Nways Multiprotocol Switched Services Family
Clients

Interface Configuration and Software User's Guide

SC30-3966-01

Nways Multiprotocol Switched Services Family
Clients

Interface Configuration and Software User's Guide

SC30-3966-01

Note

Before using this document, read the general information under “Notices” on page xvii.

Second Edition (February 1999)

This edition applies to Version 2.2 of the IBM Multiprotocol Switched Services (MSS) Family Clients and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

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

IBM welcomes your comments. A form for readers' comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation
Design and Information Development
Department CGF
P.O. Box 12195
Research Triangle Park, NC 27709-9990
U.S.A.

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 any obligation to you.

Contents

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent 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 subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Notice to Users of Online Versions of This Book

For online versions of this book, you are authorized 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.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Advanced Peer-to-Peer Networking
AIX
AIXwindows
APPN
BookManager
Common User Access
CUA
IBM
Micro Channel
NetView
Nways
OS/2
Operating System/2
RS/6000
System/370
VTAM
Web Explorer
PS/2

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

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

Other company, product, and service names may be trademarks or service marks of others.

Preface

This manual contains the information you will need to use the command line interface for configuration and operation of the MSS Client or the MSS Domain Client, hereafter referred to as “the MSS Family Client.” With the help of this manual, you should be able to perform the following processes and operations:

- Configure, monitor, and use the base code on your MSS Family Client
- Configure, monitor, and use the interfaces and Link Layer software supported by your the router.

Note: In this book, the MSS Family Client will be referred to as the router.

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

Conventions Used in This Manual

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

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

   reload

   In this example, you can enter either the whole command (reload) or its abbreviation (rel).
2. Keyword choices for a parameter are enclosed in brackets and separated by the word or. For example:

   ```
   command [keyword1 or keyword2]
   ```

   Choose one of the keywords as a value for the parameter.
3. In information displayed in response to a command, defaults for an option are enclosed in brackets immediately following the option. For example:

   ```
   Media (UTP/STP) [UTP]
   ```

   In this example, the media defaults to UTP unless you specify STP.
4. Keyboard key combinations are indicated in text in the following way:

   -
     - **Ctrl-P**

     The key combination **Ctrl P** indicates that you should press the Ctrl key and the ″P″ key simultaneously. In certain circumstances, this key combination changes the command line prompt.
   - Names of keyboard keys are indicated like this: **Enter**

Part 1. User’s Guide

Chapter 1. Getting Started

This chapter shows you how to get started with using the following components related to the MSS Client and MSS Domain Client:

- Console terminals
- Software (IBM Multiprotocol Switched Services Family Client)
- Software user interface

The information in this chapter is divided into the following sections:

- “MSS Family Client Introduction and Overview”
- “Before You Begin” on page 11
- “Accessing the Software Using Local and Remote Consoles” on page 12
- “Discussing the User Interface System” on page 17

MSS Family Client Introduction and Overview

The Multiprotocol Switched Services Client and Multiprotocol Switched Services Domain Client (hereafter called the MSS Family Clients) provide a way to increase the functionality of the existing IBM 827x LAN Switch family. The MSS Family Clients are an extension of the MSS Server function in the IBM 8210 Multiprotocol Switched Services Server. Depending on the LAN switch configuration, the MSS Family Client can also be used to enhance the performance of the base switch. The new features added to the base LAN switch by the MSS Family Client depend on the type of switch with which the client is used.

The reasons for using an MSS Family Client in the IBM 827x LAN Switch Family can be grouped into four categories:

- The ability to enable Layer 3 routing functionality at the edge of the network, for example IP and IPX
- Support for enhanced bridging for Source Route Bridge (SRB) configurations
- The ability to use LAN Network Management (LNM) to enhanced bridge management
- Enhanced ATM support for LAN Emulation and native protocol support for IP and IPX

In Figure 1 on page 4, the left side shows a model of a base Token-Ring LAN switch on which the physical ports have been sectioned off into four isolated domains. If you need to interconnect the domains, you can use the SRB function provided by the base LAN switch. However, the MSS Family Client model on the right side of Figure 1 on page 4 enhances this model by distributing the SRB function between the base LAN switch and the MSS Family Clients or allowing the domains to be routed rather than bridged.

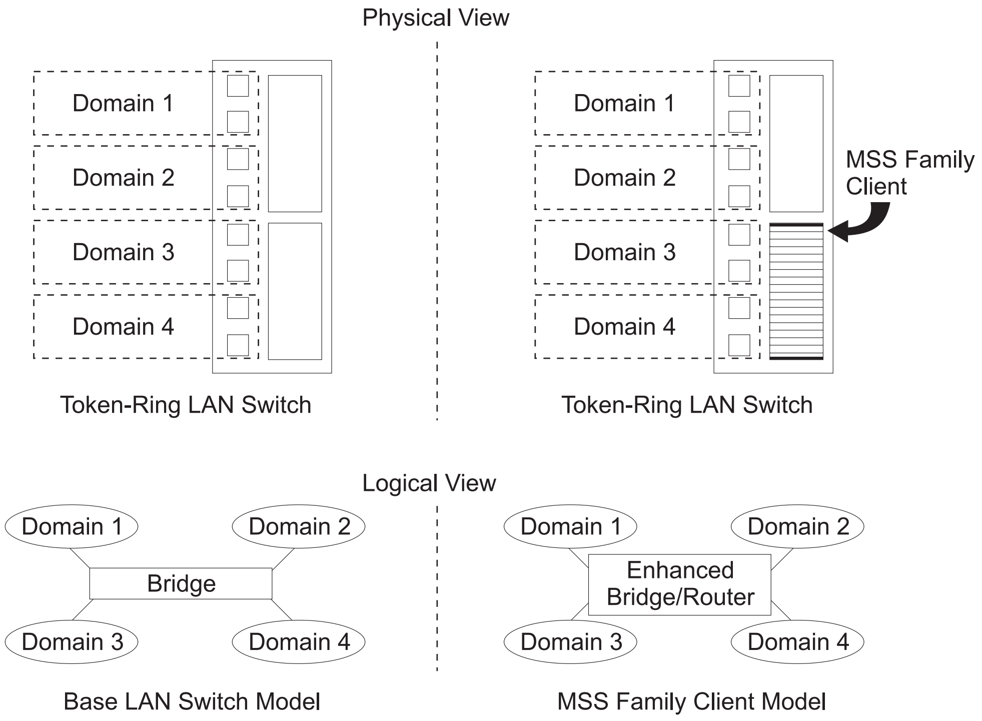


Figure 1. MSS Family Client Model in a Token-Ring LAN Switch

When you enable the MSS Family Client's SRB function, the MSS Family Clients process the Spanning Tree Protocol and all forwarding of explorer frames. The SRB function in the base switch continues to process all known and unknown specifically routed frames (SRFs) for unicast and multicast traffic. This processing creates a distributed system environment between the base switch and MSS Family Clients, which enhances performance.

When you use the MSS Client, the model is enhanced with ATM support for LAN Emulation, MPOA, NHRP, and native protocol support for IP and IPX. The MSS Client model shown in Figure 2 on page 5 provides a single 0C3 ATM interface for connecting to the campus backbone. When you enable the MSS Client SRB function, traffic between the ATM interface and the switch domains is bridged through the hardware. When the traffic between the ATM interface and the switch domains is routed, the software path of the MSS Client's CPU is used.

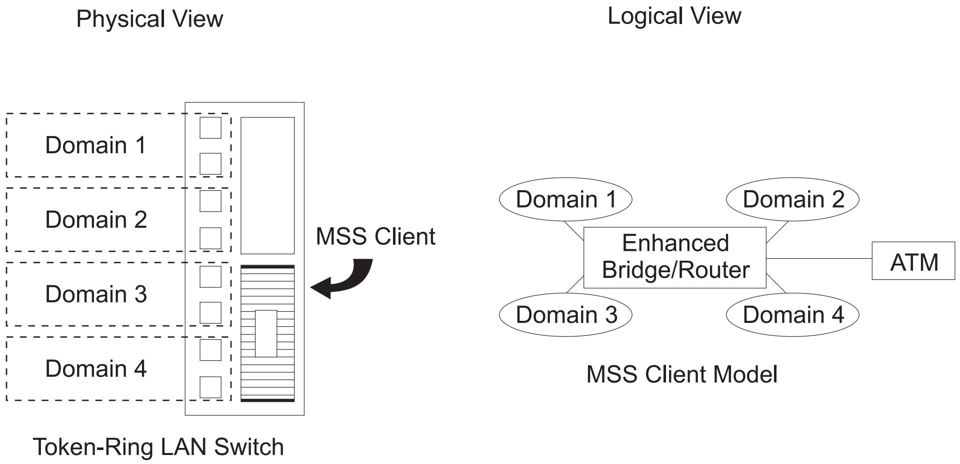


Figure 2. MSS Client Model in a Token-Ring LAN Switch

In either the bridging or routing model, the system is still distributed. The base LAN switch and MSS Client are distributing the work load, which enhances performance. Also, you can install the MSS Domain Client in a base Token-Ring switch with an ATM UFC. This installation allows you to enable most of the enhanced bridging and routing features in the base LAN switch but does not provide MPOA, NHRP, or native protocol support over ATM.

The enhanced network management support provided by LNM is a key feature of the MSS Family Clients. LNM is not supported in the base Token-Ring LAN switches, but is used to manage many Token-Ring networks. The support MSS Family Clients provide for LNM and SRB performance enhancements alone is a strong motivator for installing MSS Family Clients in existing switches.

The MSS Domain Client can also be installed in Ethernet-based LAN switches as shown in Figure 3 on page 6. The model on the left side shows that if you segment the physical ports into four domains, there is no way to interconnect the domains together. The only way to resolve this problem is to put all the physical ports into one domain or to use an external router or bridge. Putting all the physical ports into one domain can cause broadcast problems, and an external router is expensive and can take up physical ports on the LAN switch, depending on the wiring scheme used. Installing an MSS Domain Client, as shown on the right side, allows the domains to be routed together using the CPU in the MSS Domain Client.

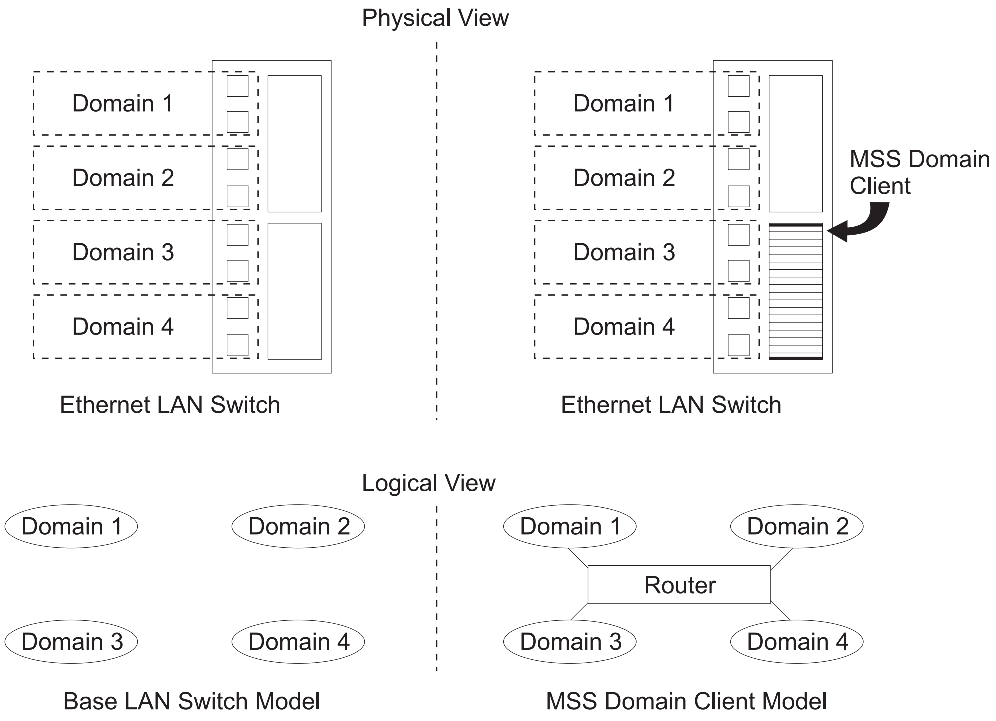


Figure 3. MSS Domain Client Model in an Ethernet LAN Switch

MSS Family Client Configuration Concepts

The following sections are intended to clarify some of the concepts behind configuring your MSS Family Clients. The sections are not intended to be a configuration guide. The configuration concepts described are:

- “Bridging”
- “Routing” on page 7
- “Multiple MSS Family Clients” on page 7
- “One Hop Routing Model” on page 8

Bridging

Note: The MSS Family Clients do not support bridging on an Ethernet LAN switch. To enable the enhanced SRB bridging support, you must configure SRB bridging support on the MSS Family Clients. Simply installing the MSS Family Client hardware in the base LAN switch will not enable this function. You must explicitly configure SRB bridging support on the MSS Family Clients. When you enable this support, the MSS Family Clients will reconfigure the base SRB support in the LAN switch to distributed SRB functionality. You can still view the SRB configuration and statistical information on the base LAN switch, but you will not be able to change configuration information for SRB on the LAN switch. When the MSS Family Client becomes disabled, the base LAN Switch SRB configuration is restored and the system administrator can make configuration changes to the SRB feature on the LAN Switch.

One significant difference between the MSS Client’s ATM support and the ATM UFC is that you can place the ATM UFC in the same domain as legacy LAN switch ports. This cannot be done with the MSS Client's ATM support. The SRB feature in the MSS Client must be used to bridge between LAN switch domains and the MSS Client's ATM interface.

Although you can use external bridges to enhance overall network performance, these bridges take up physical port space and are limited to a physical port's bandwidth. The MSS Family Clients attach virtual bridging interfaces, which are limited only by the LAN switch's internal bus between the ports and not the 16-Mbps speed of a physical Token-Ring port. Each MSS Family Client's bridge port is attached to a domain virtually and is involved with processing Explorer frames, managing Spanning Tree Protocol (STP) frames, and LNM frames.

The MSS Family Clients do not automatically configure support for PVLANs. You must configure PVLANs on the MSS Family Client and enable SRB bridging support. (PVLANs provide a way for system administrators to limit broadcast scope among domains but do not want to enable routing at the edge of the network.)

Routing

The system administrator must explicitly configure the routing support provided by the MSS Family Client. When you define a routing interface, the MSS Family Clients attach a virtual routing interface to a domain in the base LAN Switch. The switch is not aware that the domains are being routed. The switch performs the intra-domain management while the MSS Family Clients handle all inter-domain communication.

One significant benefit of using the MSS Family Clients for routing instead of an external router is that the virtual interface's bandwidth is limited by the switch's internal bandwidth and not by the bandwidth of the physical port. Because the interface is virtual, the system uses no physical port resources but can still communicate with any existing routers in the network without any cable modifications to the network.

