for more information.

2333 Cannot get resource label from OVw, for <Resource Label>.

Meaning: The Token Ring management application failed on getting the label from NetView for AIX for the specific resource.

Action: Exit from the AIX NetView/6000 graphical interface. Stop LNM for AIX. Clear the LNM databases using `SMIT .. LNM for AIX .. Maintain .. Clear LNM for AIX databases`. Restart LNM for AIX and AIX NetView/6000. If the problem persists, contact IBM Service for more information.

2334 Memory fault error.

Meaning: A memory fault has occurred. This usually indicates a shortage of resources in the RS/6000 workstation.

Action: Shut down some of the applications. Restart LNM for AIX and monitor the memory usage.

You may need more memory for this workstation. If the problem persists, contact IBM Service for more information.

2335 Termination signal received.

Meaning: The lnmtrmgr process received an unexpected termination signal from operating system.

Action: If kill -15 was used, this is informative only. Otherwise, check the log to verify why the termination signal was sent. If the problem persists, contact IBM Service for more information.

2336 Database internal error. rc=<DB internal error code>.

Meaning: An error occurred when the lnmtrmgr process tried to access the internal database.

Action: Check the nettl log and correct any problems found. Then, restart LNM for AIX. If the problem is not solved, delete the /usr/CML/databases/lnmTrsnmpData.* files.

Warning: If you delete these files you will lose such information as labels, access control policy, resource monitoring definitions, and location definitions for the SNMP token-ring segments.

If the problem persists, contact IBM Service for more information.

2337 Cannot resynchronize segment. Connection with discovery not established. Restart LNM for AIX.

Meaning: A connection to lnmtrmon is required to resynchronize segments.

Action: Restart LNM for AIX.

2338 Discovery application connection error. Socket info lost.

Meaning: lnmtrmgr process tried to connect with lnmtrmon and some socket information was lost.

Action: Use cmlstop to stop LNM for AIX and restart it using cmlstart. If the problem persists, contact IBM Service for more information.

2339 Cannot update RMON Configuration Table. Some variables will not be available.

Meaning: lnmtrmgr process failed on trying to set the RMON MIB. To set some variables in the RMON Configuration Table, you must first set the variable ringStationConfigUpdateStats.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing set requests to the agent on which the problem occurred. This problem generally happens when a community name does not have write permission, which is required for a set operation. Use the SNMP configuration option in NetView for AIX menu bar, and verify that you have set the correct community name to have write access permission. If the problem persists, contact IBM Service for more information.

2340 Get Isolating Table Error.

Meaning: lnmtrmgr process failed on trying to get information from Isolating Table.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing get requests to the agent on which the problem occurred. This problem generally happens when a community name does not have read permission which it must have for a get operation. If the problem persists, contact IBM Service for more information.

2343 Cannot access internal DB.

Meaning: An error occurred when the lnmtrmgr process tried to access the internal database.

Action: Use cmlstop to stop LNM for AIX and restart it using cmlstart. Ensure that lnmtrmon application is up and running. If the problem persists, contact IBM Service for more information.

2344 SNMP get operation error.

Meaning: The lnmtrmgr process failed on getting a variable from the agent in which the problem occurred.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing get requests to the agent on which the problem occurred. This problem generally happens when a community name does not have read permission, which is required for a get operation. If the problem persists, contact IBM Service for more information.

2345 SNMP get operation suspected.

Meaning: This error occurs when there was already an error getting a PDU variable. This indicates that the validity of remaining PDU variables cannot be assured. This messages is always displayed in conjunction with message number 2344.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing get requests on the agent that the problem occurred. This problem generally happens when a community name does not have read permission, which is required for a get operation. If the problem persists, contact IBM Service for more information.

2346 SNMP get operation error - Agent timeout.

Meaning: The lnmtrmgr process failed to get a variable from the agent due to an agent time-out.

Action: Verify that the agent on which the problem occurred is running. If the agent is already running, increase the time-out value for the SNMP configuration using the SNMP Configuration option in the NetView for AIX menu bar.

The SNMP Token-Ring application of AIX requires that you do one of the following:

Stop and restart the SNMP Token-Ring daemon

Delete the agent, then reconfigure and rediscover it using SMIT.

Execute `cml_agent_remove` followed by `cml_agent_found` from the command line.

2347 SNMP set operation error.

Meaning: The lnmtrmgr process failed to set a variable on the agent on which the problem occurred.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing set requests to the agent on which the problem occurred. This problem generally happens when a community name does not have write permission, which is required for a set operation. Use the SNMP configuration option in NetView for AIX menu bar, and verify that you have set the correct community name to have write access permission. If the problem persists, contact IBM Service for more information.

2348 SNMP set operation suspected.

Meaning: This error occurs when there was already an error on setting a PDU variable. This indicates that the validity of remaining PDU variables cannot be assured. This messages is always displayed in conjunction with message number 2347.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing set requests on the agent that the problem occurred. This problem generally happens when a community name does not have a write permission, which is required for a set operation. Use the SNMP configuration option in NetView for AIX menu bar, and verify that you have set the correct community name to have write access permission. If the problem persists, contact IBM Service for more information.

2349 SNMP set operation error - Agent timeout.

Meaning: The lnmtrmgr process failed to set a variable on the agent due to time-out.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing set requests to the agent on which the problem occurred. This problem generally happens when a community name does not have write permission, which is required for a set operation. Use the SNMP configuration option in NetView for AIX menu bar, and verify that you have set the correct community name to have write access permission. Also, increase the time-out value.

The SNMP Token-Ring application of AIX requires that you do one of the following:

Stop and restart the SNMP Token-Ring daemon

Delete the agent, then reconfigure and rediscover it using SMIT.

Execute `cml_agent_remove` followed by `cml_agent_found` from the command line.

If the problem persists, contact IBM Service for more information.

2350 Cannot get resource label from OVw DB.

Meaning: The Token Ring management application failed to get the label from NetView for AIX.

Action: Exit from the AIX NetView/6000 graphical interface. Stop LNM for AIX. Clear the LNM databases using `SMIT .. LNM for AIX .. Maintain .. Clear LNM for AIX databases`. Restart LNM for AIX and AIX NetView/6000. If the problem persists, contact IBM Service for more information.

2352 Connection with discovery not established.

Meaning: The lnmtrmgr process has an interface with lnmtrmon process, and setting attributes requires that this interface be up.

Action: Restart LNM for AIX.

2353 Cannot resynchronize all segments. Connection with discovery not established. Restart LNM for AIX.

Meaning: This message occurs when lnmtrmgr process tries to resynchronize all segments that are

managed by the lnmtrmon. lnmtrmon must be running.

Action: Restart LNM for AIX.

2354 **Resync segment <segment name> failed.**

Meaning: This message occurs when the lmntrmon application fails when trying to resynchronize a segment that it is managing.

Action: None.

2355 **Resync segment <segment name> has completed successfully.**

Meaning: This message occurs when lnmtrmon finishes resynchronizing a segment.

Action: None.

2356 **Segment <segment name> not managed.**

Meaning: This message occurs when lnmtrmon cannot resynchronize a segment because it is not managing it.

Action: None.

2357 **Resync all failed for at least one of the segments.**

Meaning: This message occurs when lnmtrmon fails to resynchronize all the segments it is managing but was able to resynchronize one or more segments successfully.

Action: None.

2358 **Resync all segments has completed successfully.**

Meaning: This message occurs when lnmtrmon finishes resynchronizing all the segments that it is managing.

Action: None.

2359 **Resync all segments already running.**

Meaning: This message occurs when the user requests a resynchronization but one is already in progress.

Action: None.

2364 **Cannot update database record in dbSet call, rc=<internal database error code>.**

Meaning: An error occurred when the lnmtrmgr process tried to update a field in internal database.

Action: Use cmlstop to stop LNM for AIX and restart them using cmlstart. Ensure that the lnmtrmon application is up and running. If the problem persists, contact IBM Service for more information.

2366 **Access control policies for Token-Ring segments managed through RMON agents will be implemented only during resynchronization. Segments managed through Surrogate and SNMP 8230 agents take effect continuously.**

Meaning: This is an informative message that pertains only to RMON segments. The message is displayed when any change is made in access control.

Action: None.

2373 **Session opened.**

Meaning: An SNMP session was successfully opened.

Action: None.

2374 **Unable to initialize SNMP session**

Meaning: The application has tried to open an SNMP session but was unsuccessful. The CAU MIB variables were not read, and the SNMP Concentrator graphical view will not display until the application can successfully initialize the session.

Action: None. The application will retry to initialize the session.

2376 **MIB elements reading error.**

Meaning: A get request for the static CAU MIB variables returned an error. A message dialog box is displayed to notify the user that the connection with the agent could not be established.

Action: Verify that the SNMP agent is up by using the MIB Browser and issuing get requests to the agent on which the problem occurred. This problem generally happens when a community name does not have read permission, which is required for a get operation. Restart

the agent if necessary. If the problem persists, contact IBM Service for more information.

2386 **The variable cauNumberOfLobes is not consistent with the number of lobes returned from the lobe table.**

Meaning: An inconsistency was detected while getting the cauLobe table variables: for at least one module, the number of entries in the cauLobe table does not match the value of the variable cauNumberOfLobes.

Action: Consult the agent documentation for how to resolve this. *xnmbrowser* may be useful in determining in which module(s) the error occurred.

2387 **Error while getting static variables from the MIB.**

Meaning: A concentrator agent communication problem (time-out) occurred while getting static variables from cau group, cauBeacon group, or MIB-II.

Action: Verify that the SNMP agent is up by pinging the SNMP 8230 concentrator. If the agent is already running, increase the time-out value for the SNMP configuration using the SNMP configuration option in NetView for AIX menu bar. Restart the agent if necessary.

The SNMP Token-Ring application of AIX requires that you do one of the following:

Stop and restart the SNMP Token-Ring daemon

Delete the agent, then reconfigure and rediscover it using SMIT.

Execute `cml_agent_remove` followed by `cml_agent_found` from the command line.

If the problem persists, contact IBM Service for more information.