Enabling routing allows the MSS Family Clients to limit broadcasts to high-speed network links such as the ATM UFC and Fast Ethernet UFC. The MSS Family Clients can act as front ends to the high-speed links, allowing only routed frames to pass through to these links.

Multiple MSS Family Clients

Because the MSS Family Clients are not limited to physical port bandwidth, they can achieve higher performance. To further extend this model, you can place multiple MSS Family Clients in a single LAN switch and achieve even greater throughput. Although multiple MSS Family Clients can reside in the same LAN switch, you can configure only one for enhanced bridging support. The base LAN switch is capable of the following MSS Family Clients combinations, depending on slot availability:

- 1 MSS Client, 1 MSS Domain Client
- 2 MSS Domain Clients
- 2 MSS Clients

Note: You can install only 1 MSS Client or 1 MSS Domain Client if you have already installed an ATM UFC in the LAN switch. You cannot install any MSS Family Clients if 2 ATM UFCs are in the LAN switch.

Installing two MSS Family Clients allows the system to distribute routing functionality between two processors, which provides performance benefits similar to those gained by distributing the SRB bridging function between the base Token-Ring LAN switch and the MSS Family Clients. The system can also use the two clients to separate the routing and bridging functions performed by the MSS Family Clients.

One Hop Routing Model

In the preceding sections, the MSS Family Clients have been described as having enhanced bridging or routing support for traffic management. There is also a third model that you can configure on the MSS Family Clients which makes use of bridging and routing functions. This model is known as One Hop Routing and makes use of the MSS Family Client’s hardware speeds for bridging and broadcast scope management through routing. In general, going between two LAN segments through a bridge is faster than going through a router; however, broadcast and multicast traffic traverses every device in the bridge model. Routing limits the broadcast scope of traffic, but imposes delays. These two models can be seen in Figure 4 on page 9.

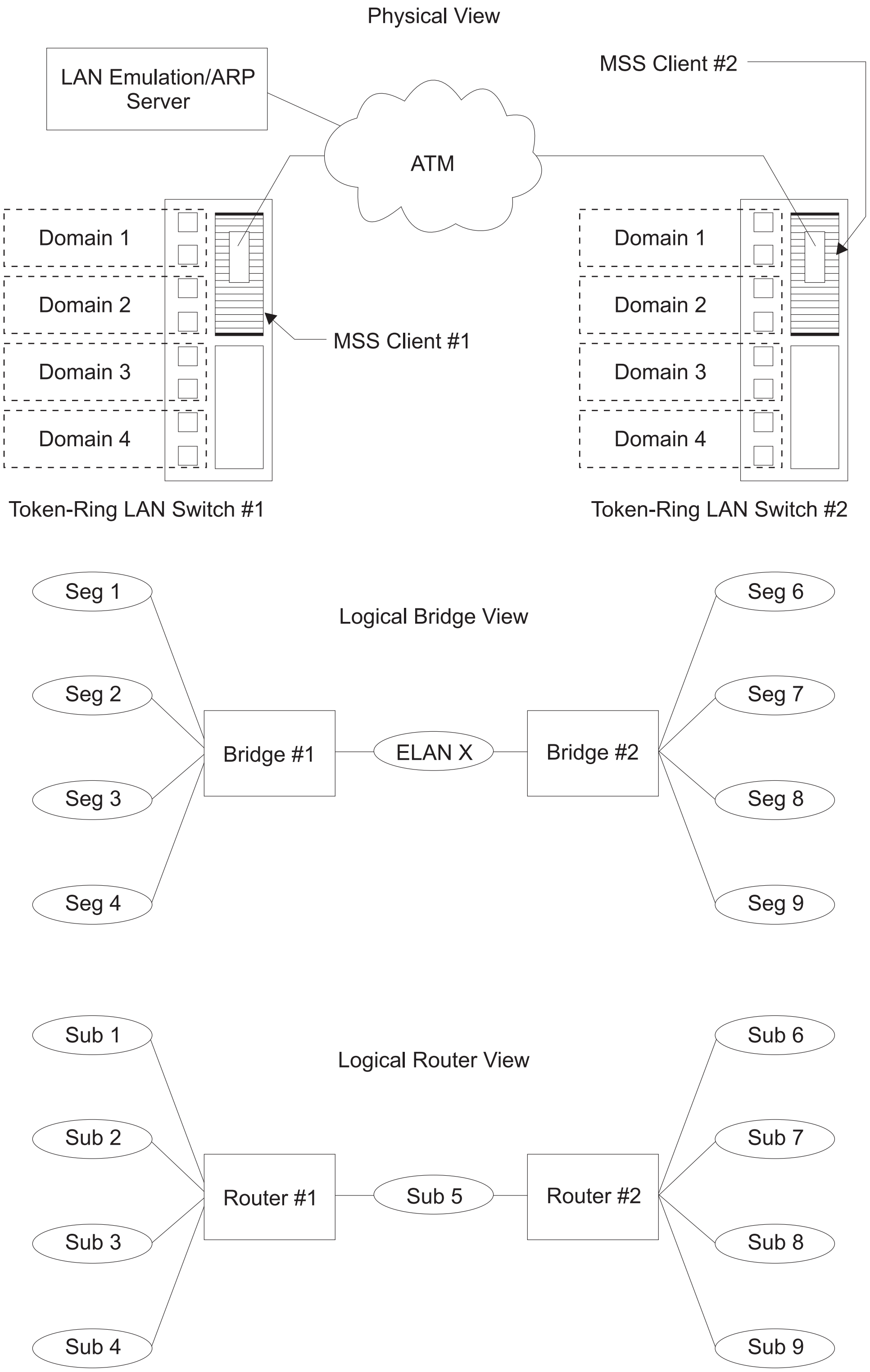


Figure 4. Standard Bridge/Router Models

Because the bridging and routing models have limitations, the MSS Family Clients, combined with the base Token-Ring LAN switch, provides several One Hop Routing solutions that route all outbound traffic and bridge all inbound traffic. This third model, depicted in Figure 5 on page 10, takes advantage of LAN Emulation to create a separate ELAN for managing traffic on each bridge network segment and the ability to route and bridge traffic to the same domain.

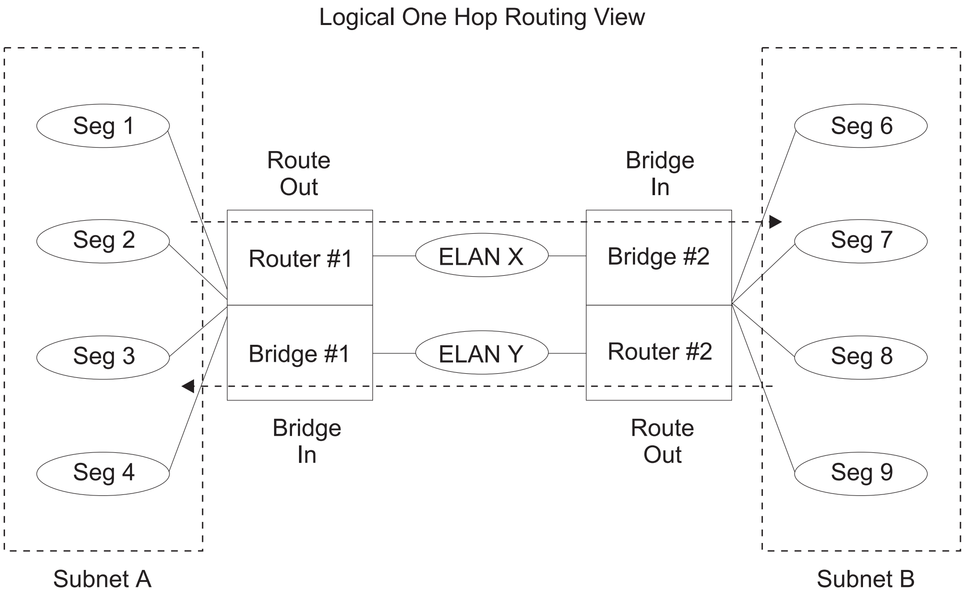


Figure 5. MSS Family Client One Hop Routing Model

When a source on Subnet A needs to forward data to a destination on Subnet B, Router #1 routes to ELAN X, and Bridge #2 has an interface on ELAN X. Because the data is routed when it leaves Subnet A and bridged in by the hardware to Subnet B, the term One Hop Routing is used to describe the flow. Once Bridge #2 receives the data, it forwards the data to the bridged network of Subnet B. In the reverse path, data traveling from Subnet B to ELAN Y is routed, and Bridge #1 has an interface on ELAN Y. Bridge #1 forwards the data to the bridged network of Subnet A. This transmission creates a One Hop Routing environment between multiple subnets while limiting the scope of broadcast traffic, thereby taking advantage of faster bridging speeds, and protecting the high-speed backbone’s bandwidth.

The One Hop Routing model also has several performance advantages from the system’s viewpoint. Because all outbound traffic is bridged to a separate ELAN than the inbound traffic, the system can process twice as many packets because the path between Subnet A and Subnet B is full duplex.

There are three methods of performing One Hop Routing with the MSS Family Clients in a Token-Ring LAN switch. The first method is to configure the ELANs and routing interfaces on the MSS Client or use the MSS Domain Client and the ATM UFC. The second method is to use the MSS Client and the NHRP feature. The third method is to use the MSS Client and the MPOA feature. Although each method is different, the same fundamental One Hop Routing procedure is used.

Before You Begin

Before you begin, refer to the following checklist to verify that your router is installed correctly.

HAVE YOU...

- Installed all necessary hardware?
- Connected to the LAN switch console?
- The latest software? Make sure to check the World Wide Web to see if the software you received has been updated (http://www.networking.ibm.com/nes/neshome.html).

For more information on any of these procedures, refer to the *IBM Multiprotocol Switched Services Family Client Installation and Initial Configuration Guide*.

Features Supported by the MSS Client and MSS Domain Client

Table 1 shows what interfaces, protocols, and services are supported by the MSS Client and the MSS Domain Client. Use this list to determine what information in this book applies to your MSS Family Client

Table 1. Interfaces, Protocols, and Services Supported by MSS Client and MSS Domain Client

Feature	MSS Client	MSS Domain Client
Interfaces		
Token-Ring LAN Emulation client	yes	no
Ethernet LAN Emulation Client	yes	no
Token-Ring Proxy LAN Emulation Client	yes	no
LAN Switch Token-Ring interface	yes	yes
LAN Switch Ethernet interface	no	yes
FasTR over ATM	yes	no
Protocols and Features		
Classical IP	yes	no
IP	yes	yes
Banyan VINES	yes	yes
AppleTalk	yes	yes
IPX	yes	yes
Source-Route Bridging	yes (on Token-Ring only)	yes (on Token-Ring only)
NHRP	yes	no
LAN Network Manager	yes	yes
MPOA	yes	no
PVLAN	yes (on Token-Ring only)	yes (on Token-Ring only)
CIP ARP Server Redundancy	yes	no
QoS LAN Emulation Client	yes	no
MARS Client	yes	no

Table 1. Interfaces, Protocols, and Services Supported by MSS Client and MSS Domain Client (continued)

Feature	MSS Client	MSS Domain Client
OSPF/MOSPF	yes	yes
RIP	yes	yes
RIP2	yes	yes
DVMRP	yes	yes
BGP	yes	yes

Accessing the Software Using Local and Remote Consoles

The router console lets you use the router user interface to monitor and change the function of the router’s networking software (IBM Multiprotocol Switched Services Family Client). The router supports local and remote consoles.

Local Consoles

Local consoles are either directly connected or connected via modems to the LAN Switch. You then need to select either “Non-Token-Ring Ports” or “Non-Ethernet Ports” (depending on your LAN Switch) to access the IBM MSS Family Client software.You may need to use a local console during the initial software installation. After the initial setup connection, you can connect directly to the router using Telnet, as long as IP forwarding has been enabled. (Refer to *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for more information on enabling IP forwarding.)

When the configured router is started for the first time, a boot message appears on the screen, followed by the OPerator's CONsole or OPCON prompt (*). The * prompt indicates that the router is ready to accept OPCON commands.

Once the IBM MSS Family Client is initially configured, you will not need a local console for router operation, as long as IP is enabled on the router.

Remote Consoles

Remote consoles attach to the router using a standard remote terminal protocol. Remote consoles provide the same function as local consoles, except that a local console must be used for initial configuration if your IBM MSS Family Client was not pre-configured at the factory.

Telnet Connections

The router supports both Telnet Client and Server. The remote console on the router acts as a Telnet server. The router acts as a Telnet client when connecting from the router to either another router or a host using the **telnet** command in the OPCON (*) process.

Remote Login Names and Passwords

During a remote login, the router prompts you for a login name and password. You can display the login name when logged in to the router from a remote console by using a router **status** command.

Logging In Remotely or Locally

Logging in to a local console is the same as logging in to a remote console except that you must connect to the router by starting Telnet on your host system. To log in remotely, begin at step 1. To log in locally, begin at step 3.

To log in from a remote console:

1. Connect to the router by starting Telnet on your host system. Your host system is the system to which remote terminals are connected.
2. Supply the router's name or Internet Protocol (IP) address.

   To use router names, your network must have a name server. Issue either the router name or the IP address as shown in the following example:

   ```
   % telnet brandenburg
   ```

   or

   ```
   % telnet 128.185.132.43
   ```

   At this point, it makes no difference whether you have logged in remotely or locally.
3. If you are prompted, enter your login name and password.

   ```
   login:
   Password:
   ```

   It is possible that there is a login and no password. The password controls access to the router. If a password has not been set, press the **Enter** key at the `Password:` prompt. Logins are not set automatically. For security, you can set up user names and passwords using the **add user** command in the CONFIG process. Remember to reload to activate any changes.

   Note: If you do not enter a login name and valid password within 1 minute of the initial prompt, or if you enter an incorrect password three times in succession, the router drops the Telnet connection.
4. Press the **Enter** key to display the asterisk (*) prompt.

   You may have to press the **Enter** key more than once or press **Ctrl-P** to obtain the * prompt.

   Once at this level, you can begin to enter commands from the keyboard. Press the **Backspace** key to delete the last character typed in on the command line. Press the **Delete** key or **Ctrl-U** to delete the whole command line entry so that you can reenter a command. See "Command Completion" on page 33 and "Command History" on page 35 for more information.

   You can also use local Telnet commands on your Telnet client to close the Telnet connection.

   Note: If you use a VT100 terminal, do not press the **Backspace** key, because it inserts invisible characters. Use the **Delete** key.
5. Exit the router as described in "Exiting the Router" on page 14.