2388 **Error while getting tables from the MIB.**

Meaning: A concentrator agent communication problem (time-out) occurred while getting variables from cauModule table or cauLobe table.

Action: Verify that the SNMP agent is up by pinging the SNMP 8230 concentrator. If the agent is already running, increase the time-out value for the SNMP configuration using the SNMP configuration option in NetView for AIX menu bar. Restart the agent if necessary.

The SNMP Token-Ring application of AIX requires that you do one of the following:

Stop and restart the SNMP Token-Ring daemon

Delete the agent, then reconfigure and rediscover it using SMIT.

Execute `cml_agent_remove` followed by `cml_agent_found` from the command line.

If the problem persists, contact IBM Service for more information.

2502 **Socket connection from <process1> to <process2> failed. process1 <lnmhubint> process2 <Process name> errno = <errnoValue> File = <File Name> Line = <Line Number>**

Meaning: The Hub Manager integration daemon (lnmhubint) lost the socket connection to another process. This message usually indicates that the other process failed and lnmhubint will terminate as a result. The error indicates the error number and the File and Line number indicates the location where the error occurred.

Action: The following list describes the processes that lnmhubint communicates with and the actions that should be taken in order to recover.

- iubd

  The iubd daemon is the daemon used by Hub Manager. If you want LNM for AIX to be integrated with Hub Manager, restart the lnmhubint daemon and then demand poll the hub.

- cmld

  The lnmhubint daemon has lost its connection to the main LNM for AIX process. Exit the NetView for AIX graphical interface and then execute ovstop. Use ovstatus and cmlstatus to verify that all of the NetView for AIX and LAN Network Manager daemons are stopped. Restart NetView for AIX and LAN Network Manager.

  If you want LAN Network Manager to be integrated with Hub Manager, start the iubd daemon. If the iubd daemon is already running, restart coupling with LAN Network Manager using the Hub Manager SMIT Control menu.

- lnmtopod

  The lnmhubint daemon has lost its connection with Topology Services. Restart LAN Network Manager to restart Topology Services.

If the actions recommended above do not solve the problem, check the nettl log for other error messages that may be causing the problem. Contact IBM Service if more information is needed.

2503 lnmhubint exiting Exit code = <errnoValue> File = <File Name> Line = <Line Number>

Meaning: lnmhubint is terminating for one of the following reasons:

0 - Normal termination

1 - Memory fault

2 - Socket connection error

3 - Socket information lost

6 - Program error

17 - Terminated after receiving SIGTERM signal

18 - Terminated from main

22 - Terminated after receiving SIGDANGER signal

Action: This message can be used in conjunction with the response from cmlstatus to understand why lnmhubint is no longer running. See the man page for cmlstatus for an explanation of the exit codes. If lnmhubint terminated abnormally, a core dump will probably be found in the root directory. You can determine the executable that generated a core dump by entering the following command while you are in the directory with the core image

```
od -c core 0x4850 | head
```

Record the information from executing dbx with the *where* subcommand or the *t* subcommand. Contact IBM Service for more information.

2504 Unexpected value in switch statement. Procedure <methodName> Switch value<value> File<File Name> Line<Line Number>

Meaning: This message is used for any unexpected values. The Procedure will identify the type of error. The Exit code indicates the error number and the File and Line number indicates the location where the error occurred.

Action:

- LNMConcServer::readyForReading

  The hub integration code received an unexpected message from Hub Manager. The message will be ignored. Issue a **kill -30 xxxxx** command to turn on tracing for the lnmhubint process. This will produce a log of all messages received from the Hub Management application so that the error can be isolated to either Hub Manager or the LNM of AIX hub integration code. Contact IBM Service if more information is needed.

- LnmCpClient::readyForReading

  The hub integration code received an unexpected message from the LNM for AIX control program. This is a programming error. The message will be ignored. Contact IBM Service for more information.

- Utility::checkTopoReturnCode

  Hub integration was attempting to recover from a topology error and received an invalid return code. The lnmhubint daemon will terminate due to the topology error. Check the nettl log for topology errors and restart LAN Network Manager.

2505 Duplicate start message received. File = <File Name> Line = <Line Number>

Meaning: The lnmhubint received a second start message from the LNM for AIX control program. The duplicate message will be ignored.

Action: None.

Part 9. Joining LAN and ATM

Chapter 45. Coupling and Navigating Between Campus Managers - LAN and ATM

Nways Manager-LAN and Nways Manager-ATM can be coupled to provide full management of ATM modules in 8260 hubs and 8265 ATM switches. Coupling involves integrating the topologies and device status used by each product.

Nways Manager-LAN and Nways Manager-ATM can be coupled in the following ways:

- 8250, 8260, and 8265 Device Manager can be coupled with Nways Manager-ATM.
- LAN Network Manager can be coupled with LAN Emulation Manager.

Coupling 8250, 8260, and 8265 Device Manager and Nways Manager-ATM

Starting Coupling

The coupling between the 8250, 8260, and 8265 Device Manager application in Nways Manager-LAN and Nways Manager-ATM is started automatically when you start Nways Manager-LAN.

To change this default setting using SMIT, follow these steps:

1. From NetView for AIX, select **Administer -> Campus Manager SMIT -> Control -> Coupling with Nways Manager-ATM**.
2. Click on the List button and select one of the values displayed:
   - Start (default)
   - Re-Sync
   - No
   - Status

For more information on configuring Nways Manager-ATM, refer to the online documentation, *Nways Manager-ATM for AIX User's Guide*.

Stopping Coupling

To stop the coupling between 8250, 8260, and 8265 Device Manager and Nways Manager-ATM, follow these steps:

1. From NetView for AIX, select **Administer -> Campus Manager SMIT -> Control -> Coupling with Nways Manager-ATM**.
2. Set the value for Nways Manager-ATM Coupling to **No**.

This stops the integration of the two topologies and removes the Nways Manager-ATM options from the menus displayed for the ATM and Switch modules in graphical views of 8260 hubs and 8265 ATM switches.

Resynchronizing Coupling

If ATM and Switch modules remain blue in Hub Level views, you may need to resynchronize the coupling between 8250, 8260, and 8265 Device Manager and Nways Manager-ATM. This can occur if many changes are made to the network since the two topologies were coupled.

To resynchronize the two topologies:

1. From NetView for AIX, select **Administer -> Campus Manager SMIT -> Control -> Coupling with Nways Manager-ATM**.
2. Set the value for Nways Manager-ATM Coupling to **Re-sync**.

Displaying Coupling Status

To display the current status of the coupling between 8250, 8260, and 8265 Device Manager and Nways Manager-ATM, select **Administer -> HubManager -> Administration** and do one of the following:

- Select **Control -> Coupling with Nways Manager-ATM** and set the value for Nways Manager-ATM Coupling to **Status**.
- Select **Administer -> Campus Manager SMIT** and set the value for Nways Manager-ATM Coupling to**Status**. .

Port Status

Table 36 shows how the status of LAN ports displayed on the Port Configuration panel corresponds to the operational state of ATM interfaces displayed in the ATM Interface Configuration panel in Nways Manager-ATM.

Table 36. Status of LAN Ports and Operational State of ATM Interfaces

Status of LAN Ports (Nways Manager-LAN)	Operational State of ATM Interfaces (Nways Manager-ATM)
unknownStatus	unknown
off	disabled-nosignal
off	disabled-idle
noPhantom	nosignal
noPhantom	idle
fatalError	idle
okay	in-service
okay	pvcOnly
fatalError	failing
fatalError	misConfigured
fatalError	wrong-network-prefix
fatalError	wrong-node-number

Module Status

The color-coded status of module icons in Hub Level views is an aggregate of the status of the module and the status of ports on the module. Because the status of modules is always reported as *unknown*, the color of the module icon is an aggregate of the status of its ports.

Coupling LAN Network Manager with LAN Emulation Manager

When you install both LAN Network Manager and LAN Emulation Manager, the two applications are automatically coupled. This coupling allows realtime, color-coded status of ATM/LAN bridges and switches to be displayed in LAN Subnet submaps.

ATM Management

In standalone mode, Nways Manager-LAN provides a subset of the management functions for ATM modules (Switch and media) installed in an 8260 Hub or 8265 ATM switch.

The coupling of Nways Manager-LAN and Nways Manager-ATM provides comprehensive management of hubs, legacy LANs, and ATM networks that allows you to:

- Start Nways Manager-LAN from Nways Manager-ATM by selecting an 8260 or 8265 icon.
- Display graphical color-coded information in Module Level views in Nways Manager-LAN about the status of ATM devices based on information received from Nways Manager-ATM.

Navigating Between Campus Managers - LAN and ATM

To navigate between Nways Manager-LAN views and Nways Manager-ATM submaps, do one of the following:

- From a Hub Level view, double-click on the icon of an ATM Switch or media module.
- From a Module Level view, double-click on an ATM device or select **Explode** from the context menu of an ATM device.

To navigate between Nways Manager-ATM submaps and Nways Manager-LAN views, do one of the following:

- From an ATM Cluster submap, select **CMA -> Device** from the context menu of an ATM Switch or device or select an ATM Switch (or device) and then select **CMA -> Device** from the menu bar.
- From an ATM Node submap, select **Device** from the context menu of an ATM Switch or device.
- From the ATM Switch Configuration panel, select **Navigation -> Device** from the menu bar.

Navigating with LAN Emulation Manager

LAN Emulation Manager is an application running under Nways Manager-ATM that allows you to emulate and manage the services of existing LANs across an ATM network. You can navigate from Nways Manager-LAN to LAN Emulation Manager in the following ways:

- From a Segment submap of LAN Network Manager that displays an emulated LAN segment:
  - Double-click on the icon of the emulated LAN.
  - Select **CMA -> LAN Emulation** from its context menu.
- From a Bridge submap of LAN Network Manager that displays an ATM device connected to an emulated LAN:
  - Double-click on the icon of the emulated LAN device.
  - Select **CMA -> LAN Emulation** from its context menu.
- From a Hub Level view that displays an ATM LAN Bridge module:
  1. Double-click on the icon of the ATM LAN Bridge module or select **CMA -> LAN Emulation** from the context menu of the module. The Bridge submap is displayed.
  2. Double-click on the icon of the emulated LAN device or select **CMA -> LAN Emulation** from its context menu.
- From a Module Level view that displays an emulated LAN device:
  - Double-click on the icon of the emulated LAN device.
  - Select **CMA -> LAN Emulation** from its context menu.

From LAN Emulation Manager, you can navigate to Nways Manager-LAN by opening:

- A Segment submap (called an *LNM View*) in LAN Network Manager with an emulated LAN device
- A Hub Level view (called a *Device View*) in 8250, 8260, and 8265 Device Manager with an ATM LAN Bridge module.

To do so, start from the LAN Emulation or the Control View panel. If you start from the LAN Emulation panel, follow these steps:

1. Double-click on the Domain icon of an emulated LAN. (A *domain* is a set of LAN emulation resources that are controlled by one LECS, LAN Emulation Configuration Server.) The Exploded Domain panel is displayed.
2. Do one of the following:
   - Select a LECS icon. Then select **Open View -> LNM View** or **Open View -> Device View** from its context menu.
   - Select a LECS icon. Then click on the **Open LNM View** or the **Open Device View** pushbutton in the tool bar.
   - Select an ELAN icon. Then click on the **Open LNM View** or the **Open Device View** pushbutton in the tool bar or select **Open View -> LNM View** or **Open View -> Device View** from its context menu.

If you start from the Control View panel, follow these steps:

1. Select one of the following emulated LAN resources:
   - ATM LAN Bridge module
   - 8281 ATM LAN bridge
   - 8210 MSS server
   - 8260 MSS module
2. Display the context menu of the resource and select **Open View -> LNM View** or **Open View -> Device View**.

A Hub Level view or a Segment submap is displayed and the selected resource is highlighted.

For information on how to use LAN Emulation Manager, see the book**Coupling with and Using Related Applications** in the online documentation set for Nways Manager-ATM.

Switching Between IP, ATM, and LAN Protocol Views

When using the IBM Nways Manager for AIX of products, you can display the protocols running in a network resource and switch between different views and submaps in which the resource icon is displayed. For example, you can select a hub from the IBM Hubs Topology and switch to the location of the hub in an IP submap.

To switch between different protocol views of a network resource, follow these steps:

1. Select the resource in the IP Internet window or in a submap of Nways Manager-LAN or Nways Manager-ATM.
2. Do one of the following:
   - From the menu bar, select **View -> -> Nways -> Nways Protocols**.
   - From the context menu of the resource, select **Nways Protocols**.

   A dialog box for switching protocol views is displayed. All protocols running in the resource and the submaps that correspond to each protocol are listed.
3. Click on the protocol and the submap which you want to display.
4. Click on **Open** to display the selected submap.

Chapter 46. Discovering Your Network

This section describes the autodiscovery feature of Nways Manager-LAN and the different components for monitoring and receiving information from your LAN Campus network. Each component allows Nways Manager-LAN to communicate with agent programs in network devices to gather configuration, fault, and performance data.

The devices that can be discovered are:

- 2210 Multiprotocol routers
- 2216 Multiaccess connectors
- 6611 Network processors
- 8224, 8230, 8237, and 8238 LAN hubs
- 8225 Fast Ethernet Stackable hubs
- 8229 Token-Ring bridges
- 8235 DIALs Remote Access servers
- 8244 FDDI Workgroup concentrators
- 8250 and 8260 Multiprotocol hubs
- 8265 ATM switches
- 8270-800, 8271 Ethernet, and 8272 Token-Ring LAN switches
- 8273 Ethernet and 8274 LAN RouteSwitches
- 8276 Ethernet RoutePorts
- 8281 ATM/LAN bridges
- SNMP bridges and routers
- Agents that manage LAN segments, such as Token Ring surrogate, LNM OS/2 proxy, RMON , IBM FDDI proxy, 8230-3, and so on.

Agents Discovered by Installed Components

Nways Manager-LAN discovers different network devices according to the components you install and have running, and the agents installed in each device.

Table 37 on page 436 lists the different Nways Manager-LAN components with:

- The daemon used by each component
- The agents discovered by each component

A Nways Manager-LAN component is*installed* or *not installed* depending on the SMIT options you selected when installing the product.

When you enter `ovstart cmld` to start Nways Manager-LAN for AIX, each installed component is started by default.

- To stop the component and change its status from *started* to *not running*, enter the command: `cmlstop daemon` (where `daemon` is the name of the daemon used by the component as shown in Table 37)
- To restart the component, enter the command: `cmlstart daemon`
- To change the default setting, do one of the following:
  - From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Configure -> Nways Campus Manager general configuration -> Capabilities to be started when Campus Manager starts**.
  - From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Capabilities to be started when Campus Manager starts**.
- In the dialog box displayed, select **Yes** for the capabilities that you want to automatically start when the **cmld** daemon is started.

Table 37. Nways Manager-LAN for AIX Components: Daemons Used and Agents Discovered

Component	Daemon Used	Agents Discovered
LAN Network Manager (LNM OS/2 Agent application)	lnmlnmemon	LNM OS/2 proxy agent
LAN Network Manager (SNMP Token-Ring application)	lnmtrmon	• IBM 8230 agent • Token-ring surrogate agent • RMON agent that supports RFC 1513
LAN Network Manager (SNMP Bridge application)	lnmbrmon	• 2210, 2216, 6611, 8210, 8270-800, 8271, 8272, 8281, and OEM • RFC 1213, RFC 1286, and RFC 1493 • 8229 bridges and 8250 integrated bridges that support RFC 1213, RFC 1286, and RFC 1493
LAN Network Manager (FDDI application)	lnmfddimon	FDDI proxy agent
8250, 8260, and 8265 Device Manager	iubd	ADMM, AMM (CPSW with DMM subset),DMM, EMM, FMM, and TRMM
Product Specific Modules and Java web-managed applications	not applicable	2210, 2216, 6611, 8224, 8225, 8230, 8235, 8237, 8238, 8270, 8271, 8272, and 8281

Note: The Nways Switching Module Manager (NSMM) component of Nways Manager-LAN uses a different method to discover the virtual LANs (consisting of Ethernet and FDDI devices with an ATM uplink) that it manages. For information on how NSMM discovers devices, see the *IBM Nways Switching Modules Manager User's Guide* shipped with 8260 Switching Series modules.

Methods of Discovery

Information supplied by agents is discovered by Nways Manager-LAN components in the following ways:

- *Automatic* discovery of the NetView for AIX topology database and traps (*node added*, *node deleted*, and *sysobjectid changed*)
- *Persistent* discovery using SMIT and the *Known Agents file*, the dedicated configuration file used by all Nways Manager-LAN components.
- *Temporary* discovery by selecting menu options from the SMIT user interface.

The methods that each Nways Manager-LAN component uses to discover network devices are shown in Table 38.

Table 38. Nways Manager-LAN for AIX Components: Discovery Method Used

Component	Automatic Discovery (NetView for AIX)	Persistent Discovery (Known Agents File)	Temporary Discovery (Command Line Interface)
LAN Network Manager (LNM OS/2 Agent application)	—	X	X
LAN Network Manager (SNMP Token-Ring application)	X	X	X
LAN Network Manager (SNMP Bridge application)	X	X	X
LAN Network Manager (FDDI application)	X	X	X
8250, 8260, and 8265 Device Manager	X	—	—
Product Specific Modules and Java web-managed applications	X	—	—

For information on the methods of discovery used by the Router and Bridge Manager component, refer to the *IBM AIX Router and Bridge/6000: User's Guide* (SC31-6489).

Persistent Discovery Using the Known Agents File

The Known Agents file provides a method to persistently discover agents that are not automatically discovered by Nways Manager-LAN. This file is used by each component and contains:

- IP addresses (or host names) of the devices from which agents respond
- IDs of the agents supported by each device (optional)

Each record in the file appears as an IP address, optionally followed by a series of agent IDs in the format:

```
ip1 <id1 id2 id3 ...>
ip2 <id1 id2 id3 ...>
```

Each agent ID in a record appears in the format <sysObjectID>/<MIB variable> where:

- sysObjectID is the MIB II variable defined in the device.
- MIB variable is the MIB variable to be discovered.

An example of an agent ID appears in the Known Agents file is shown below:

```
1.3.6.1.4.1.49.2.3.5/1.3.6.1.2.1.17.1.1.0
```

Nways Manager-LAN uses the list of agent IDs to discover:

- Each agent, even when an agent does not respond
- LNM OS/2 agents

Defining an Alias for an Agent ID

To define an alias for an agent ID that you can use to modify the Known Agents file, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Configure -> Nways Campus Manager general configuration -> Define an agent ID**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Define an agent ID**.

In the dialog box displayed, enter the agent ID in the format <sysObjectID>/<MIB variable> as described in the preceding section. In the Agent Identifier field, enter the alias to be used instead of the agent ID. You can also enter a text description of the alias.

To remove an alias that you defined for an agent ID, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Configure -> Nways Campus Manager general configuration -> Undefine an agent ID**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Undefine an agent ID**.

Modifying the Known Agents File

To modify the Known Agents file, use the SMIT interface to add and remove IP addresses and agent IDs.

To add an IP address or an agent ID, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Configure -> Nways Campus Manager general configuration -> Add an IP address for forced discovery**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Add an IP address for forced discovery**.

In the dialog box displayed, enter the IP address or the host name of the device. Then enter the agent ID supported by the device. To display the list of existing agent IDs, click the List button.

To remove an IP address or an agent ID, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Configure -> Nways Campus Manager general configuration -> Remove an IP address for forced discovery**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Remove an IP address for forced discovery**.

Editing the Known Agents File

When you edit the Known Agents file, follow these conventions:

- The file name is `/usr/CML/data/cml.discovery.agents`
- Any line beginning with `#` is a line of comments and can be inserted anywhere in the file.
- Any line that is not a line of comments must contain either one IP address or hostname, optionally followed by a list of agent_ids, optionally followed by a `#` and comments
- All the agent_ids for a given IP address (if any exist) must be entered on the same line; duplicate IP address and hostname entries are not allowed.