Reloading the Router

Use the **reload** command to reboot the device by loading a new copy of the configuration from memory. Whenever you change a user-configurable parameter that is not dynamically configurable, you must reload the device for the change to take effect. For example:

```
* reload

The configuration has been changed, save it? (Yes or [No] or Abort)

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

Exiting the Router

Return to the * prompt and use the **logout** command to close the Telnet connection. For example:

```
    IP Config> exit
    Config> Ctrl-P
    * logout

    %
```

You can also use local Telnet commands on your Telnet client to close the Telnet connection.

Preparing the LAN Switch for an MSS Family Client

Before you can configure an MSS Family Client, you must configure the LAN Switch. Preparing for the MSS Family Clients involves sectioning the LAN switch into domains. This section briefly describes the sequence of events needed to configure the LAN Switch domains correctly. This description is provided only as a reference; for details see the publications for your LAN switch.

Note: The screens in this section are examples only. The screens on your particular LAN Switch may differ.

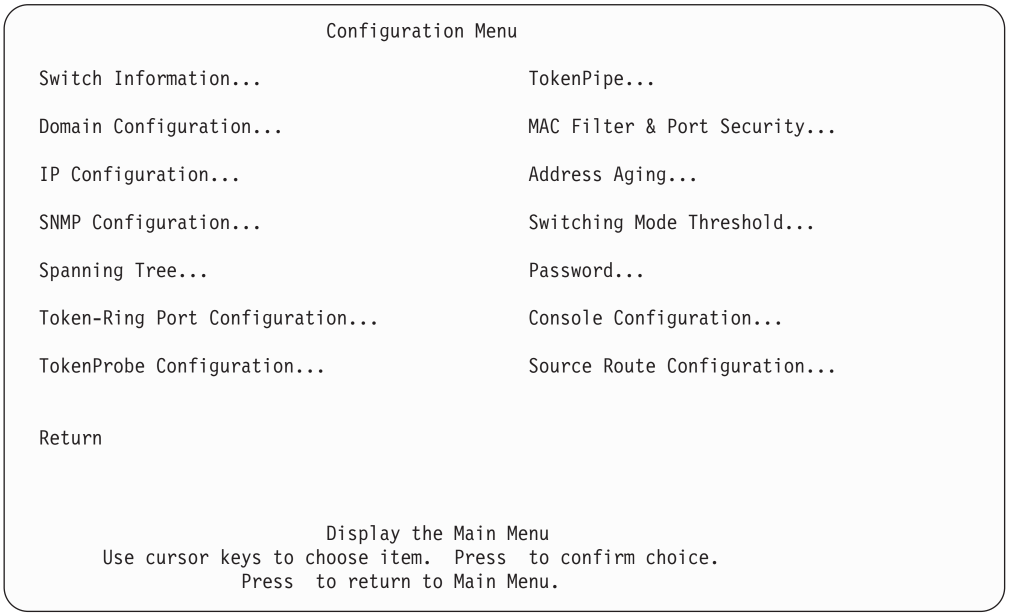
When you first start the LAN Switch, you will see something similar to the following:

```
- Port 1-1  of the MSS Family Client is READY
- Initializing Ports: 1-1
                      5-1  5-2  5-3  5-4  6-1  6-2  6-3  6-4
                      7-1  7-2  7-3  7-4  8-1  8-2  8-3  8-4
- Initializing system address table
- Starting Power Up Diagnostic
  - Downloading Ports:
                        5-1  5-2  5-3  5-4  6-1  6-2  6-3  6-4
                        7-1  7-2  7-3  7-4  8-1  8-2  8-3  8-4
  - UART loopback test on diagnostic port...Passed
  - UART loopback test on console port...Passed
  - Real Time Clock memory test...Passed
  - Real Time Clock test...Passed
  - CPU Port loopback test..............Passed
  - Token Ring Port Loopback Test......................Passed
  - Token Ring Port Cross Port Loopback Test...Passed
  - Token Ring POE test ......................Passed
  - Token Ring Port Broadcast Test...Passed
  - CPU Port Broadcast Test...Passed
- Completing Power Up Diagnostic
- Activating Ports: 1-1
                    5-1  5-2  5-3  5-4  6-1  6-2  6-3  6-4
                    7-1  7-2  7-3  7-4  8-1  8-2  8-3  8-4

- Activating IP
- IBM 8270 Nways Token-Ring LAN Switch Model 800 initiating bootp requests on one
  or more domains
- System initialization complete

Press ENTER key to activate console...
```

When you press **Enter** you will see:

```
                  IBM 8270 Nways Token-Ring LAN Switch Model 800

            (c) Copyright International Business Machines Corporation
                   and others, 1995 - 1997 All rights reserved.


            Switch Base MAC Address:   000629 2205A0

            System Contact:

         A later level of 8270 microcode may be available electronically.
           Consult the current Release Notes for detailed instructions.

             Type Password, then press :


            -- No password has been set, press  to continue. --
```

When you enter a password (or press enter if no password is defined), you will see the LAN Switch Main Menu. To configure the domains on the LAN switch, select **Configuration** from the menu. You should then see the configuration menu as follows:



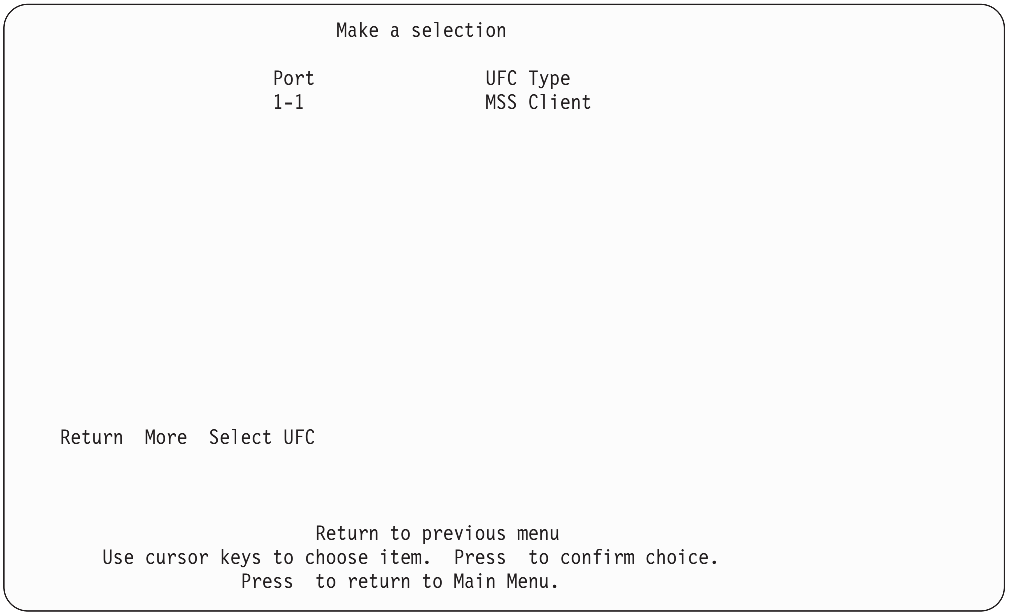
```
                              Configuration Menu

   Switch Information...                          TokenPipe...

   Domain Configuration...                        MAC Filter & Port Security...

   IP Configuration...                            Address Aging...

   SNMP Configuration...                          Switching Mode Threshold...

   Spanning Tree...                               Password...

   Token-Ring Port Configuration...               Console Configuration...

   TokenProbe Configuration...                    Source Route Configuration...


   Return



                              Display the Main Menu
         Use cursor keys to choose item.  Press  to confirm choice.
                      Press  to return to Main Menu.
```

The ports on the LAN switch must be organized into domains. To configure the domains, select **Domain Configuration**. The default domain is domain 0. Configure a domain for each LAN segment in your network. The MSS Family Clients will have interfaces on each of the domains, so record the domain information.

You are now ready to perform the initial configuration of the MSS Family Client.

Accessing the MSS Family Client Software from the LAN Switch

To access the MSS Family Client software from the LAN Switch, select Non-Token-Ring Ports or Non-Ethernet Ports from the LAN Switch main menu. You should see something similar to the following:



```
                               Make a selection

                         Port                UFC Type
                         1-1                 MSS Client
















     Return  More  Select UFC




                              Return to previous menu
         Use cursor keys to choose item.  Press  to confirm choice.
                      Press  to return to Main Menu.
```

When you select **MSS Client** from this menu, you should see the following messages:

```
Please press the space bar once to obtain the console.
Console granted to this interface.
Please type "return" at the MOS Operator Console
prompt (*) or enter Ctrl-b to exit console.

Copyright Notices:

Licensed Materials - Property of IBM
MSS Client
(C) Copyright IBM Corp. 1998
All Rights Reserved. US Gov. Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.


MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

*
```

You can now configure the MSS Family Client. See “Accessing the Network Interface Configuration Process” on page 28 for a sample configuration procedure.

Discussing the User Interface System

The software (IBM Multiprotocol Switched Services Family Client) is a multitasking system that schedules use of the CPU among various processes and hardware devices. The router software:

- Provides timing and memory management, and supports both local and remote operator consoles from which you can view and modify the router’s operational parameters.
- Consists of functional modules that include various user interface processes, all network interface drivers, and all protocol forwarders purchased with the router.

Understanding the First-Level User Interface

The user interface to the software consists of the main menu (process) and several subsidiary menus (processes). These menus are related to the multiple levels of processes in the software.

The first level of processes consists of the OPCON and CONFIG-ONLY processes. In most cases, you will use the OPCON process to access the second level to configure or operate the base services, features, interfaces, and protocols you will run on your IBM MSS Family Client.

The second level contains processes such as Configuration (CONFIG), Console (GWCON) and Event Logging System (MONITR). You may use the OPCON commands **configuration**, **console** or **event** to access these second level processes. Alternatively, you may use the **status** command to list the second level processes and then use the **talk** *pid* command to access the second-level processes. There are processes that you cannot use in the software. See Table 2 on page 22 for an overview of the processes.

Figure 6 on page 18 shows the processes and how they fit within the structure of the router software.

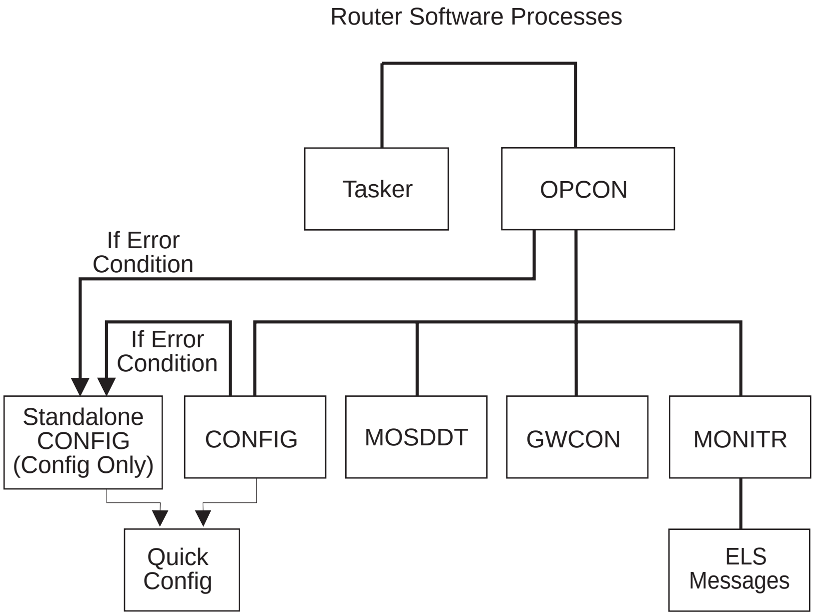


Figure 6. IBM Multiprotocol Switched Services Family Client

Figure 7 is an example of the relationship between the various process levels.

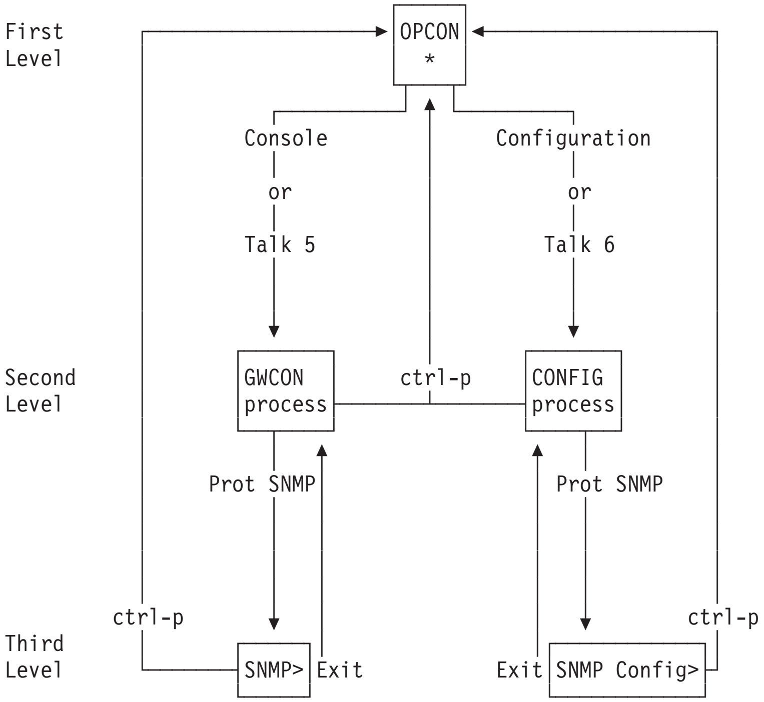


Figure 7. Relationship of Processes and Commands

Note: Also shown in Figure 7 are the various commands to access each process level and return from each process level.

See “What is the OPCON Process?” on page 69 for more information about OPCON, and “Config-Only Mode” on page 81 for more information about CONFIG-ONLY.

The ROPCON process handles processing from remote consoles and is essentially the same as the OPCON process.

Quick Configuration Process

Quick Configuration, or Quick Config, allows you to quickly configure portions of the router without dealing with the specific operating system commands. When you initially load or the router with no configuration, you enter Config-Only and you can access Quick Config menus from that process. If the router has devices configured and the devices do not have any protocols configured, the router automatically starts Config-Only and then enters Quick Config.

You can also enter Quick Config from the CONFIG process using the **qconfig** command.

System Security

Multiple users with login permissions can be added using the **add user** command. See “Configuring User Access” on page 83 for details on security issues and for information on the **set password** and **add user** commands.

Chapter 2. Using the Software

This chapter describes how to use the software. It consists of:

- “Entering Commands”
- “Connecting to a Process”
- “Some Configuration Suggestions” on page 23
- “Accessing the Second-Level Processes” on page 26
- “Accessing the Third-Level Processes” on page 28
- “Command Completion” on page 33
- “Command History” on page 35

Entering Commands

When typing a command, remember the following:

- You may type only enough sequential letters of the command to make it unique among the available commands. For example, to execute the **reload** command you must enter **rel** as a minimum. The minimum number of required characters are underlined in the command syntax chapters.
- Commands are not case-sensitive.
- Sometimes, only the first letter of the command (and subsequent options) is required to execute the command. For example, typing **s** at the * prompt followed by pressing the **Enter** key causes the **status** command to be executed.
- You may type **Escape ?** to obtain help on entering commands. See “Command Completion” on page 33 and “Command History” on page 35 for more information.

Connecting to a Process

When you start the router, the console displays a boot message. The OPCON prompt (*) then appears on the screen indicating that you are in the OPCON process and you can begin entering OPCON commands. This is the command prompt from which you communicate with different processes.

Commands that are needed more often appear before the “- - - - -” separator. Enter the appropriate command at the OPCON prompt (*). See Table 5 on page 70 for a list of commands.

Alternatively, you can:

1. Find out the process ID (PID) number of a process by entering the **status** command at the * prompt.

   The **status** command displays information about the router processes, such as the process IDs (PIDs), process names and status of the process. Issuing the **status** command is shown in the following example:

   ```
   * status
   Pid  Name      Status TTY  Comments
   1    COpCON    RDY    TTY0
   2    Monitr    DET     --
   3    Tasker    RDY     --
   ```

```
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELScon    DET     --
8    ROpCon    IDL    TTY1 128.185.210.125
9    ROpCon    IDL    TTY2
10   WEBCon    IDL     --
```

2. Use the **talk** *pid* command, where *pid* is the number of the process to which you want to connect. (For more information about these and other OPCON commands, refer to "What is the OPCON Process?" on page 69.)

   Note: Not every process listed has a user interface (for example, the **talk 3** process). The **talk 4** command is for use by IBM service representatives.

Identifying Prompts

Each process uses a different prompt. You can tell which process your console is connected to by looking at the prompt. (If the prompt does not appear when you enter the **talk** *pid* command, press **Enter** again.)

The following list shows the prompts for the five main processes:

Table 2. Processes, Their Purpose, and Commands to Access

Process	Level and Purpose	Command to Access	Input Prompt
OPCON	Level 1 - access to all secondary levels	**Ctrl-P**	asterisk (*)
CONFIG	Level 2 - base services configuration and access to configuration third level	**Configuration or talk 6**	Config >
GWCON	Level 2 - base services operation and monitoring and access to operations and monitoring on third level	**Console or talk 5**	plus sign (+)
MONITR	level 2 - message display	**Event or talk 2**	(none)
ELSCon	level 2 - direct monitoring and access to ELS console	**els or talk 7**	ELS Secondary Console>
MOSDBG	level 2 - diagnostic environment	**talk 4**	db>
Note: Only enter the **talk 4** command under the direction of a service representative.			

At the OPCON prompt level, you can begin to enter commands from the keyboard. Use the **Backspace** key to delete the last character typed in on the command line. Use **Ctrl-U** to delete the whole command line entry so that you can reenter a command. See "Command Completion" on page 33 and"Command History" on page 35 for additional details or press **Escape ?**.

Getting Help

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

```
*?
        CONFIGURATION         (Talk 6)
        CONSOLE                 (Talk 5)
        EVENT Logging System  (Talk 2)
        ELS Console              (Talk 7)
        LOGOUT
        PING (IP-Address)
        RELOAD
        RESTART
        TELNET to IP-Address (this terminal type)
-----------------------------------------------
        DIVERT output from process
        FLUSH output from process
        HALT output from process
        INTERCEPT character is
        MEMORY statistics
        STATUS of Processes(es)
        TALK to process
(you may cycle through these commands by pressing the TAB key)
```

Exiting a Lower Level Environment

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

For example, to exit the IP protocol configuration process:

```
IP config> exit
Config>
```

If you need to get to the primary level (OPCON), enter the intercept character (**Ctrl P** by default).

Getting Back to OPCON

To get back to the OPCON prompt (*), press **Ctrl-P**. You must always return to OPCON before you can communicate with another process. For example, if you are connected to the console (GWCON) process and you want to connect to the CONFIG process, you must press **Ctrl-P** to return to OPCON first. The **Ctrl-P** key combination is the default *intercept character*.

If you use the intercept character from a third-level or lower level menu to return to the * prompt, the next time you use the **talk** command to talk to the same process, you will reenter that same level menu. This link goes away when the router is re-initialized.

Getting to the LAN Switch Software

To return to the LAN Switch console to perform any of the functions provided by the LAN Switch, press **Ctrl-B** or enter **return** from the OPCON (*) prompt.

Some Configuration Suggestions

Configuring a MSS Family Client is different depending on whether you are configuring for the first time, creating a configuration based on an existing configuration, or just updating a configuration. Use the following sections as a guide to the best procedure to use, depending on your needs.

Creating a First Configuration

This procedure assumes that you have no other MSS Family Client that contains a configuration similar to the one for the MSS Family Client you are configuring. The procedure also assumes that you are configuring the MSS Family Client for the first time. Although this procedure specifies an order, you can perform the actual configuration (after step 4) in any order.

To configure a IBM MSS Family Client for the first time:

1. Install the MSS Family Client into the LAN switch. See *Multiprotocol Switched Services Client Universal Feature Card Planning and Installation*, GA27-4170 for the MSS Client and *Multiprotocol Switched Services Domain Client Universal Feature Card Planning and Installation*, GA24-4171 for the MSS Domain Client for the installation procedures.
2. Configure the domains on the LAN switch.
3. Connect to the MSS Family Client as described in “Accessing the Software Using Local and Remote Consoles” on page 12.
4. Initially configure a port on the MSS Family Client and at least an internal IP address for the device using Quick Config as described in “Quick Configuration” on page 82 or “Appendix A. Quick Configuration Reference” on page 329. Configure the minimum needed to allow you to Telnet into the device.
5. Configure any base services, such as boot options. Access the configuration process as described in “Accessing the Configuration Process, CONFIG (Talk 6)” on page 26.
6. Configure the interfaces. Access the interface configuration process as described in “Accessing the Network Interface Configuration Process” on page 28.
7. Configure any required features. Access the feature configuration process as described in “Accessing Feature Configuration and Operating Processes” on page 31.
8. Configure any protocols that will run through this device. Access the protocol configuration process as described in “Accessing Protocol Configuration and Operating Processes” on page 31.

   Note: At the very least, you will configure IP in this step.
9. Reload the router as described in “Reloading the Router” on page 14.

Basing a Configuration on an Existing Configuration

This section describes how to:

- Base a configuration on the configuration in an operating MSS Family Client
- Permanently update the configuration in a MSS Family Client
- Temporarily update the configuration of a MSS Family Client while the MSS Family Client is operating

Basing on an Existing Configuration

If you already have a MSS Family Client that has the same interfaces, features, and protocols that you want to configure on a new MSS Family Client, you can save time by basing the configuration on the existing MSS Family Client. You can perform this type of configuration either using the command line interface or by using the configuration program that comes with the MSS Family Client. In both cases, the procedures assume that the MSS Family Client is not in your production network.

To base a configuration on an existing configuration using the command line interface:

1. Obtain a copy of the configuration you want to use.
   a. Enter **talk 6** at the OPCON (*) prompt.
   b. Enter **boot** at the `Config>` prompt.
   c. Enter the **tftp put configuration** *file* command at the `Boot config>` prompt. See “Chapter 8. Using BOOT Config to Perform Change Management” on page 105 for more information.
2. Connect to the MSS Family Client that you are configuring.
3. Load the configuration you obtained in step 1 into the MSS Family Client using TFTP GET. See “Chapter 8. Using BOOT Config to Perform Change Management” on page 105.
4. Update the configuration.
5. Write the configuration. See “What is CONFIG?” on page 81.
6. Reload the MSS Family Client.

To base a configuration on an existing configuration using the configuration program:

1. Start the configuration program.
2. Retrieve the configuration from the MSS Family Client on which you want to base the new configuration.
3. Make the changes you need for the new configuration. These changes include addresses, the host names, users, and other items.
4. Save the configuration with a different name from the name that you used to retrieve the configuration.
5. Send the configuration to the MSS Family Client you are configuring.
6. Reload the MSS Family Client.

For more about using the configuration program, see *IBM Multiprotocol Switched Services Client Configuration Program User’s Guide for Nways Multiprotocol and Access Services Products* GC30-3830.

Permanently Updating a Configuration

To permanently update a configuration:

1. Access the MSS Family Client you are updating as described in “Accessing the Software Using Local and Remote Consoles” on page 12. You will see the `*` prompt.
2. Enter the **talk 6** command to access the configuration process.
3. Enter the appropriate commands to access the third-level process that configures the areas that you are changing.
4. Enter **exit** as many times as needed to return to the configuration process.
5. Write the configuration. See “What is CONFIG?” on page 81.
6. Reload the MSS Family Client.

Temporarily Updating a Configuration

The ability to temporarily update a configuration allows you to make changes to some of the operating characteristics of a MSS Family Client until you can make permanent updates to the configuration. This enables you to implement changes immediately to resolve problems or improve performance and avoid an outage during a peak period. You can then make permanent updates to the configuration and schedule an outage so you can reload to pick up the change.

To temporarily update a configuration:

1. Access the MSS Family Client you are updating as described in “Accessing the Software Using Local and Remote Consoles” on page 12. You will see the `*` prompt.
2. Enter the **talk 5** command to access the operating/monitoring process.

   Note: Not all interface types, protocols, or features allow you to make temporary config changes via talk 5 commands.
3. Enter the appropriate commands to access the third-level process that monitors the areas that you are changing.
4. Enter **exit** as many times as needed to return to the operating/monitoring process.
5. Enter **Ctrl-P** to return to the `*` prompt.
6. Exit the router as described in “Exiting the Router” on page 14

Accessing the Second-Level Processes

All interfaces, features, and protocols have commands that you use to access the following processes:

- The configuration process to initially configure and enable the interface, feature, or protocol, as well as perform later configuration changes.
- The operating/monitoring process to display information about each interface, feature, or protocol, to make temporary configuration changes, or to activate configuration changes.

You can also configure or operate some base system services through the second-level processes. The commands to perform these functions are described starting in “What is CONFIG?” on page 81.

The next sections describe the procedures for accessing the second-level processes.

Accessing the Configuration Process, CONFIG (Talk 6)

Each protocol configuration process is accessed through the router’s CONFIG process. CONFIG is the second-level process of the router user interface that lets you communicate with third-level processes. Protocol processes are examples of third-level processes.

The CONFIG command interface is made up of levels of menus. Protocol configuration command interfaces are menus within the CONFIG interface. Each protocol configuration interface has its own prompt. For example, the prompt for the SNMP protocol command interface is `SNMP config>`.

The next sections describe these procedures in more detail.

Entering the CONFIG Process

To enter the CONFIG process from OPCON and obtain the CONFIG prompt, enter the **configuration** command. Alternatively, you can enter the OPCON **talk** command and the PID for CONFIG. The PID for CONFIG is 6.

```
* configuration
```

or

```
* talk 6
```

The console displays the CONFIG prompt (`Config>`). If the prompt does not appear, press the **Enter** key again.

Quick Configuration Process: Quick Configuration, or Quick Config, allows you to quickly configure portions of the router without dealing with the specific operating system commands. You enter the Quick Config menus from the CONFIG process using the **qconfig** command (see “Quick Configuration” on page 82).

Reloading the Router

Changes that you make to the protocol parameters through CONFIG do not take effect until you either activate the net that contains any dynamic changes or the router software.

Accessing the Console Operating/Monitoring Process, GWCON (Talk 5)

To view information about the interfaces, features, or protocols or to change parameters while running, you must access and use the operating (monitoring) process. Operating command interfaces are modes of the GWCON interface. Within the GWCON mode, each interface, feature, or protocol interface has its own prompt. For example, the prompt for the SNMP protocol is `SNMP>`.

Note: Any parameters you change in this process will not remain active across any event that causes the MSS Family Client to reload the operational code, such as a power outage or entering the **reload** command.

The next sections describe these procedures in more detail.

Entering the GWCON Command Process

To enter the GWCON process from OPCON and obtain the GWCON prompt, enter the **console** command. Alternatively, you may enter the **talk** command and the PID for GWCON. The PID for GWCON is 5. For example:

```
* console
```

or

```
* talk 5
```

The GWCON prompt (+) then displays on the console. If the prompt does not appear, press **Enter** again.

Accessing the Secondary ELS Console Process, ELSCon (Talk 7)

The Secondary ELS Console provides convenient access to GWCON `talk 5` ELS without disrupting the current state of GWCON. You may be in the middle of a **ping** in `talk 5`, or deep inside a `talk 5` menu structure, and want to control ELS without disrupting the current state of GWCON. The secondary ELS console (Talk 7) serves this purpose.

To enter the Secondary ELS Console (ELScon) process from OPCON and obtain the Secondary ELS Console prompt, enter the **els** command. Alternatively, you may enter the **talk 7** command.

In the following example, another ELS event is displayed while performing a **ping** command.

Note: The intercept character (Ctrl-P by default) is used to obtain the OPCON prompt (*).

```
*talk 5
+protocol ip
IP>ping 10.0.0.9
PING 10.0.0.2 -> 10.0.0.9: 56 data bytes, ttl=64, every 1 sec.

*talk 7

ELS Secondary Console>display event ip.7
Complete
ELS Secondary Console>
*talk 2
00:20:48   IP.007: 10.0.0.2 -> 10.0.0.9
00:20:49   IP.007: 10.0.0.2 -> 10.0.0.9
```

Accessing the Third-Level Processes

After accessing the second level, you must enter commands on the third level to configure or operate the interfaces, features, and protocols in your IBM MSS Family Client. The following sections describe how to access the third level processes.

Accessing Network Interface Configuration and Operating Processes

This section describes how to get started with accessing the network interface configuration and operating processes. Accessing these processes lets you change and monitor software-configurable parameters for network interfaces used in your router.

Accessing the Network Interface Configuration Process

Use the following procedure to access the router's configuration process. This process gives you access to a specific interface's configuration process.

1. At the OPCON prompt, enter the **configuration** command.

   ```
   client0 * configuration
   ```

   After you enter the **configuration** command, the CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter **CONFIG**, press **Enter** again.

2. Use the **add device** command to create a network interface for each port on the MSS Family Client. The **add device** command automatically assigns the interface number. To determine the device types supported by the MSS Family Client, enter **add device ?** command.

   ```
   client0 Config>add dev tok
   Device Domain #(0-15) [0]?
   Adding Token Ring device in domain 0 as interface #1
   Use "net 1" to configure Token Ring parameters
   client0 Config>add dev tok
   Device Domain #(0-15) [0]? 1
   Adding Token Ring device in domain 1 as interface #2
   Use "net 2" to configure Token Ring parameters
   ```

3. Configure the IP protocol for each device.

   ```
   client0 Config>p ip
   Internet protocol user configuration
   IP config>add address
   Which net is this address for [0]? 1
   New address []? 1.1.1.1
   Address mask [255.0.0.0]? 255.255.255.0
   IP config>add address
   Which net is this address for [0]? 2
   New address []? 2.2.2.2
   Address mask [255.0.0.0]? 255.255.255.0
   IP config>ex
   ```

4. Write the new configuration to memory.

   ```
   client0 Config>write
   Config Save: Using bank F and config number 1
   Writing config #1 starting at sector 0 (00000000)
   Erasing sector 1
   Writing data to FLASH
   Writing 64k block starting at 0x00000000
   client0 Config>
   ```

5. At the `Config>` prompt, enter the **list devices** command to display the network interface numbers for which the MSS Family Client is currently configured.
6. Record the interface numbers.
7. Enter the CONFIG **network** command and the number of the interface you want to configure. For example:

   ```
   client0 Config> network 1
   ```

   The appropriate configuration prompt, now displays on the console.

   Note: Not all network interfaces are user-configurable. For interfaces that cannot be configured, you receive the message:

   ```
   That network is not configurable
   ```

8. Enter **Ctrl-B** to return to the LAN Switch menus.

MSS Family Client Restrictions: The following rules apply when adding devices to the MSS Family Client:

- Only one physical ATM interface may be defined on the MSS Client.
- Adding an MSS Client in a LAN Switch will disable the next higher slot in the pair. For example, if you add an MSS Client into an IBM 8270 model 800 slot 4, slot 5 will be disabled. Likewise, if you add the MSS Client to slot 3, slot 4 will be disabled.
- If your base LAN Switch is a Token-Ring switch, you cannot configure an Ethernet device to a MSS Family Client. Likewise, if your base LAN Switch is an Ethernet switch, you cannot configure a token-ring device. See “Accessing the Network Interface Configuration Process” on page 28.

Configuring the Network Interface: Refer to the specific chapters in this guide for complete information on configuring your IBM MSS Family Client's network interfaces.

The MSS Client supports a 155 Mbps ATM interface.

Accessing the Network Interface Console Process

To monitor information related to a specific interface, access the interface console process by using the following procedure:

1. At the OPCON prompt, enter the **console** command . For example:

   ```
   * console
   ```

2. The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Enter** again.
3. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the router is configured. For example:

   ```
   + configuration