Temporary Discovery

To *temporarily* modify the agents that are discovered (if the discovery process is running), use the SMIT interface to find and delete an SNMP agent. The changes you make are only valid during the current Nways Manager-LAN session. When you stop and restart Nways Manager-LAN, only the information supplied by *automatic* and *persistent* discovery is used.

To find an SNMP agent, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Find SNMP Agent**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Control -> Find SNMP Agent**.

To delete an SNMP agent, do one of the following:

- From SMIT, select **Communications Applications and Services -> Nways Campus Manager -> Control -> Delete SNMP Agent**.
- From the menu bar, select **Administer -> Campus Manager SMIT**. Then from the SMIT menu, select **Configure -> Nways Campus Manager general configuration -> Control -> Delete SNMP Agent**.

The Known Agents File is not changed.

Agents Filter File

The Agents Filter file allows you to determine what agents are discovered by Nways Manager-LAN components. To create or modify the file, you use a standard ASCII text editor.

The Agents Filter file contains the `ip_address_wildcard` field. This field limits agent discovery according to the range of IP addresses you specify. Enter parameters in the same format as in NetView for AIX.

You can filter the discovery of agents for:

- NetView for AIX (automatic discovery)
- Known Agents file (persistent discovery)

You cannot filter the discovery of agents when you use temporary discovery.

To determine if an agent is to be discovered, the discovery process checks the agents using information from:

1. NetView for AIX
2. Persistent discovery
3. Temporary discovery

Note that even if an agent is listed on more than one method to be discovered, Nways Manager-LAN only discovers and receives information from it once.

The conventions used for the Agents Filter file are as follows:

- The file name is: `/usr/CML/data/cml.discovery.filter`
- The format of the file is similiar to the NetView for AIX seed file.
- Any line beginning with `#` is a line of comments and can be inserted anywhere in the file.
- Any line that is not a line of comments can contain one IP address or hostname and is optionally followed by a `#` and comments
- Wildcards in IP addresses are allowed (for example, 9.*, 9.100.*, 9.100.*.*, 9.100.*.66, and so on).
- Ranges are specified using the `-` separator (for example, noumea.lagaude.ibm.com-9.100.*).

Part 10. Appendixes

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area.

References in this publication to IBM products, programs, and 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 that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

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

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

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

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

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

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Authorized Use of IBM Online Books

For online versions of this book, we authorize you to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine readable documentation.

Industry Standards Reflected in This Product

Nways Manager-LAN is designed according to the specifications of the following industry standards as understood and interpreted by IBM as of September 1994.

- RFC 854 - Telnet protocol
- RFC 1084 - BootP
- RFC 1350 - Trivial file transfer protocol (TFTP)
- SNMP:
  - RFC 1155 - Structure and Identification of Management Information (SMI) for TCP/IP based Internet.
  - RFC 1156 - Management Information Base (MIB) for Network Management of TCP/IP based Internets (MIB-I)
  - RFC 1157 - Simple Network Management Protocol (SNMP)
  - RFC 1212 - Concise MIB definitions
  - RFC 1213 - Management Information Base (MIB) for Network Management of TCP/IP based Internets (MIB-II)

  - RFC 1215 - Convention for defining Traps for use with SNMP.
- FDDI:
  - RFC 1285 - FDDI MIB updated by RFC1512
  - RFC 1512 - FDDI MIB
  - SMT 7.3
- Token-Ring:
  - RFC 1231 (1239) - IEEE 802.5 Token Ring MIB
- Bridges
  - RFC 1286 and RFC 1493 - Definitions of managed objects for bridges
- Ethernet
  - RFC 1398 (former RFC1284) - Definitions of managed objects for Ethernet-like interfaces
  - RFC 1516 - Repeater MIB
- RMON
  - RFC 1271 - Remote Network Monitoring MIB
  - RFC 1513 - Token Ring Remote Network Monitoring MIB

Trademarks

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

Nways	AIX
OS/2	EtherStreamer
NetView for AIX	APPN
Advanced Peer-to-Peer Networking	RS/6000
System /36	AS/400

NetView and TME 10 are trademarks of Tivoli Systems, Inc. in the United States, or other countries, or both.

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

Lotus and LotusNotes are trademarks of the Lotus Development Corporation in the United States, or other countries, or both.

List of Abbreviations

The following abbreviated terms refer to products in the IBM Nways Manager:

Hub Manager
8250, 8260, and 8265 Device Manager component of Nways Manager-LAN

LAN Network Manager (LNM)
LAN Network Manager component of Nways Manager-LAN

Router and Bridge Manager (RABM)
Router and Bridge Manager component of Nways Manager-LAN

The following abbreviations are used in this book:

AIX	Advanced Interactive Executive operating system
ASCII	American National Standard Code for Information Interchange
Async	Asynchronous
ATM	Asynchronous transfer mode
BNC	Bayonet node connector
BOOTP	Bootstrap protocol
CNM	Communication network management
CRC	Cyclic redundancy check
DMM	Distributed Management Module
E-MAC	Ethernet media access control
EMM	Ethernet management module
FDDI	Fiber distributed data interface
FMM	FDDI management module
FOIRL	Fiber optic interconnection repeater link
GTM	Generic topology manager
HE-MAC	High-end Ethernet media access control
H-TMAC	High-end token-ring media access control
IBM 8250	8250 Hub
IBM 8260	8260 Hub
ICMP	Internet control message protocol
ICS	IBM cabling system
IEEE	Institute of Electrical and Electronic Engineers (USA)

IP	Internetwork protocol (OSI)
ISO	International Organization for Standardization
kbps	kilo bits per second
LAN	Local area network
LCT	Live call transfer
LLC	Logical link control
MAC	Media access control
MAU	1) Multi-station access unit (Token Ring) 2) Medium attachment unit
Mbps	Mega bits per second
MIB	Management information base
MIC	Medium interface connector
NMC	Network monitor card
OSF	Open System Foundation
OSI	Open System Interconnection
OVw	OpenView windows
OVsnmp	OpenView SNMP
PBS	Per-bank switching
PC	Personal computer
PCM	Physical Connection Management
PCS	Per-connector switching
PDB	Power distribution board
PING	Packet Internet Groper
PMS	Per-module switching
PPS	Per-port switching
PS/2	Personal System/2
RFC	Request for comments
RISC	Reduced instruction set computer
RJ12	6-pin connector
RJ45	8-pin connector
RJ58	x-pin connector
SDDI	Shielded distribution data interface
SMIT	System Management Interface Tool

SNA	System network architecture
SNMP	Simple network management protocol
SQE	Signal quality error
STP	Shielded twisted pair
TCP	Transmission control protocol
TELCO	Telephone company
TELNET	Telecommunication network protocol
TFTP	Trivial file transfer protocol
T-MAC	Token-ring media access control
TP	Twisted pair
TPDDI	Twisted pair distribution data interface
TRMM	Token-ring management module
UDP	User datagram protocol
UFC	Universal feature card
UTP	Unshielded twisted pair
10BASE2	IEEE standard for Ethernet
10BASE-T	IEEE standard for Ethernet

Other abbreviations used are as follows:

- **Version** and **Release** are abbreviated as **V** and **R**, respectively.
- A small **x** is used to mean ″the specified version and all later versions of the operating system″, as in OS/2 2.**x**. It is also used to stand for a family of products, as in IBM 786**x** Modems and IBM 37**xx** Communication Controllers.

For other abbreviations, see the “Glossary” on page 451.

Glossary

This glossary defines terms and abbreviations used in this manual. It includes terms and definitions from the *IBM Dictionary of Computing* (New York; McGraw-Hill, Inc., 1994).

- The symbol (A) identifies definitions from the *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 1430 Broadway, New York, New York 10018.
- The symbol (E) identifies definitions from the *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronics Industries Association (EIA). Copies can be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, DC 20006.
- The symbol (I) identifies definitions from the *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1).
- The symbol (T) identifies definitions from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1.

The following cross-references are used in this glossary:

Contrast with. This refers to a term that has an opposed or substantively different meaning.

See. This refers to multiple-word terms in which this term appears.

See also. This refers to terms that have a related, but not synonymous, meaning.

Synonym for. This indicates that the term has the same meaning as a preferred term, which is defined in the glossary.

A

access unit. A unit that allows attaching devices to access a local area network (LAN) at a central point, such as a wiring closet or an open work area.

active. The state of a resource when it has been activated and is operational. Contrast with *inactive* and *inoperative*.

adapter. In a LAN, within a communicating device, a circuit card that, with its associated software and/or microcode, enables the device to communicate over the network.

address. In data communication, the IEEE-assigned unique code or the unique locally administered code assigned to each device or workstation connected to a network. To refer to a device or an item of data by its address. (I) (A)

address mask. For Internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with *subnet mask* and *subnetwork mask*.

agent. In the TCP/IP environment, a process running on a network node that responds to requests and sends information.

AIX. Advanced Interactive Executive.

AIX operating system. IBM's implementation of the UNIX operating system. The RISC System/6000 system, among others, runs the AIX operating system.

alert. In the NetView for AIX program, a high-priority event that warrants immediate attention. This database record is generated for certain event types that are defined by user-constructed filters.

API. Application programming interface.

application. A collection of software components used to perform specific types of user-oriented work on a computer.

application program. A program written for or by a user that applies to the user's work. Some application programs receive support and services from a special kind of application program called a network application program. A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities.

application registration file. A file created by a programmer to integrate an application into the NetView for AIX program by defining its place in the program's menu structure, where help information is found, the number and types of parameters allowed, the command line used to start the application, and other characteristics of a user-written application.

application registration file. A file created by a programmer to integrate an application into the NetView for AIX program by defining its place in the program's menu structure, where help information is found, the number and types of parameters allowed, the command line used to start the application, and other characteristics of a user-written application.

arc. In topology, an arc represents connectivity between vertices or graphs. The connection is independent of either end point.

ASCII (American National Standard Code for Information Interchange). The standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters. (A)

Note: IBM has defined an extension to ASCII code (characters 128–255).

attach. To make a device a part of a network logically. Contrast with *connect*.

attaching device. Any device that is physically connected to a network and can communicate over the network. See also *station*.

attribute. A characteristic that identifies and describes an object. The characteristic can be determined, and possibly changed, through operations on the managed object.

attribute list. A list that displays the attributes that can be set for specific objects. These are global object attributes that are valid for an object across maps. The attributes list box is available in the Add Object, Add Connection, and Describe Object dialog boxes. When adding or describing an object, the attributes associated with the object can be viewed or modified.

B

background picture. A picture or graphic that has been added to a submap to serve as a background for the displayed symbols. Background graphics provide contextual information, such as a floor plan for systems or a map of geographically diverse sites. Both users and applications can specify a separate background graphic for each submap. Background graphics are added to a submap when a new submap is created or when Edit..Submap..Description is selected from the menu bar of the submap. The background graphic must be in graphic interchange format (GIF).

background process. A process that does not require operator intervention but can be run by the computer while the workstation is used to do other work. In the AIX operating system, a mode of program execution in which the shell does not wait for program completion before prompting the user for another command.

beacon frame. A frame sent by an adapter indicating a serious ring problem, such as a broken cable. An adapter is “beaconing” if it is sending such a frame.

bridge. An attaching device that connects two LAN segments to allow the transfer of information from one LAN segment to the other. A bridge may attach the LAN segments directly by network adapters and software in a single device, or may connect network adapters in two separate devices through software and use of a telecommunications link between the two adapters. A functional unit that connects two LANs that use the same logical link control (LLC) procedures but may use the same or different medium access control (MAC) protocols. (T) Contrast with *gateway* and *router*.

bridging. In LANs, the forwarding of a frame from one LAN segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadband LAN. A local area network in which data are encoded, multiplexed, and transmitted with modulation of carriers.

Note: A broadband LAN consists of more than one channel. (T)

buffer. A portion of storage used to hold input or output data temporarily. A routine or storage used to compensate for differences in data rate or time of occurrence of events, when transferring data from one device to another. (A)

bus. A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment. (T) One or more conductors used for transmitting signals or power. (A)

button. A word or picture on the screen that can be selected. Once selected and activated, a button begins an action in the same manner that pressing a key on the keyboard can begin an action.

C

cache. A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. To place, hide, or store in a cache.

card. A unique place to display information that relates to an event. A card provides a repository for information and a fast path to the MIB browser application and the topology map representation of managed objects. Cards are placed in workspaces and can be sent to other users, searched, ordered, and reports can be generated from them. See also *MIB*.

CCITT. International Telegraph and Telephone Consultative Committee. This was an organization of the International Telecommunication Union (ITU). On 1 March 1993 the ITU was reorganized, and responsibilities for standardization were placed in a subordinate organization named the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-TS). “CCITT” continues to be used for recommendations that were approved before the reorganization.

child. Pertaining to a secured resource, either a file or library, that uses the user list of a parent resource. A child resource can have only one parent resource. A child is a process, started by a parent process, that shares the resources of the parent process. Contrast with *parent*.

child submap. A submap that represents a detailed view of an object, or the “contents” of an object (called the parent object) on a map. Double-clicking on an explodable symbol that represents the parent object opens the child submap. See also *parent object*.

click. To press and release a mouse button without moving the pointer off the choice.

client. A functional unit that receives shared services from a server. (T) A user. In an AIX distributed file system environment, a system that is dependent on a server to provide it with programs or access to programs.

CMIP. Common Management Information Protocol.

CNM. Communication network management.

command. A request from a terminal for the performance of an operation or the execution of a particular program.

command list. In the NetView for AIX program, a list of commands and statements designed to perform a specific function for the user. Command lists can be written in REXX or in the NetView command list language.

Common Management Information Protocol (CMIP). The OSI standard protocol defined in ISO/IEC 9596-1 for the interaction between managers and agents that use the Common Management Information Service Element (CMISE).

communication network management (CNM). The process of designing, installing, operating, and managing distribution of information and control among users of communication systems.

community name. A password that must be used for certain SNMP requests. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

component. Any part of a network other than an attaching device, such as an IBM 8228 Multistation Access Unit. Hardware or software that is part of a functional unit.

compound status. The compound status scheme determines how status is propagated from symbols in child submaps to symbols of the parent object. The combined status of symbols determines the resulting compound status. Compound status can propagate up through multiple levels of submaps in the network

map. The compound status setting applies to the entire map. In effect, the status of specific nodes propagates up to a symbol on a higher-level submap. Compound status is configured by using one of three schemes:

- Default
- Propagate Most Critical
- Propagate at Threshold Value

See also *default compound status*.

concentrator. A unit that allows multiple attaching devices access to the ring at a central point such as a wiring closet or in an open work area. A star-wired ring consists of one or more concentrators connected together to form a ring.

configuration file. A file that specifies the characteristics of a system device or network.

configuration parameter. A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

connect. In a LAN, to physically join a cable from a station to an access unit or network connection point. Contrast with *attach*.

context menu. A menu containing a list of choices that are currently applicable to the object from which the context menu was requested. Context menus for a group of selected objects contain only those choices that are currently applicable to the all of the objects in the selected group.

controller. A unit that controls input/output operations for one or more devices.

copy. In the NetView for AIX program, a menu item function that copies selected symbols and objects to the cut buffer. To complete the copy operation, select the Paste menu item.

CRC. Cyclic redundancy check.

critical status. In the NetView for AIX program, the status state, displayed by a symbol, that indicates a problem with the object. If the status is compound status, it reflects a critical condition in the parent object's child submap. If the status is direct status, it may reflect a critical condition for the symbol or the object. The default color for critical status is red. See *compound status* and *normal status*.

D

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automatic means. (I) (A)

data communication. Transfer of information between functional units by means of data transmission according to a protocol. (T) The transmission, reception, and validation of data. (A)

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following

table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	In-channel signaling
1–15	reserved
16–991	Assigned using frame-relay connection procedures
992–1007	Layer-2 management of frame-relay bearer service
1008–1022	Reserved
1023	In-channel layer management

default. Pertaining to an attribute, value, or option that is assumed when none is explicitly specified. (I)

default compound status. When a new map is created, compound status is set to a default value. The default value for compound status causes the graphical interface to propagate status.

destination. Any point or location, such as a node, station, or particular terminal, to which information is to be sent.

device. A mechanical, electrical, or electronic contrivance with a specific purpose. In the AIX operating system, a valuator, button, or the keyboard. Buttons have values of 0 or 1 (up or down); valuators return values in a range, and the keyboard returns ASCII values.

diagnostics. Modules or tests used by computer users and service personnel to diagnose hardware problems.

dialog box. A movable window, fixed in size, containing controls that a user uses to provide information required by an application so that it can continue to process a user request.

disabled. Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions.

discovery. The automatic detection of network topology changes (for example, new and deleted nodes, new and deleted interfaces).

display. To present data visually. (I) (A)

DLCI. Data link connection identifier.

domain. In the Internet, a part of a naming hierarchy in which the domain name consists of a sequence of names (labels) separated by periods (dots). In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies.

double-click. To press and release a mouse button twice in rapid succession.

downstream. In the direction of data flow from the host to the end user. Contrast with *upstream*.

drag. In CUA architecture, to use a pointing device to move an object; for example, clicking on a window border, and dragging it to make the window larger.

dynamic. Pertaining to an operation that occurs at the time it is needed rather than at a predetermined or fixed time.

E

edit menu. An action bar menu that contains items that enable the user to edit symbols and objects in an open map or submap. Editing includes tasks such as adding, deleting, and copying.

EMM. Ethernet management module.

end user. The ultimate source or destination of application data flowing through an SNA network. An end user can be an application program or a workstation operator.

enterprise. An entire business organization. An enterprise may consist of one or more establishments, divisions, plants, warehouses, and so on that require an information system.

enterprise-specific MIB. An SNMP Management Information Base (MIB) developed by individual vendors for specific products. Vendors register their private MIBs under the enterprise object identifier subtree. See also *MIB*.

entity. Any concrete or abstract thing of interest, including associations among things; for example, a person, object, event, or process that is of interest in the context under consideration, and about which data may be stored in a database. (T) In Open Systems Interconnection architecture, an active element within a subsystem. Cooperation between entities in a layer is controlled by one or more protocols. (T)

equipment rack. A metal stand for mounting network components, such as distribution panels and IBM 8228 Multistation Access Units. Synonymous with *rack*.

error. A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. (I) (A).

Ethernet network. A baseband LAN with a bus topology in which messages are broadcast on a coaxial cable using a carrier sense multiple access/collision detection (CSMA/CD) transmission method.

event. An occurrence of significance to a task; for example, the completion of an asynchronous operation, such as an input/output operation. In the NetView program, a record indicating irregularities of operation in physical elements of a network.

executable symbol. A symbol configured such that double-clicking on it causes an application to perform an action on a set of target objects. When you change the behavior of a symbol to executable, you choose from a list of registered applications and actions, and you choose a set of objects (target objects) that the application acts upon. You can modify these settings at any time. Executable symbols are useful for easily performing complex network management tasks as often as needed. Contrast with *explodable symbol*.

explodable symbol. A symbol configured such that double-clicking on it displays the child submap of the parent object that the symbol represents. The child submap displays the contents of the parent object. If the object the symbol represents has no child submap, a question dialog box appears enabling you to create and configure a child submap. After the submap is created, double-clicking on the symbol opens the child submap. Contrast with *executable symbol*.

F

fault. An accidental condition that causes a functional unit to fail to perform its required function. (I) (A)

FDDI. Fiber Distributed Data Interface.

FDDI network. A collection of FDDI nodes interconnected to form a trunk, or a tree, or a trunk ring with multiple trees. This topology is sometimes called a dual ring of trees.

feature. A part of an IBM product that can be ordered separately by the customer.

fiber. See *optical fiber*.