   IBM Nways Multiprotocol Switching Server
   Host name: MSS Client
   Version: MSSC Feature 0 V2.1 Mod 0 PTF 0 RPQ 0

   Num Name  Protocol
   0   IP     DOD-IP
   3   ARP    Address Resolution
   7   IPX    NetWare IPX
   11  SNMP   Simple Network Management Protocol
   12  OSPF   Open SPF-Based Routing Protocol
   23  ASRT   Adaptive Source Routing Transparent Enhanced Bridge
   25  LNM    LAN Network Manager
   29  NHRP   Next Hop Resolution Protocol

   Num Name  Feature
   2   MCF    MAC Filtering
   6   QOS    Quality of Service

   9 Networks:
   Net Interface  MAC/Data-Link        Hardware                     State
   0   ATM/0      ATM                  ATM                          Up
   1   NHRPL/0    NHRP LANE Shortcut   ATM                          Up
   2   TKR/0      Token-Ring/802.5     Token-Ring                   Up
   3   TKR/1      Token-Ring/802.5     Token-Ring                   Up
   4   TKR/2      Token-Ring/802.5     Token-Ring                   Up
   5   TKR/3      Token-Ring/802.5     Token-Ring                   Up
   6   TKR/4      Token-Ring/802.5     ATM                          Up
   7   TKR/5      Token-Ring/802.5     ATM                          Up
   8   ATM/1      ATM                  Virtual ATM interface        Up
   ```

4. Enter the GWCON **network** command and the number of the interface you want to monitor. For example:

   ```
    + network 0
   ATM>
   ```

   In this example, the ATM console prompt is displayed on the console. You can then view information about the ATM interface by entering the ATM console commands.

Monitoring the Network Interface: Refer to the specific chapters in this manual for complete information on monitoring your IBM MSS Family Client's network interfaces.

Accessing Feature Configuration and Operating Processes

To help you access the IBM Multiprotocol Switched Services Family Client feature configuration and operating processes, this section outlines both of these procedures.

Accessing the Feature Processes

Use the **feature** command from the CONFIG process to access configuration commands for specific IBM Multiprotocol Switched Services Family Client features outside of the protocol and network interface configuration processes.

Use the **feature** command from the GWCON process to access console commands for specific features that are outside of the protocol and network interface console processes.

Enter a question mark after the **feature** command to display a listing of the features available for your software release. For example:

```
Config> feature ?

QOS
MCF

Feature name or number [2] ?
```

To access a particular feature's configuration or operating prompt, enter the **feature** command at the `Config>` or + (GWCON) prompt, respectively, followed by the feature number or short name. For example:

```
Config> feature mcf

MAC filtering user configuration

Filter Config>
```

Table 8 on page 95 lists the available feature numbers and names.

Once you access the configuration or operating prompt for a feature, you can begin entering specific commands for the feature. To return to the previous prompt level, enter the **exit** command at the feature's prompt.

Accessing Protocol Configuration and Operating Processes

This section describes how to access the protocol configuration and operating processes.

Entering a Protocol Configuration Process

To enter the desired protocol configuration process from the `CONFIG>` prompt:

1. At the `CONFIG>` prompt, enter the **list configuration** command to see the numbers and names of the protocols purchased in your copy of the software. See page 96 for sample output of the **list configuration** command.
2. From the `Config>` prompt, enter the **protocol** command with the number or short name (for example, SNMP) of the protocol you want to configure. The protocol number and short name is obtained from the **list configuration** command display. In the following example, the command has been entered for accessing the SNMP protocol configuration process:

   ```
   Config> protocol SNMP
   ```

or

```
Config> protocol 11
SNMP user configuration
```

The protocol configuration prompt then displays on the console. The following example shows the SNMP protocol configuration prompt:

```
SNMP config>
```

You can now begin entering the protocol’s configuration commands. See the corresponding protocol section of the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for more information on specific protocol configuration commands.

In summary, the **protocol** command lets you enter the configuration process for the protocol software installed in your router. The **protocol** command enters a protocol’s command process. After entering the protocol command, the prompt of the specified protocol appears. From the prompt, you can enter commands specific to that protocol.

Entering a Protocol Operating Process

To enter a protocol console process from the GWCON prompt:

1. At the GWCON prompt, enter the **configuration** command to see the protocols and networks configured for the router. For example:

   ```
   +configuration

   IBM Nways Multiprotocol Switching Server
   Host name: MSS Client
   Version: MSSC Feature 0 V2.1 Mod 0 PTF 0 RPQ 0

   Num Name  Protocol
   0   IP     DOD-IP
   3   ARP    Address Resolution
   7   IPX    NetWare IPX
   11  SNMP   Simple Network Management Protocol
   12  OSPF   Open SPF-Based Routing Protocol
   23  ASRT   Adaptive Source Routing Transparent Enhanced Bridge
   25  LNM    LAN Network Manager
   29  NHRP   Next Hop Resolution Protocol

   Num Name  Feature
   2   MCF    MAC Filtering
   6   QOS    Quality of Service

   9 Networks:
   Net Interface  MAC/Data-Link         Hardware                       State
   0   ATM/0      ATM                   ATM                            Up
   1   NHRPL/0    NHRP LANE Shortcut    ATM                            Up
   2   TKR/0      Token-Ring/802.5      Token-Ring                     Up
   3   TKR/1      Token-Ring/802.5      Token-Ring                     Up
   4   TKR/2      Token-Ring/802.5      Token-Ring                     Up
   5   TKR/3      Token-Ring/802.5      Token-Ring                     Up
   6   TKR/4      Token-Ring/802.5      ATM                            Up
   7   TKR/5      Token-Ring/802.5      ATM                            Up
   8   ATM/1      ATM                   Virtual ATM interface          Up
   ```

2. Enter the GWCON **protocol** command with the protocol number or short name of the desired protocol displayed in the configuration information.

   In the following example, the command has been entered for accessing the SNMP protocol console process.

   ```
   + protocol 11
   ```

   or

   ```
   + protocol SNMP
   ```

The protocol console prompt then displays on the console. This example shows the SNMP protocol console prompt:

```
SNMP>
```

You can now begin entering the protocol's commands. See the corresponding protocol section of the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for more information on specific protocol console commands.

Command Completion

The automatic command completion function assists you with the syntax for commands entered at the command line.

To illustrate the behavior of Command Completion, assume that the following commands are allowed in a given menu context. (This is an example menu only.)

enable	
	auto-refresh
	caching
set	cache-size
	cache-timeout
	priority

- If you type **ena** and hit the Space Bar, the full command is shown as **ENABLE**. If you now type **?**, a list of possible items to enable are shown (**auto-refresh** and **caching**) and the command **ENABLE** remains on the command line.
- If you type **ena** and press **Enter**, a message is printed that the command is not fully specified, and a list of possible items to enable are shown (**auto-refresh** and **caching**) and the command **ENABLE** remains on the command line.
- Since the **ENABLE** command requires an item to enable, it appears in a list of possible command completions with "**...**" in the left margin to indicate that more input is required for the command.
- If your input matches multiple commands, a list of possible completions is displayed. Your input on the new command line is expanded to the longest common prefix. For example, if you enter **set ca**, and then press the space bar, **CACHE-SIZE** and **CACHE-TIMEOUT** will be listed, and the new command line will be expanded to **SET cache-**, since "cache-" is common to both possible completions. Now you must type the letter "s" or the letter "t" to distinguish between the possible completions ″size″ or ″timeout″.
- Common commands sometimes appear in an alternate form (**SHOW**, **DISPLAY**, **LIST**). If the Command Completion does not yield a match on a common command, such as **SHOW**, the alternatives **DISPLAY** or **LIST** will be displayed, if found.
- If the search for a command (and alternatives) does not yield an exact match, you are presented with a list of possible completions, using some portion of your input. For example, **enanle** followed by the Space Bar would be replaced with **ena** and **ENABLE** would be listed as the possible completion.
- When a list of possible commands is shown, you can use the Tab key to cycle through one command at a time on the current command line. You can use the Space Bar or Enter key to select the command shown.

Online Help When Command Completion is Enabled

The following online help is available when command-completion is enabled.

See 93 for the **enable command-completion** syntax.

? Question mark displays a list of possible completions. A message appears if the command is already complete.

Space bar
Attempts to complete the current word on the command line. If a unique match is not found, possible completions are listed.

Tab Attempts to complete the current word on the command line. If a unique match is not found, possible completions are listed and you may cycle through these possible completions using the Tab key. Use the Space Bar or the Enter key to select the currently displayed command.

Enter Attempts to complete the current word on the command line. If the command is complete, Enter executes the command and stores it in the Command History. If the command is incomplete, a list of possible completions is displayed.

Ctrl-P Returns to the MOS Operator Console prompt (*). (CTL-P is the default Intercept Character.)

Backspace
Deletes the last character on the command line.

Ctrl-W Deletes the last word on the command line.

Ctrl-U Aborts the current command.

Ctrl-L Refreshes the current command line to display its contents.

Ctrl-B Retrieve Backward. Replaces the current command line with the previous command in the circular Command History.

Ctrl-F Retrieve Forward. Replaces the current command line with the next command in the Command History.

Ctrl-R Marks the start of a Repeat Sequence in the Command History. Use with the **Ctrl-N** function.

Ctrl-N Replaces the current command line with the next command in the Repeat Sequence whose starting command was marked with **CTL-R**.

Ctrl-C Cancels Easy-Start, if active.

Escape ?
Escape, followed by “?” prints this Command Line Help:

The following rules apply to automatic command completion:

- Completed commands are shown in UPPERCASE on the command line.
- Common commands sometimes appear in an alternate form (**ADD** versus **CREATE**). If the command completion does not yield a match on a common command, any alternative commands will be displayed.
- If the search for a command (and alternative commands) does not yield a unique match, a list of possible completions is shown, and the longest common prefix is presented.
- When possible completions are listed, commands requiring further command input are shown with “...” in the left margin.

- When a Command History retrieve key (CTL-B,F,N) is pressed, the Command History is scanned for a command that successfully parses in the current command context. A tone will be sounded if no such command exists.
- Some command menus are built dynamically. Command Completion cannot always follow these dynamic links. ’?’ can be entered in these cases.
- To disable Command Completion for just one command (to enter a comment), type any Comment Character as the first character on the command line. The Comment Characters are !@#$%*:;/’″
- Command Completion will be disabled in the event of an internal error. Report the Debug information on the screen to Customer Support.
- Command Completion is currently Enabled. To Disable this option, use the **disable command-completion** command from Configuration `talk 6`.

Online Help When Command Completion is Disabled

The following online help is available when command-completion is disabled:

? When a ’?’ (Question Mark) is entered at the end of the command line, a list of possible completions is shown.

Enter Executes the command and stores it in the Command History. A message is printed if the command is not fully specified

Ctrl-P Returns to the MOS Operator Console prompt (*). (CTL-P is the default Intercept Character.)

Backspace
Deletes the last character on the command line.

Ctrl-U Aborts the current command.

Ctrl-B Retrieve Backward. Replaces the current command line with the previous command in the circular Command History.

Ctrl-F Retrieve Forward. Replaces the current command line with the next command in the Command History.

Ctrl-R Marks the start of a Repeat Sequence in the Command History. Use with the **Ctrl-N** function.

Ctrl-N Replaces the current command line with the next command in the Repeat Sequence whose starting command was marked with **CTL-R**.

Ctrl-C Cancels Easy-Start, if active.

Escape ?
Escape, followed by “?” prints this Command Line Help:

-

```
Command Completion is currently Disabled.  To Enable this option,
use the enable command-completion command from Configuration talk 6.
```

Command History

The Command History contains up to the last 50 commands entered by the user in OPCON, GWCON (Talk 5) or CONFIG (Talk 6) command line menus.

Backward and Forward retrieve keys can be used to recall previously entered commands. In addition, a facility is provided to enable the advanced user to repeat a particular series of commands.

Repeating a Command in the Command History

By pressing **Ctrl -** (backward) or **Ctrl-F** (forward) at any command line prompt in an OPCON, GWCON or CONFIG menu, the current command line is replaced by the previous or next command in the Command History. The Command History is common across the command line interface. That is, a command entered while in a GWCON menu can be retrieved from within CONFIG and a command entered while in a CONFIG menu can be retrieved from within GWCON.

When automatic Commmand Completion is enabled (See"Command Completion" on page 33) and a Command History retrieve key (CTL-B,F,N) is pressed, the Command History is scanned for a command that successfully parses in the current command context. A tone will be sounded if no such command exists.

The Command History contains the most recently entered commands, up to a maximum of the last 50 commands. If only three commands have been entered since a restart, pressing **Ctrl-F** or **Ctrl -** circles through only those three commands. If no commands have been entered thus far, **Ctrl-F** or **Ctrl -** results in tone sound.

Note: A command aborted by pressing **Ctrl-U** will not be entered into the Command History. When Command Completion is enabled, only complete commands are entered into the Command History.

To enter two similar commands:

```
display sub arp
display sub lec
```

Enter:

`display sub arp`, then press **Enter**

Ctrl - for Backward, and the current line is replaced with-

`display sub arp`

Press **Backspace** and replace "arp" with "lec" to get

`display sub lec` and then press **Enter**

Repeating a Series of Commands in the Command History

There is an additional feature for advanced users to facilitate repeating a particular series of GWCON or CONFIG commands. C1, C2,...,Cn in the Command History is referred to as a *repeat sequence*. This feature may be more convenient than simply using **Ctrl -** and **Ctrl-F** when you must repeat a given task that requires multiple commands. Enter **Ctrl-R** (repeat) to set the start of the *repeat sequence* at command C1. Enter **Ctrl-N** (next) successively to retrieve the next command(s) in the repeat sequence. Commands are not automatically entered, but are placed on the current command line allowing you to modify or enter the command.

To produce the desired behavior of a repeat sequence, the first command retrieved using the first **Ctrl-N** (next) depends on the manner in which the start of the repeat sequence was set using **Ctrl-R** (repeat).

Setting the start of the repeat sequence with **Ctrl-R** can be done in two ways:

1. When C1 is initially entered
2. When C1 is retrieved from the Command History with **Ctrl -** or **Ctrl-F**.

Starting a Repeat Sequence As Commands Are Entered

If you enter **Ctrl-R** as command C1 is being keyed in, and then enter commands C2, C3... Cn. **Ctrl-N** will successively bring commands C1, C2, ... Cn, C1, C2, ... Cn, C1, ... to the command line.

In Example 1, the start of the repeat sequence is set as the first command is keyed in. The user knows ahead of time that the same commands to be entered in GWCON need to be repeated in CONFIG.

Example 1

1. As the first command in the sequence is keyed in, use **Ctrl-R** (repeat) to set the start of the repeat sequence.

   ```
   *console
   +event Ctrl-R
   ```

   then press **Enter** to set the start of the repeat sequence.
2. Continue typing the subsequent commands in the sequence:

   ```
   Event Logging System user console
     ELS>display sub arp
     ELS>display sub lec
     ELS>exit
     +
   ```

3. To enter these same commands in CONFIG, press

   Ctrl-P (the default OPCON intercept character) and go to CONFIG.

   ```
   +-press Ctrl-P-
   *configuration
   Config>Ctrl-N for NEXT to retrieve the start of this sequence-
   Config>event Enter
   Event Logging System user configuration
   ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
   ELS config>display sub arp Enter
   ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
   ELS config>display sub lec Enter
   ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
   ELS config>exit Enter
   Config>
   ```

Starting a Repeat Sequence After All Commands Are Entered

On the other hand, if you first enter C1, C2, ... Cn, and retrieve C1 via **Ctrl -** or **Ctrl-F**. Entering **Ctrl-R**, entering **Ctrl-N** successively brings commands C2,..., Cn, C1, C2,..., Cn, C1,...,Cn to the command line (see Example 2). The first occurrence of C1 is bypassed since C1 is already available on the command line at the time it was retrieved, and does not need to be recalled again by the first **Ctrl-N**.

In Example 2, all the commands are entered and then the first command in the sequence to be repeated is retrieved. A sequence of commands has been entered in GWCON, and the same sequence needs to be repeated in CONFIG.

Example 2

1. Enter the following commands in GWCON:

```
*console
+event
Event Logging System user console
ELS>display sub arp
ELS>display sub lec
ELS>exit
+
```

2. To enter these same commands in CONFIG, press **Ctrl-P** (the default OPCON intercept character) and go to CONFIG.

```
+Ctrl-P-
*configuration
Config>Ctrl - four times to retrieve the start of
        the four command sequence in this example-
Config>event
Config>event Ctrl-R for REPEAT to set the start of the repeat sequence-
 Config>event Enter
 Event Logging System user configuration
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>display sub arp Enter
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>display sub lec Enter
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>exit Enter
 Config>
```

Chapter 3. Using MSS Family Client Firmware

The MSS Family Client contains firmware that tests the hardware each time the MSS Family Client is powered on. If the MSS Family Client has not loaded its operational code, the firmware will be running.

One of the functions is to perform hardware checking after a power-on, and decide which version of the operational code will be loaded. It also allows you to change some of the hardware-related parameters, and manage the operational code and your configuration files.

The System Management Services menu appears when the MSS Family Client is set up to boot up in “Attended Mode.”

Important:

1. You can access the firmware by stopping the boot process. When you reset the MSS Family Client, you will be asked if you want to disable the unattended start mode.
2. From the LAN switch menus select “Non-Token Ring Ports” (or “Non-Ethernet Ports”) and the UFC slot for the MSS Family Client you want to access.
3. You can use the up(↑) and down arrow (↓) keys or the Tab key to move around the firmware panels.

Accessing the Firmware Prompt

Before booting the MSS Family Client, note that:

- You will need a terminal or IP workstation connected to the LAN Switch. This can be a VT100 TTY device connected directly through the serial port or a telnet session to the LAN Switch’s IP address.

Boot Options Available for the MSS Family Client

The MSS Family Client can be configured for Unattended mode. In Unattended mode, you must have chosen which load image and which configuration to load. The structure of the image banks is as follows:

- IMAGE - Status of image
- CONFIG 1 - Status of Config
- CONFIG 2 - Status of Config
- CONFIG 3 - Status of Config
- CONFIG 4 - Status of Config

See “List” on page 110 for a description of file statuses.

Attended Mode

When the client is configured to come up in attended mode, you have access to the Firmware System Management Services.

In attended mode, you can start booting the client by pressing **F9** and then **Enter** to start the operating system.

Unattended Mode

This is the normal mode for the MSS Family Client. It will come up on the Active, Local, or Pending image and config based on your choice.

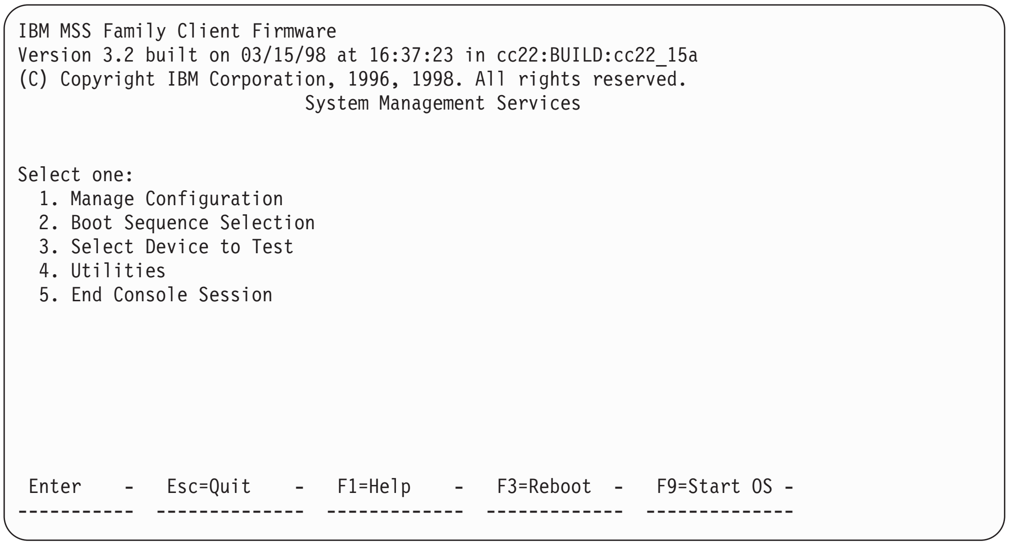
A password is not required to boot up in unattended mode.

Starting the MSS Family Client Firmware

You can begin using the information in this section after you have prepared your service terminal and have established connection with the client.

From the Main Menu panel (as shown in Figure 8), you can select one of four services. The following sections explain these services and provide instructions for going through the associated panels:

- “Managing the Configuration” on page 41
- “Selecting the Boot Sequence” on page 41
- “Selecting a Device To Test” on page 42
- “Using the Utilities” on page 44



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Services


Select one:
  1. Manage Configuration
  2. Boot Sequence Selection
  3. Select Device to Test
  4. Utilities
  5. End Console Session







 Enter    -   Esc=Quit    -   F1=Help    -   F3=Reboot  -   F9=Start OS -
-----------  --------------  -------------  -------------  --------------
```

Figure 8. Main Menu Panel

The Function Keys

As seen in Figure 8, various function keys appear at bottom of the panels. These keys are common among the MSS Family Client Firmware panels. On other panels the functions keys are stacked at the right of the panel. Use the F1 Help key to get descriptions for the function keys associated with the MSS Family Client Firmware.

Obtaining Help

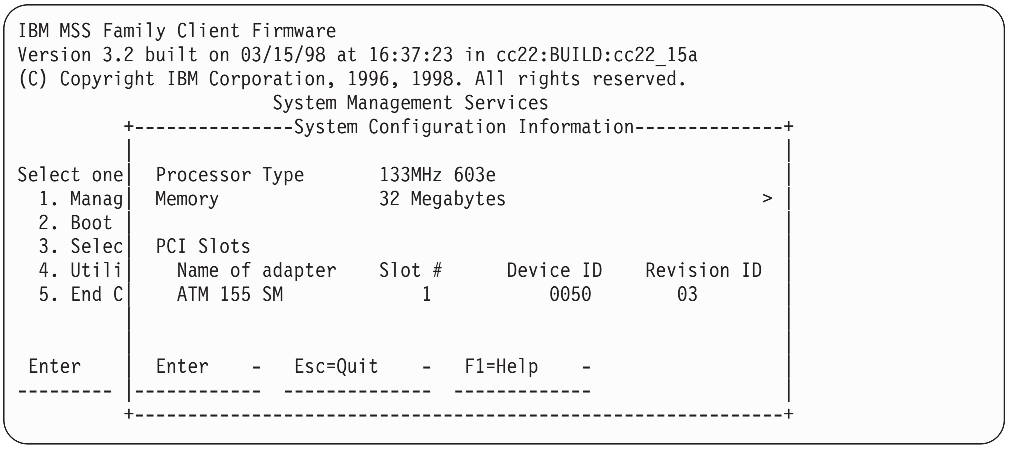
Online helps are available for panels whenever the F1 key appears at the lower portion of the panel. Pressing F1 presents a pop-up help window with information relating to the currently active panel.

Managing the Configuration

Managing the configuration involves defining and modifying some configuration values.

1. Select **1. Manage Configuration** from the main menu as shown in Figure 8 on page 40.
2. The *System Configuration Information* panel appears as shown in Figure 9.

Note: The manage configuration screen on the MSS Family Client provides information related to the hardware of the MSS Client or MSS Domain Client. You cannot modify any of the parameters from this menu.



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                        System Management Services
          +----------------System Configuration Information--------------+
          |                                                              |
Select one|  Processor Type       133MHz 603e                            |
  1. Manag|  Memory               32 Megabytes                         > |
  2. Boot |                                                              |
  3. Selec|  PCI Slots                                                   |
  4. Utili|    Name of adapter    Slot #      Device ID    Revision ID   |
  5. End C|    ATM 155 SM             1           0050        03         |
          |                                                              |
          |                                                              |
 Enter    |  Enter    -   Esc=Quit    -   F1=Help    -                   |
--------- |------------  --------------  -------------                  |
          +--------------------------------------------------------------+
```

Figure 9. System Configuration Information

Selecting the Boot Sequence

This function enables you to select a sequence for the various boot devices, display the current boot device settings, restore the default setting, and boot from other boot devices.

Attention: It is not recommended that you use this function. Use the Change Management option under the Utilities menu instead. See “Chapter 8. Using BOOT Config to Perform Change Management” on page 105 for more information about change management.

Selecting a Device To Test

The firmware performs hardware tests when the MSS Family Client boots up. But there may be times when you have removed and replaced a failing part and you want to run an individual test before a full boot up or reset. The firmware allows you to run these individual tests:

- Test All Subsystems: This test runs all the subsystem tests that are listed on this panel.

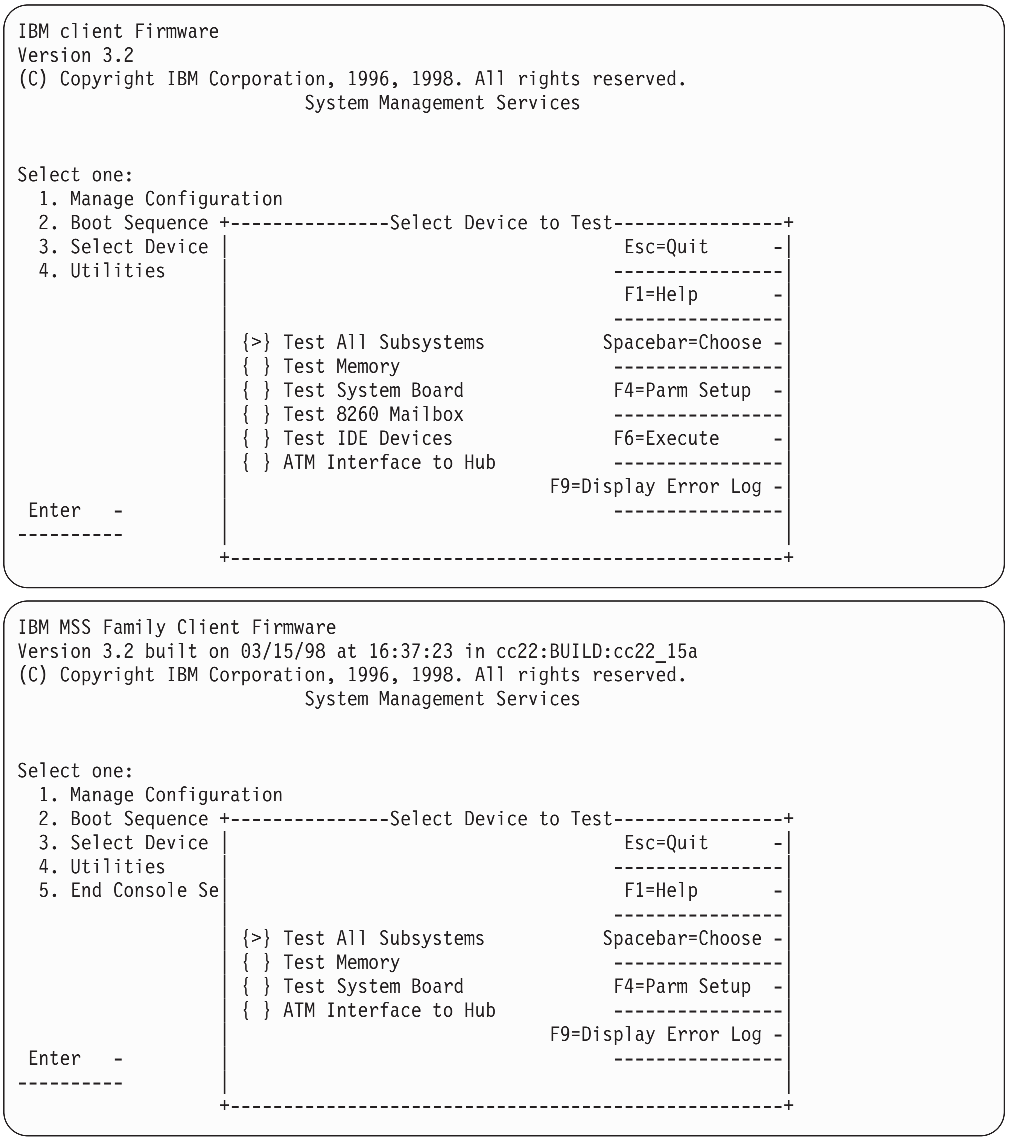
  Note: This list is a variable list and the entries are based on diagnostic files.
- Test Memory: This test searches all available memory regions, tests the regions, and presents a consolidated list of test results.
- Test System Board: This tests the PowerPC CPU and the System Board interrupts.
- 155-Mbps ATM Adapter: This tests the ATM adapter and allows the testing of the physical interface in the MSS Family Client when used with an optical wrap plug.
- LAN Switch Interface: This tests the interface between the MSS Family Client and the LAN Switch.

To test a device:

- Select **3. Select Device to Test** from the main menu.

  The *Select Device to Test* panel appears (Figure 10 on page 43).

  Note: The *Select Device to Test* panel is created dynamically, depending on what diagnostics have been loaded.



```
IBM client Firmware
Version 3.2
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Services


Select one:
  1. Manage Configuration
  2. Boot Sequence +---------------Select Device to Test----------------+
  3. Select Device |                                     Esc=Quit      -|
  4. Utilities     |                                    ----------------|
                   |                                     F1=Help       -|
                   |                                    ----------------|
                   | {>} Test All Subsystems           Spacebar=Choose -|
                   | { } Test Memory                    ----------------|
                   | { } Test System Board              F4=Parm Setup  -|
                   | { } Test 8260 Mailbox              ----------------|
                   | { } Test IDE Devices               F6=Execute     -|
                   | { } ATM Interface to Hub           ----------------|
                   |                              F9=Display Error Log -|
 Enter   -         |                                    ----------------|
----------         |                                                    |
                   +----------------------------------------------------+
```

```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Services


Select one:
  1. Manage Configuration
  2. Boot Sequence +---------------Select Device to Test----------------+
  3. Select Device |                                     Esc=Quit      -|
  4. Utilities     |                                    ----------------|
  5. End Console Se|                                     F1=Help       -|
                   |                                    ----------------|
                   | {>} Test All Subsystems           Spacebar=Choose -|
                   | { } Test Memory                    ----------------|
                   | { } Test System Board              F4=Parm Setup  -|
                   | { } ATM Interface to Hub           ----------------|
                   |                              F9=Display Error Log -|
 Enter   -         |                                    ----------------|
----------         |                                                    |
                   +----------------------------------------------------+
```

Figure 10. Test Selection Panel

- Use the spacebar and up arrow and down arrow keys to select the test that you want to run.
- Move the cursor to a selection and press **F4** to define additional test parameters.

  Note: Errors encountered during diagnostics are logged in the hardware error log.
- The *Test Parameters* panel appears. From this panel you can select:
  – Run Interactive Test
  – Run Wrap Tests
  – Stop On Error
  – Loop Tests
  – Loop Count

  Press **Esc** to return to the *Select Device Test* panel.
- Press **F6** to start a test.

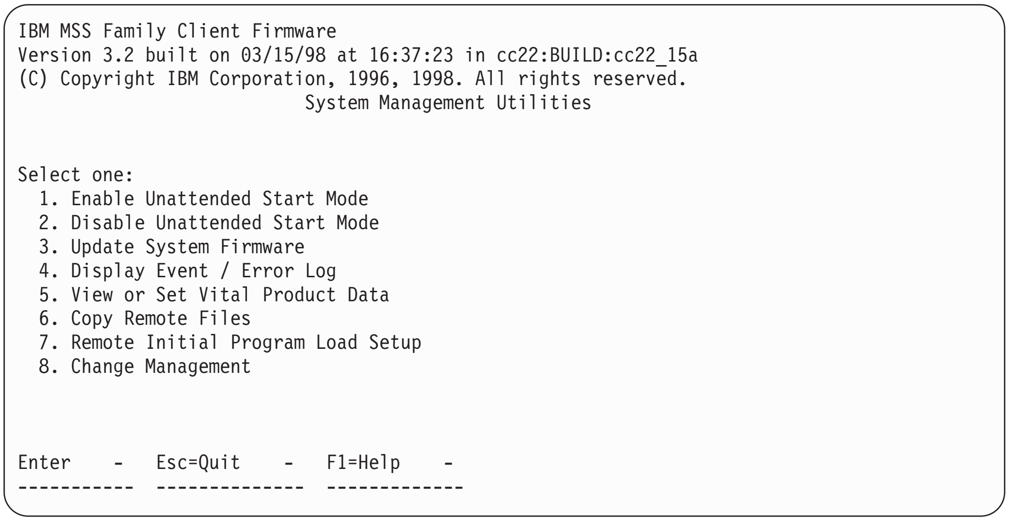
- After the test is complete, press **Esc** to return to the main menu panel.

Using the Utilities

To use the utilities:

1. Select **4. Utilities** from the main menu.

   A panel listing the available utilities appears (Figure 11).



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Utilities


Select one:
  1. Enable Unattended Start Mode
  2. Disable Unattended Start Mode
  3. Update System Firmware
  4. Display Event / Error Log
  5. View or Set Vital Product Data
  6. Copy Remote Files
  7. Remote Initial Program Load Setup
  8. Change Management



Enter    -   Esc=Quit    -   F1=Help    -
-----------  --------------  -------------
```

Figure 11. Utilities Selection Panel

2. Make your selection. Additional panels appear to prompt you for additional information, and messages appear to indicate that the task is completed.

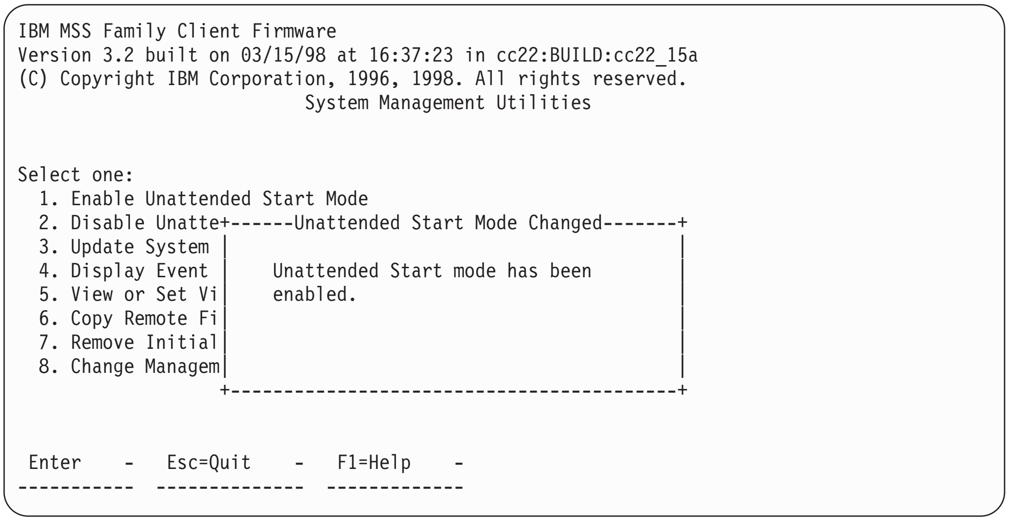
Enabling Unattended Start Mode

The default is that the unattended start mode is enabled, which causes the MSS Family Client to load operational code automatically.

Note: You can perform this function only if you do it immediately after you perform a power-on reset.

1. Select **Enable Unattended Start Mode** from the utilities panel.

   The *Unattended Start Mode Changed* panel appears. See Figure 12 on page 45.



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Utilities


Select one:
  1. Enable Unattended Start Mode
  2. Disable Unatte+------Unattended Start Mode Changed-------+
  3. Update System |                                          |
  4. Display Event |    Unattended Start mode has been        |
  5. View or Set Vi|    enabled.                              |
  6. Copy Remote Fi|                                          |
  7. Remove Initial|                                          |
  8. Change Managem|                                          |
                   +------------------------------------------+


 Enter    -   Esc=Quit    -   F1=Help    -
-----------  --------------  -------------
```

Figure 12. Unattended Start Mode Changed (Enabled) Panel

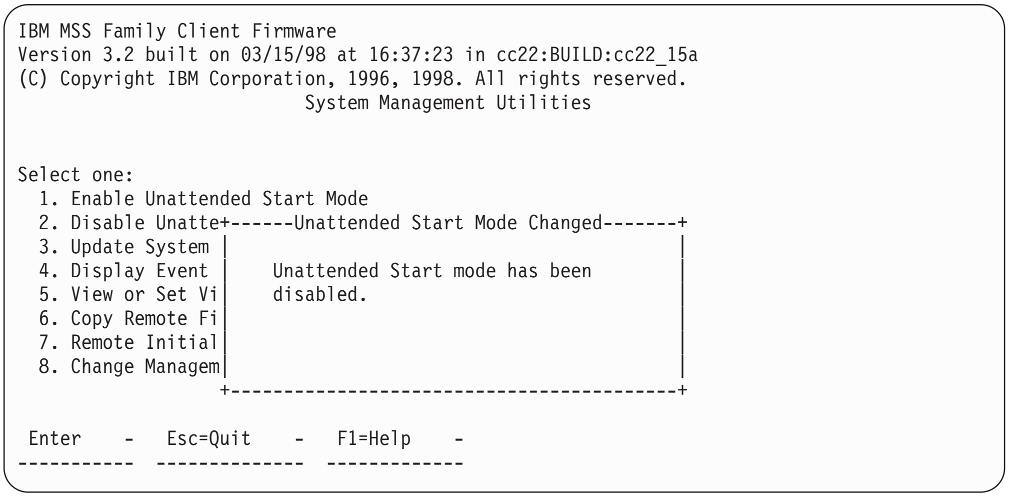
Disabling Unattended Start Mode

The default for the MSS Family Client firmware is that the unattended start mode is enabled. You disable Unattended Start Mode using this utility.

Note: Disabling unattended start mode from the firmware overrides the prompts you will receive from the LAN Switch.

1. Select **Disable Unattended Start Mode** from the utilities panel.

   The *Unattended Start Mode Changed* panel appears. See Figure 13.



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Utilities


Select one:
  1. Enable Unattended Start Mode
  2. Disable Unatte+------Unattended Start Mode Changed-------+
  3. Update System |                                          |
  4. Display Event |    Unattended Start mode has been        |
  5. View or Set Vi|    disabled.                             |
  6. Copy Remote Fi|                                          |
  7. Remote Initial|                                          |
  8. Change Managem|                                          |
                   +------------------------------------------+

 Enter    -   Esc=Quit    -   F1=Help    -
-----------  --------------  -------------
```

Figure 13. Unattended Start Mode Changed (Disabled) Panel

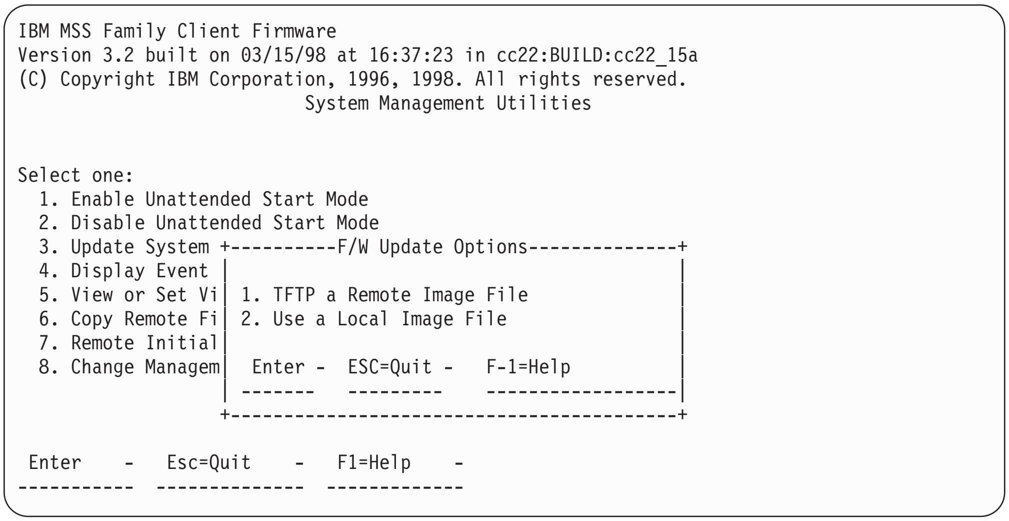
Updating System Firmware

Use this utility to update the MSS Family Client firmware.

Note: Do not power off or reset the MSS Family Client during the process of updating the firmware. If the update fails, the MSS Family Client will boot a backup firmware image. If this happens, repeat the update procedure to reload the onboard firmware image.

1. Select **Update System Firmware** from the utilities panel.

   The *System Firmware Update* panel appears. See Figure 14.



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Utilities


Select one:
  1. Enable Unattended Start Mode
  2. Disable Unattended Start Mode
  3. Update System +----------F/W Update Options---------------+
  4. Display Event |                                           |
  5. View or Set Vi| 1. TFTP a Remote Image File               |
  6. Copy Remote Fi| 2. Use a Local Image File                 |
  7. Remote Initial|                                           |
  8. Change Managem|  Enter -  ESC=Quit -   F-1=Help           |
                   | -------   ---------    -------------------|
                   +-------------------------------------------+

 Enter    -   Esc=Quit    -   F1=Help    -
-----------  --------------  -------------
```

Figure 14. Update System Firmware Panel

2. Select the option that you want to use from those listed. For TFTP, the system prompts you for the remote (the “from”) file name that you want to use.

   If you need to set the IP address of the MSS Family Client, use the **Remote Initial Program Load** menu.

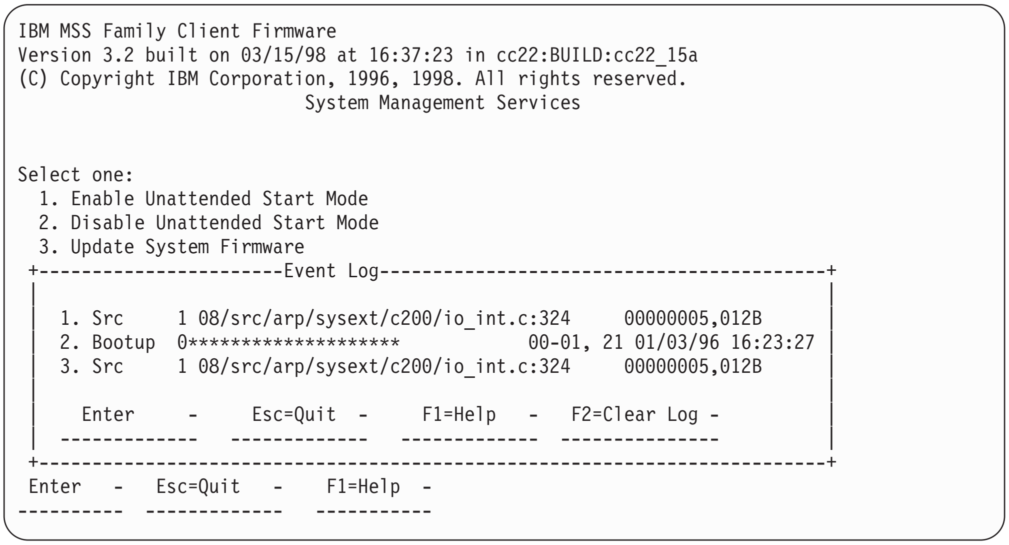
   The firmware update process begins. It informs you that the system firmware has been updated.

Displaying the Event/Error Log

To display the Event/Error Log:

1. Select **Display Event / Error Log** from the utilities panel.

   The *Event / Error Log* panel appears. See Figure 15 on page 47.



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Services


Select one:
  1. Enable Unattended Start Mode
  2. Disable Unattended Start Mode
  3. Update System Firmware
 +-----------------------Event Log------------------------------------------+
 |                                                                          |
 |  1. Src     1 08/src/arp/sysext/c200/io_int.c:324     00000005,012B      |
 |  2. Bootup  0********************            00-01, 21 01/03/96 16:23:27 |
 |  3. Src     1 08/src/arp/sysext/c200/io_int.c:324     00000005,012B      |
 |                                                                          |
 |    Enter     -     Esc=Quit  -     F1=Help   -   F2=Clear Log -          |
 |  -------------   -------------   -------------  ---------------          |
 +--------------------------------------------------------------------------+
 Enter   -   Esc=Quit   -    F1=Help  -
----------  -------------   -----------
```

Figure 15. Event/Error Log Panel

If the log is too large to appear on one panel, you can move through the log by using the up and down arrow keys or the PgUp/PgDn keys.