Fiber Distributed Data Interface (FDDI). A high-performance, general-purpose, multi-station network designed for efficient operation with a peak data transfer rate of 100 Mbps. It uses token-ring architecture with optical fiber as the transmission medium over distances of several kilometers.

field. An identifiable area in a window. Examples of fields are: an entry field, into which a user can type or place text, and a field of radio button choices, from which a user can select one choice. In NetView for AIX, the building block of which objects are composed. A field is characterized by a field name, a data type (integer, Boolean, character string, or enumerated value), and a set of flags that describe how the field is treated by NetView for AIX. A field can contain data only when it is associated with an object.

file. A named set of records stored or processed as a unit. (T)

filter. In the NetView for AIX program, a set of criteria that determines which events are received by registered applications, selected for displaying, or forwarded to the NetView and NETCENTER programs as alerts. In the NetView program, a function that limits the data that is to be recorded on the database and displayed at the terminal.

FMM. FDDI management module.

FOIRL. Fiber optic interconnection repeater link.

fork. In the Distributed Computing Environment (DCE), to create and start a child process. Forking is similar to creating an address space and attaching. It creates a copy of the parent process, including open file descriptors.

frame. A unit of transmission in some LANs, including the IBM Token-Ring Network and the IBM PC Network. It includes delimiters, control characters, information, and checking characters. On a token-ring network, a frame is created from a token when the token has data appended to it. On a token bus network (IBM PC Network), all frames including the token frame contain a preamble, start delimiter, control address, optional data and checking characters, end delimiter, and are followed by a minimum silence period. A protocol data unit transmitted between cooperating MAC entities on a ring, consisting of a variable number of octets.

function index. An index that enables you to get online help that describes the functions of the graphical interface. You can display the Function index from the Help menu.

G

gateway. A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T)

graphical user interface. In the NetView for AIX program, the integrating interface application that provides the means for displaying submaps and for integrating network applications. The graphical interface is a single, consistent interface that enables multiple applications to interact.

grayed. A menu selection or button that is not currently enabled for the given context and appears dim in comparison to other selections.

gtmd daemon. A background process that receives generic topology information for the multiprotocol topology functions of the NetView for AIX program.

H

hard error. An error condition on a network that requires that the network be reconfigured or that the source of the error be removed before the network can resume reliable operation. Contrast with *soft error*. Synonym for *hard failure*. (T)

hardware. Physical equipment as opposed to programs, procedures, rules, and associated documentation. (I) (A)

Help. A choice that gives a user access to helpful information about objects, choices, tasks, and products. A Help choice can appear on a menu bar or as a push button.

help menu. An action bar menu that provides detailed help information about the NetView for AIX graphical interface. It also provides information about registered applications that are integrated with the graphical interface.

help panel. Information displayed by a system in response to a help request from a user.

highlighting. In the NetView for AIX program, a visual cue showing the nodes or connections that are the output of certain operations. Emphasizing a display element or segment by modifying its visual attributes. (I) (A)

host. In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe.

host computer. In a computer network, a computer that usually performs network control functions and provides end users with services such as computation and database access. (T) The primary or controlling computer in a multiple computer installation. In a network, a processing unit in which a network access method resides. Synonymous with *host processor*.

host processor. Synonym for *host computer*.

I

ICMP. Internet Control Message Protocol.

icon. A graphic symbol, displayed on a screen, that a user can point to with a device, such as a mouse, in order to select a particular function or software application. (T)

ID. Identifier.

IEEE. Institute of Electrical and Electronic Engineers (U.S.A.).

inactive. Not operational. Pertaining to a node or device not connected or not available for connection to another node or device. In the AIX operating system, pertaining to a window that does not have an input focus. Contrast with *active*. See also *inoperative*.

initialize. In a LAN, to prepare the adapter (and adapter support code, if used) for use by an application program.

inoperative. The condition of a resource that has been active, but is no longer active. The resource may have failed, received an INOP request, or be suspended while a reactivate command is being processed. See also *inactive*.

interface. A shared boundary between two functional units, defined by functional characteristics, common physical interconnection characteristics, signal characteristics, and other characteristics as appropriate. (I) Hardware, software, or both, that links systems, programs, or devices.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The Internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols. See also *internet*.

Internet address. See *IP address*.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

IP. Internet Protocol.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comments (RFC) 791. It is usually represented in dotted decimal notation.

ISO. International Organization for Standardization

K

kbps. Kilobits per second.

L

label. A label is used to distinguish a symbol from other symbols on a submap and map. The label is displayed below a symbol. Labels can be assigned or modified at any time by using the Symbol Description dialog box.

LAN. Local area network.

LAN adapter. The circuit card within a communicating device that, together with its associated software, enables the device to be attached to a LAN.

LAN Network Manager for AIX. LAN Network Manager for AIX is an IBM licensed program that monitors and manages local area network (LAN) resources. LAN Network Manager for AIX can manage logical link control-based and simple network management protocol (SNMP) based token-ring LAN segments, fiber distributed data interface segments, and SNMP-managed bridges. This program monitors other LAN and wide area network (WAN) segment types.

LAN segment. Any portion of a LAN (for example, a bus or ring) that can operate independently, but that is connected to other parts of the network by means of bridges. A ring or bus network without bridges.

layer. One of the seven levels of the Open Systems Interconnection (OSI) reference model. In open systems architecture, a collection of related functions that comprise one level of hierarchy of functions. Each layer specifies its own functions and assumes that lower level functions are provided.

link. The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration. To interconnect items of data or portions of one or more computer programs: for example, the linking of object programs by a linkage editor, linking of data items by pointers. (T)

LLC. Logical link control.

lobe. In the IBM Token-Ring Network, the section of cable that attaches a device to an access unit. The cable may consist of several segments.

local area network (LAN). A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) See also *Ethernet network* and *token-ring network*.

local registration file (LRF). A file that provides information about an agent or daemon, such as the name, the location of the executable code, and details about the objects that an agent manages.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

logical link control (LLC). The data link control (DLC) LAN sublayer that provides two types of DLC operation for the orderly exchange of information. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery.

M

MAC. Medium access control.

managed node. In Internet communications, a workstation, server, or router that contains a network management agent. In the Internet Protocol (IP), the managed node usually contains a Simple Network Management Protocol (SNMP) agent.

managed object. A component of a system that can be managed by a management application. The OSI management view of a resource that can be managed through the use of OSI management protocols.

Management Information Base (MIB). A collection of objects that can be accessed by means of a network management protocol. A definition for management information that specifies the information available from a host or gateway and the operations allowed. In OSI, the conceptual repository of management information within an open system.

map. A set of related submaps that provides a graphical and hierarchical presentation of a network and its systems.

MAT. Management application transfer.

MB. Megabyte

medium. A physical carrier of electrical or optical energy.

medium access control (MAC). The portion of the data link layer responsible for scheduling and routing data transmissions on a local area network (for example, an FDDI ring).

megabyte. For processor storage and real and virtual memory, 2^{20} or 1 048 576 bytes. For disk storage capacity and transmission rates, 1 000 000 bytes.

menu. A list of options displayed to the user by a data processing system, from which the user can select an action to be initiated. (T)

menu bar. A rectangular area at the top of the client area of a window that contains the titles of the standard pull-down menus for that application.

menu item. One of a list of options contained in a menu.

message. An assembly of characters and sometimes control codes that is transferred as an entity from an originator to one or more recipients. A message consists of two parts: envelope and content. (T) In VTAM, the amount of function management data (FMD) transferred to VTAM by the application program with one SEND request.

MIB. Management Information Base.

microcode. One or more microinstructions. A code, representing the instructions of an instruction set, that is implemented in a part of storage that is not program-addressable. To design, write, and test one or more microinstructions.

motif. See *OSF/Motif*.

mouse. A commonly used pointing device, containing one or more buttons, with which a user can interact with a product or the operating environment.

N

NetBIOS. Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols.

NETCENTER. A software product that assists the network operator and other technical personnel at a network control center in managing the network.

netmon daemon. A background process that discovers and monitors nodes on the network.

NetView for AIX. Also known as *SystemView NetView for AIX* (part of *SystemView for AIX*). An IBM licensed program for systems management in the AIX environment. NetView for AIX can use the NetView for AIX Service Point to communicate with the NetView and NETCENTER programs.

network. An arrangement of nodes and connecting branches. (T) A configuration of data processing devices and software connected for information interchange. A group of nodes and the links interconnecting them. See also *FDDI network*.

network adapter. A physical device, and its associated software, that enables a processor or controller to be connected to a network.

network address. In a subarea network, an address, consisting of subarea and element fields, that identifies a link, link station, physical unit, logical unit, or system services control point. Subarea nodes use network addresses; peripheral nodes use local addresses or local-form session identifiers (LFSIDs). The boundary function in the subarea node to which a peripheral node is attached transforms local addresses or LFSIDs to network addresses and vice versa. According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network application program. A program used to connect and communicate with adapters on a network, enabling users to perform application-oriented activities and to run other application programs.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network monitor card (NMC). A daughter card that is carried by a module. A daughter card may be a MAC daughter card (Chipcom NMC) or a security daughter card.

node. In a network, a point at which one or more functional units connect channels or data circuits. (I) Any device, attached to a network, that transmits and receives data. An endpoint of a link or a junction

common to two or more links in a network. Nodes can be processors, communication controllers, cluster controllers, or terminals. Nodes can vary in routing and other functional capabilities.

node submap. Contains the addressable resources of a network, such as a gateway, router, workstation, and personal computer.

normal status. Indicates that a network object is functioning normally. The default icon symbol color for normal status is green. The default connection symbol color for normal status is black. See *critical status*.

notification. An unscheduled, spontaneously generated report of an event that has occurred. In OSI management, information emitted by a managed object relating to an event that has occurred within the managed object.

O

object. In the NetView for AIX program, a generic term for any entity that NetView for AIX discovers and displays on the topological map, or any entity that you add to the topology map.

object ID. The unique name identification of a management information base object.

Open Software Foundation (OSF). A consortium of various computer and software manufacturers whose purpose is to provide enabling technology.

Open Systems Interconnection (OSI). The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) The use of standardized procedures to enable the interconnection of data processing systems.

Note: OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

operating system (OS). Software that controls the execution of programs and that may provide services such as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial hardware implementations are possible. (T)

optical cable. A fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications. (E)

optical fiber. Any filament made of dielectric materials that guides light, regardless of its ability to send signals. (E) See also *fiber optics*.

optical fiber cable. Synonym for *optical cable*.

option. A specification in a statement, a selection from a menu, or a setting of a switch, that can be used to influence the execution of a program. A hardware or software function that can be selected or enabled as part of a configuration process. A piece of hardware (such as a network adapter) that can be installed in a device to modify or enhance device function.

OS/2. IBM Operating System/2.

OSF. Open Software Foundation.

OSF/Motif. A graphical interface that contains a tool kit, presentation description language, window manager, and style guideline. See also *Open Software Foundation*.

OSI. Open Systems Interconnection.

output device. A device in a data processing system by which data can be received from the system. (I) (A) Synonymous with *output unit*.

output unit. Synonym for *output device*.

ovspmd daemon. A background process that coordinates the start and stop of the other NetView for AIX daemons.

ovtopmd. A process that puts Internet Protocol (IP) topology information in the NetView for AIX program's database.

P

packet internet groper (PING). In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply.

panel. A formatted display of information that appears on a display screen. See *help panel*.

parameter. A variable that is given a constant value for a specified application and that may denote the application. (I) (A) An item in a menu or for which the user specifies a value or for which the system provides a value when the menu is interpreted. Data passed between programs or procedures.

parent. A process that spawns a child process using forking. Contrast with *child*. See also *fork*.

parent object. The relationship that an object has with its child submap. Symbols of a parent object can appear on multiple submaps.

parent submap. The view from which an object was expanded. Each segment has a parent Network submap. Each network has the Internet submap for its parent. See also *parent window*.

parent window. In AIX Enhanced X Windows, the window that controls the size and location of its children. If a window has children, it is a parent window. See also *parent submap*.

path. In a network, any route between any two nodes. (T) The route traversed by the information exchanged between two attaching devices in a network.

PBS. Per-bank switching

PCS. Per-connector switching

physical layer. In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish and release physical connections over the transmission medium. (T)

physical link. In FDDI, the simplex path (through PMD and attached medium) from the transmit function of one PHY entity to the receive function of an adjacent PHY entity (in concentrators, repeaters, or stations) in an FDDI ring.

PMS. Per-module switching

polling. On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. An access point for data entry or exit. A connector on a device to which cables for other devices such as display stations and printers are attached. Synonymous with *socket*.

PPS. Per-port switching

process ID. A unique number that is assigned by the AIX Operating System to each program that is running.

processor. In a computer, a functional unit that interprets and executes instructions. A processor consists of at least an instruction control unit and an arithmetic and logic unit. (T)

propagate at threshold value. A compound status scheme in which the NetView for AIX program propagates marginal or critical status based on threshold values. The default threshold to propagate marginal status is 50%. The default threshold to propagate critical status is 90%. See also *compound status, default compound status,* and *propagate most critical*.

propagate most critical. A compound status scheme in which the NetView for AIX program propagates the status of the most critical symbol in the child submap to the symbol of the parent object. See *compound status, default compound status,* and *propagate at threshold value*.

protocol. A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I)

proxy agent. A “translator” routine that manages an object and converts its communications defined by one protocol.

PS/2. IBM Personal System/2.

PSM. Product-specific module.

pull-down menu. A list of choices extending from a selected menu-bar choice that gives users access to actions, routings, and settings related to an object.

push button. A rectangle that appears as three-dimensional with text inside. Push buttons are used in windows for actions that occur immediately when the push button is selected.

R

rack. Synonym for *equipment rack*.

read-only access. In the NetView for AIX program, an open map that a user can view. A map open with read-only access displays status, allows submap and snapshot traversal, and enables you to monitor and

locate objects. The File..Refresh Map menu item is used to update the topology of a map open with read-only access. Objects, symbols, submaps, and snapshots cannot be deleted or modified. See *read-write access*.

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

read-write access. In the NetView for AIX program, an open map that a user can change. This map is continuously updated with status and topology changes. With read-write access, objects, symbols, submaps, and snapshots can be added or deleted within the map. Only one user can have a map open with read-write access at a given time. See *read-only access*.

recommended action. Procedures suggested by the NetView for AIX program that can be used to determine the causes of network problems.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

registration file. See *application registration file*

remote. Pertaining to a system, program, or device that is accessed through a telecommunication line. A device that does not use the same protocol and is, therefore, unknown.

remove. In the IBM Token-Ring Network, to take an attaching device off the ring.

repeater. In a network, a device that amplifies or regenerates data signals in order to extend the distance between attaching devices. A physical layer relay in an FDDI network.

resource. Any facility of a computing system or operating system required by a job or task, and including main storage, input/output devices, the processing unit, data sets, and control or processing programs. In the NetView for AIX program, any hardware or software that provides function to the network.

response. In data communication, a reply represented in the control field of a response frame. It advises the primary or combined station of the action taken by the secondary or other combined station to one or more commands. See also *command*.

RFC. Request for Comments (Internet document).

ring. A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

RISC. Reduced instruction-set computer.

root submap. Contains the highest level of the submap hierarchy. Multiple networks can be placed within the root submap.

root user. Synonym for *superuser authority*.

route. An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. The path that network traffic uses to get from source to destination.

router. An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. Contrast with *bridge* and *gateway*.

routine. Part of a program, or a sequence of instructions called by a program, that may have some general or frequent use.

routing. The process of determining the path to be used for transmission of a message over a network. (T)

S

SAA. Systems Application Architecture.

SAP. Service access point.

screen. In the AIX extended curses library, a window that is as large as the display screen of the workstation.

scroll. To move a display image vertically or horizontally to view data that cannot be observed within a single display screen.

segment. A group of display elements. In the IBM Token-Ring network, a section of cable between components or devices on the network. A segment may consist of a single patch cable, multiple patch cables connected together, or a combination of building cable and patch cables connected together.

segment submap. A submap that represents the topology of a segment of a network. A segment submap contains network nodes and connectors.

select. In the AIX operating system, to choose a button on the display screen. To place the cursor on an object (name or command) and press a button on the mouse or the appropriate key on the keyboard.

service access point (SAP). In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

shell procedure. In the AIX operating system, a series of commands, combined in a file, that carry out a particular function when the file is run or when the file is specified as a value to the SH command.

shell script. Synonym for *shell procedure*.

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

SMIT. System Management Interface Tool

SNA. Systems Network Architecture.

SNMP. Simple Network Management Protocol.

socket. Synonym for *port*.

soft error. An error that occurs sporadically and that may not appear on successive attempts to read data. Synonymous with *transient error*. (T) An intermittent error on a network that requires retransmission. Contrast with *hard error*.

Note: A soft error by itself does not affect overall reliability of a network, but reliability may be affected if the number of soft errors reaches the ring error limit.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

status. The condition or state of hardware or software, usually represented by a status code. In the NetView for AIX program, the condition of a node or portion of the network as represented by the color of a symbol on a submap.

subagent. In the AIX Systems Monitor/6000 program, a background process called sysmond. The sysmond daemon provides local and remote systems monitoring, using the Simple Network Management Protocol (SNMP).

submap. A particular view of some aspect of a network that displays symbols that represent objects. Some symbols may explode into other submaps, usually having a more detailed view than their parent submap. The application that creates a submap determines what part of the network the submap displays. See also *root submap, node submap,* and *segment submap*.

submap stack. A component of the graphical interface shown on the left side of each submap window. The submap stack represents the ancestry of all submaps. Selecting a submap representation from the stack causes the contents of the current submap window to be replaced with the selected submap. Dragging a submap representation from the stack causes a new window to be opened.

submap window. A submap window contains an NetView for AIX menu bar, a submap viewing area, a status line, and a button box. You can display multiple submap windows of an open map and an open snapshot at any given time.

subnet. In TCP/IP, a part of a network that is identified by a portion of the Internet address. Synonym for *subnetwork*.

subnetwork. Any group of nodes that have a set of common characteristics, such as the same network ID. In the AIX operating system, one of a group of multiple logical network divisions of another network, such as can be created by the Transmission Control Protocol/Internet Protocol (TCP/IP) interface program. Synonymous with *subnet*.

superuser authority. In the AIX operating system, the unrestricted authority to access and modify any part of the operating system, usually associated with the user who manages the system.

symbol. In the NetView for AIX program, a picture or icon that represents an object. Each symbol has an outside and inside component.

- The outside component differentiates the object classes.
- The inside component differentiates the objects within the class.

synchronous. Pertaining to two or more processes that depend on the occurrences of specific events such as common timing signals. (I) (A) Occurring with a regular or predictable timing relationship. A class

of data transmission service whereby each requester is preallocated a maximum bandwidth and guaranteed a response time not to exceed a specific delay.

System Management Interface Tool (SMIT). An interface tool that is provided with the AIX Operating System for installing, maintaining, configuring, and diagnosing tasks.

SystemView NetView for AIX. See *NetView for AIX*.

T

task. In a multiprogramming or multiprotocol environment, one or more sequences of instructions treated by a control program as an element of work to be accomplished by a computer. (I) (A)

task index. An index that provides online help entries for a variety of tasks that are available in the NetView for AIX program and applications that are integrated with the NetView for AIX program. The Task Index can be accessed from the Help menu.

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol.

terminal. A device, usually equipped with a keyboard and a display device, that is capable of sending and receiving information.

TFTP. Trivial File Transfer Protocol.

threshold. In the NetView for AIX program, a setting that specifies the maximum value a statistic can reach before notification that the limit was exceeded. For example, when a monitored MIB value has exceeded the threshold, SNMPCollect generates a threshold event.

toggle button. In AIXwindows and Enhanced X Windows, a graphical object that simulates a toggle switch; it switches sequentially from one optional state to another.

token ring. According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. See also *local area network (LAN)*.

topology. The physical or logical arrangement of nodes in a computer network. Examples include ring topology and bus topology.

trace. A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) For data links, a record of the frames and bytes transmitted or received.

tralert daemon. A background process that receives SNMP traps, converts the traps to NMVT alerts, and sends the alerts to the host system that is running the NetView for AIX and NETCENTER programs.

Transmission Control Protocol (TCP). A communications protocol used in Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet Protocol is the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission medium. A physical carrier of electrical energy or electromagnetic radiation. The physical medium that conveys data between data stations; for example, twisted-pair wire, optical fiber, coaxial cable. (T)

transmit. To send data from one place for reception elsewhere. (A) The action of a station in generating a token, frame, or other symbol sequence and placing it on the outgoing medium.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

trapd daemon. A background process that receives events and traps, logs them to a specific log file, and upon request can forward the events to other daemons or processes.

tree. A physical topology consisting of a hierarchy of master-slave connections between a concentrator and other FDDI nodes (including subordinate concentrators).

TRMM. Token-ring management module.

trunk. A physical topology, either open or closed, employing two optical fiber signal paths, one in each direction (that is, counter-rotating), forming a sequence of peer connections between FDDI nodes. When the trunk forms a closed loop it is sometimes called a trunk ring.

twisted pair. A transmission medium that consists of two insulated conductors twisted together to reduce noise. (T)

U

UNIX operating system. An operating system developed by Bell Laboratories that features multiprogramming in a multiuser environment. The UNIX operating system was originally developed for use on minicomputers but has been adapted for mainframes and microcomputers. The AIX operating system is IBM's implementation of the UNIX operating system. See *AIX operating system*.

unknown status. The status of an object that is not yet known or does not actually exist in the network. The default icon symbol color for unknown status is blue. The default connection symbol color is black. See also *critical status, normal status, unmanaged status,* and *status*.

unmanaged status. The status that indicates that an object is unmanaged. The default icon symbol color displayed to indicate unmanaged status is wheat. The default connection symbol color displayed is black. See also *critical status, normal status, compound status, unknown status,* and *status*.

upstream. In the direction of data flow from the end user to the host. Contrast with *downstream*.

user. A person who requires the services of a computing system. Any person or any thing that may issue or receive commands and messages to or from the information processing system. (T) Anyone who requires the services of a computing system.

V

value. A specific occurrence of an attribute; for example, “blue” for the attribute “color.” (T) A quantity assigned to a constant, a variable, a parameter, or a symbol.

variable. In the NetView command list language, a character string beginning with “&” that is coded in a command list and is assigned a value during execution of the command list. In the Simple Network Management Protocol (SNMP), a match of an object instance name with an associated value.

version. A separately licensed program that usually has significant new code or new function.

view. Synonym for *submap*.

W

WAN. Wide area network.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) Contrast with *local area network (LAN)*.

wildcard character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character.

window. A portion of a display surface in which display images pertaining to a particular application can be presented. Different applications can be displayed simultaneously in different windows. (A)

wiring closet. A room that contains one or more distribution panels and equipment racks that are used to interconnect cables. Sometimes called a *network wiring closet* to distinguish it from a telephone wiring closet.

workstation. A functional unit at which a user works. A workstation often has some processing capability. (T) A personal desktop computer consisting of a monitor, keyboard, and central processing unit. Workstations can have voice/data application program software enabled by CallPath for Workstations.

X

X.25. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks.

X.25 interface. An interface consisting of a data terminal equipment (DTE) and a data circuit-terminating equipment (DCE) in communication over a link using the procedures described in the CCITT Recommendation X.25.

X-Window System. A network-transparent windowing system developed by the Massachusetts Institute of Technology (MIT). It is the basis for the Enhanced X-Windows Toolkit.

Bibliography

NetView for AIX Publications

- *NetView for AIX User's Guide Version 3* (SC31-7024)
- *NetView for AIX Installation and Configuration* (SC31-7020)

In addition to these printed books, hypertext documentation of the NetView for AIX library is available through InfoExplorer. An online Help Index is also available from the NetView for AIX Help pull-down window. The Help Index provides dialog box help, function help, and task help.

IBM RISC System/6000 and AIX Operating System Publications

In addition to the NetView for AIX documentation, the following publications may also be helpful to users:

- *AIX Quick Reference* (SC23-2401)
- *Task Index and Glossary for IBM RISC System/6000* (GC23-2201)
- *AIX Commands Reference for IBM RISC System/6000* (GC23-2366, GC23-2367, GC23-2376, GC23-2393)
- *AIX Communications Concepts and Procedures for IBM RISC System/6000* (GC23-2203)
- *IBM RISC System/6000 Problem Solving Guide* (SC23-2204)

OSF/Motif Publications

- *OSF/Motif Style Guide* (ISBN 0-13-640491-X)
- *OSF/Motif User's Guide* (ISBN 0-13-640525-8)
- *OSF/Motif Programmer's Guide* (ISBN 0-13-640509-6)
- *OSF/Motif Programmer's Reference* (ISBN 0-13-640517-7)

X Window Publications

- *X Window System: Programming and Applications with Xt, OSF/Motif Edition*, Douglas A. Young, Prentice-hall, 1990 (ISBN 0-13-497074).
- *IBM AIX X-Windows Programmer's Reference* SC23-2118.
- *Introduction to the X Window System*, Oliver Jones, Prentice-Hall, 1988 (ISBN 0-13-499997)

Token-Ring Network Publications

IBM Token-Ring Network Problem Determination Guide (SZ27-3710)

IBM 8230 Token-Ring Network Controlled Access Base Unit Customer Setup Instructions (GA27-3905) This book is shipped with the Controlled Access Unit and is required for general planning tasks.

IBM Local Area Network Administrator's Guide (GA27-3748)

IBM Token-Ring Network Introduction and Planning Guide (GA27-3677)

IBM Token-Ring Network Installation Guide (GA27-3678)

IBM Token-Ring Network Architecture Reference (SC30-3374)

IBM Token-Ring Network Bridge Program The appropriate version for your bridge program.

LAN Cabling System Planning and Installation Guide (GA27-3361)

FDDI Network Publications

FDDI Introduction and Planning Guide (GA27-3892)

FDDI User's Guide and Programmer's Reference (SC28-2823)

FDDI Introduction and Programming Guide (GA27-3892)

8240 Concentrator CC 85062 (ZZ25-9741)

FDDI SNMP Proxy Agent User's Guide (GC17-0383)

Nways Manager-ATM Publications

- *Nways Manager-ATM User's Guide* (online DynaText books) installed with the product

Remote Monitor Publications

Remote Monitor Publications

- *Remote Monitor User's Guide* (online book) installed with the product

Traffic Monitor Publications

- *Traffic Monitor User's Guide* (online book) installed with the product

Miscellaneous

- **Marshall T Rose** *The Simple Book* Prentice-Hall (ISBN-0-13-8126607)
- **D Comer and D Stevens** *Internetworking with TCP/IP* Prentice-Hall
- *TCP/IP Tutorial and Technical Overview* (Red Book) GG24-3376

Index

Special Characters

<< Port >> pushbutton 33
<< Trunk >> pushbutton 33

Numerics

10-slot chassis 35
17-slot chassis 35, 36
6611s, displaying 105
7-slot chassis 35
8229s, displaying 105
8260 hubs managed by ATM Switch with DMM subset 36

A

abbreviations 447
abbreviations, list of 451
access control 23
access to a LAN, controlling 108
adapter kits, using 67
adapter monitoring 210, 222
adapter problems 352
adapters that are allowed to trace 213
add object connection 40
adding
  additional management modules 66
  ports to a group 82
additional information for pop-up messages 175
addtrap command 255
advanced DMM module 73
agent discovery problems 351
agent level view 46
agent modules
  8250 management modules 66
  8260 management modules 67
  introduction 65
agents
  FDDI 317
  FDDI SNMP Proxy Agent 311
  LNM OS/2 205
  OS/2 agent 199
  SNMP 276
agents, discovery 435
aggregation, status 37
alarm cards 26
alert filter 116
alert table 103
All option 81
application help 33
application level configuration parameters 173
applications
  FDDI 317
  LNM OS/2 agent 205
applications *(continued)*
  SNMP bridge 317
  SNMP token-ring 275
applications, LAN Network Manager 23
Apply pushbutton 32
architecture support, TriChannel 66
ASCII terminal configuration 78
ATM cluster view 47
ATM management 431
ATM switch acting as master agent 157
ATM Switch with DMM subset 36
attachment
  bridge definition 231
  configuration 334
  data
    LLC token-ring 226
    SNMP token-ring 286
  information 334
  mapped addresses 236
  profile 334
  static entries 235
  station definition 223
attribute panel, statistics 134
attributes section 32
authorized use of IBM online books 444
automatic detection faults 66
automatic handling of changes, prerequisites 171
automatic handling of management module changes 171
auxiliary port 78

B

backplane ports 33
backup ports 61
bank
  configuration 71
  switching 61
basic principles of lost connection with master SNMP recovery 173
beep command, NetView for AIX 154
bibliography 473
BootP function 106
box management 66
bridges 61
  bridge 232
  configuration
    FDDI 331
    LLC token-ring 232, 249, 252, 253
    SNMP 295
    SNMP token-ring 292
  configuration information 295
  configuring SNMP parameters 272

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Readers' Comments — We'd Like to Hear from You

Nways Manager for AIX
LAN Network Manager/Intelligent Hub Management Program User's Guide
Version 2.0

Publication No. GA27-4232-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

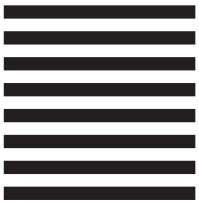
Phone No. _____

Readers' Comments — We'd Like to Hear from You
GA27-4232-00

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Department CGF
Design & Information Development
IBM Corporation
PO Box 12195
RESEARCH TRIANGLE PARK, NC
U.S.A. 27709-9990

Fold and Tape | **Please do not staple** | Fold and Tape

GA27-4232-00

Cut or Fold
Along Line

Program Number: 5697-C30

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

Nways Management Web site:
http://www.networking.ibm.com/netmgt

GA27-4232-00