2. Press **F2** to clear the log.

Hardware Error Codes

The error log that is displayed when you use the Display Event/Error Log firmware utility contains error codes. Table 3 explains these codes.

Table 3. Hardware Error Codes

Error Code	Physical Location	Software Subsystem	Explanation
00010000	System Board	Processor	Error occurred during processor test
00011000	System Board	NVRAM	Non-volatile RAM Test Failure
00015001	System Board	Firmware	Error occurred while erasing the system firmware
00015002	System Board	Firmware	Error occurred while updating the system firmware
00015011	System Board	Main Flash Array	Error occurred while erasing the system main flash array
00015500	System Board	Interrupts	System board interrupt test failure
00015501	System Board	Interrupts	Error occurred during processor interrupt test
00015502	System Board	Interrupts	Error occurred during real-time clock interrupt test
00015503	System Board	Interrupts	Error occurred during timer interrupt test
00016000	System Board	RTC-NVRAM	CRC error
00016002	System Board	RTC-NVRAM	Read/write failure
00017001	System Board	RTC-NVRAM	Battery drained
00017006	System Board	RTC-NVRAM	Security data missing or not valid

Table 3. Hardware Error Codes (continued)

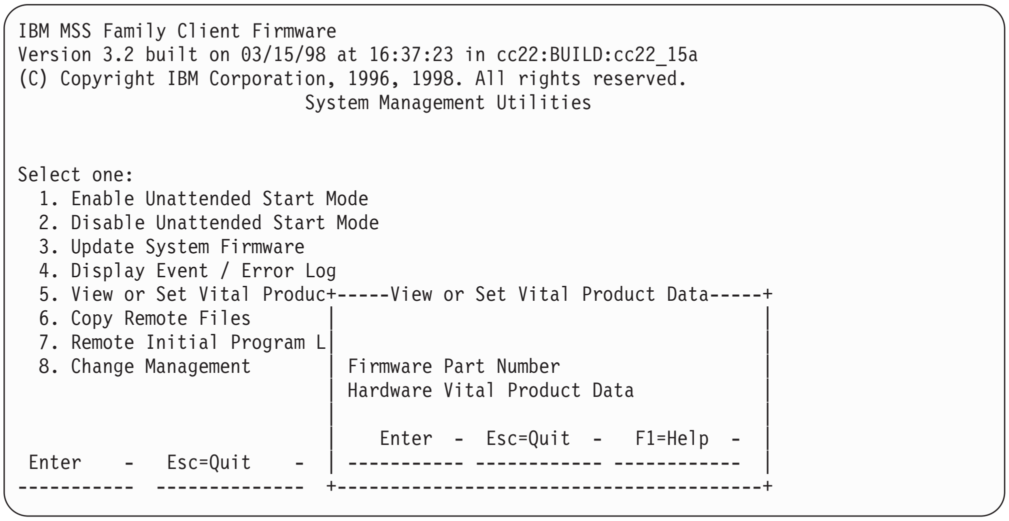
Error Code	Physical Location	Software Subsystem	Explanation
00017007	System Board	Security	Maximum unsuccessful attempts to enter password was reached
4000xxxx	UFC Base Card	UFC Interface Diagnostics	An error occured during testing of the LAN Switch UFC Interface Packet Memory, xxxxx = detailed information
41000000	UFC Base Card	UFC Interface Diagnostics	Error occurred during the LAN Switch UFC Interface Wrap Test
50001100	System Board	Firmware	The level of System Management Services does not match the level of system firmware
710sdddd	155-Mbps MMF adapter	ATM diagnostics	Error occurred with ATM adapter in slot “s” dddd = detailed status
720sdddd	155-Mbps SMF adapter	ATM diagnostics	Error occurred with ATM adapter in slot “s” dddd = detailed status

7msceddd	PCI slots		Adapters m=unique for adapter type
			s=subtest, c=slot id, e=error id,
			ddd = debug

81xyzzzz	System Board	Memory	Error occurred while testing main flash array memory pages x, y, zzzz = detailed information

Viewing Vital Product Data

This utility allows you to view vital product data (VPD) for the MSS Family Client



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Utilities


Select one:
  1. Enable Unattended Start Mode
  2. Disable Unattended Start Mode
  3. Update System Firmware
  4. Display Event / Error Log
  5. View or Set Vital Produc+-----View or Set Vital Product Data-----+
  6. Copy Remote Files       |                                        |
  7. Remote Initial Program L|                                        |
  8. Change Management       | Firmware Part Number                   |
                             | Hardware Vital Product Data            |
                             |                                        |
                             |    Enter  -  Esc=Quit  -   F1=Help  -  |
 Enter    -   Esc=Quit    -  | ----------- ------------ ------------  |
-----------  --------------  +----------------------------------------+
```

Figure 16. View of Set Vital Product Data

1. Select **View or Set Vital Product Data** from the utilities panel.

   The *View or Set Vital Product Data* panel appears (Figure 16). From this panel you can select the type of vital product data you want to view.

2. For each selection, a *View Part Number* panel appears that contains the part number you selected. Version number and dates are provided for the firmware and System Management Services.
3. Select **Hardware Vital Product Data** if you want to view vital product data. VPD is stored in keyword format. The following is a list of the keywords and their meanings. Depending on the configuration of your system, all of the keywords listed may not be present or have meaningful values.

   Vital product data fields are:

   AT - Main logic card type

   DS - Text description of card

   FN - FRU number

   PN - Manufacturing part number

   ML - Maintenance level

   MF - Manufacturing location

   SN - Serial number

   BF - Boot flash level and ID

   NA - Burned in MAC Address in ASCII Format

   F# - Feature Number

   BS - Box serial number

   RC - Recycle count

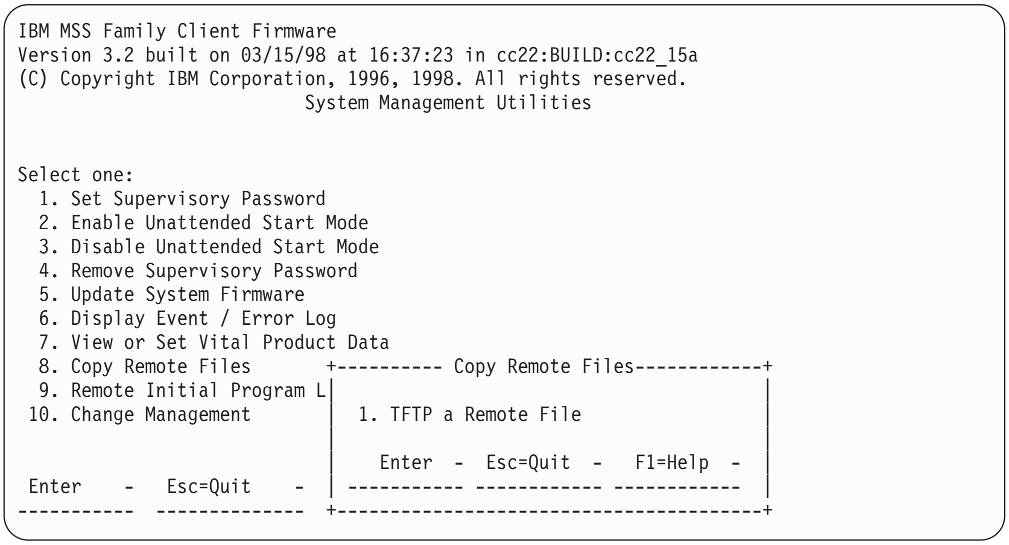
   Z0 - Vendor ID
4. Press **Esc** when you are through.

Copying Remote Files

This utility allows you to tftp remote files from another machine into memory.

1. Select **Copy Remote Files** from the utilities panel.

   The *Copy Remote Files* panel appears (Figure 17 on page 50). From this panel you select the method of file transfer. Subsequent panels allow you to enter the names of the files that you want to copy.



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Utilities


Select one:
  1. Set Supervisory Password
  2. Enable Unattended Start Mode
  3. Disable Unattended Start Mode
  4. Remove Supervisory Password
  5. Update System Firmware
  6. Display Event / Error Log
  7. View or Set Vital Product Data
  8. Copy Remote Files       +---------- Copy Remote Files------------+
  9. Remote Initial Program L|                                        |
 10. Change Management       |  1. TFTP a Remote File                 |
                             |                                        |
                             |    Enter  -  Esc=Quit  -   F1=Help  -  |
 Enter    -   Esc=Quit    -  | ----------- ------------ ------------  |
-----------  --------------  +----------------------------------------+
```

Figure 17. Copy Remote Files Panel

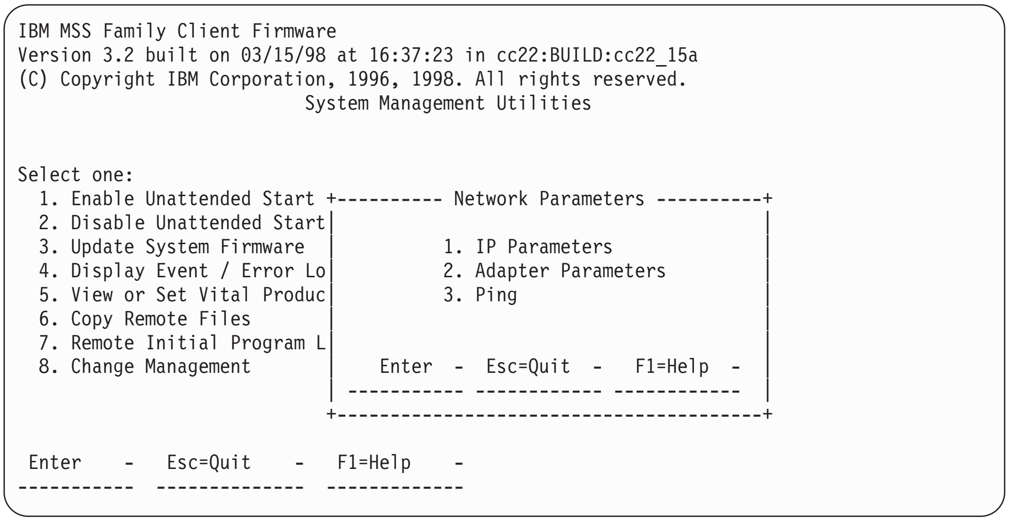
Setting Up Remote Initial Program Load

Before you can configure an MSS Family Client in the network, it must have an IP address that is recognized within your network.

This utility allows you to load this minimum information to install this device in your network so that you can send it a configuration file, or otherwise communicate with it. This utility allows you to Ping the MSS Family Client, after loading its minimum network parameters, to see if you can communicate with it.

1. Select **Remote Initial Program Load Setup** from the utilities panel.

   The *Network Parameters* panel appears (Figure 18). From this panel you can select to enter the IP address of the MSS Family Client and the host, input adapter parameters, or Ping from the MSS Family Client to the host.



```
IBM MSS Family Client Firmware
Version 3.2 built on 03/15/98 at 16:37:23 in cc22:BUILD:cc22_15a
(C) Copyright IBM Corporation, 1996, 1998. All rights reserved.
                           System Management Utilities


Select one:
  1. Enable Unattended Start +---------- Network Parameters ----------+
  2. Disable Unattended Start|                                        |
  3. Update System Firmware  |          1. IP Parameters              |
  4. Display Event / Error Lo|          2. Adapter Parameters         |
  5. View or Set Vital Produc|          3. Ping                       |
  6. Copy Remote Files       |                                        |
  7. Remote Initial Program L|                                        |
  8. Change Management       |    Enter  -  Esc=Quit  -   F1=Help  -  |
                             | ----------- ------------ ------------  |
                             +----------------------------------------+


 Enter    -   Esc=Quit    -   F1=Help    -
-----------  --------------  ------------
```

Figure 18. Setup Remote Initial Program Load Panel

- If you select **IP Parameters**, a panel appears on which you can enter:

- Client IP Address (the IP address of the MSS Family Client)
- Server IP Address
- Gateway IP Address
- Subnet Mask

An MSS Family Client comes from the factory with the following default IP addresses:

Client	10.1.1.3
Server	10.1.1.2
Gateway	10.1.1.2
Subnet Mask	255.255.255.0

2. If you select **Adapter Parameters**, a panel appears with options to:
   - Display the MAC address of the MSS Family Client
   - Display the network type - either Ethernet or Token-Ring
   - Display or set the LAN Switch domain number that the firmware uses

   Note: This release of the MSS Family Client firmware only supports communication over domain 0 (the default domain) on the LAN Switch.
3. The **Ping** option allows you to test connectivity.

Change Management

Change Management enables you to manipulate the client level of software code that will run on the client See “Chapter 8. Using BOOT Config to Perform Change Management” on page 105 for detailed information about change management.

Chapter 4. Getting Started with Configuring the MSS Family Client

This chapter explains how to access the MSS Family Client using a workstation and how to manage operational software images and configuration files. It also provides a brief overview of the configuration methods available for the MSS Family Client.

Configuration and Monitoring Tools

These are the various configuration and monitoring tools that are supported by the physical connections:

Multiprotocol Switched Services Client Configuration Program

This is a standalone program that is installed in a workstation which uses TCP/IP to connect to the MSS Family Client. You must use this program differently before and after the initial configuration of the MSS Family Client.

Before configuration:

Initial configuration of the MSS Family Client must be through a local console on the LAN switch. When the MSS Family Client is in this state, you cannot use the Communications options of the Configuration Program. You can create configuration files and download them later to the MSS Family Client using TFTP.

Note: If you are using a Windows 95 workstation, you must obtain a TFTP daemon as the daemon is not part of the base TCP/IP software.

After configuration:

After the MSS Family Client has been made operational with an IP address and subnet mask, you can create and download the configuration files using the communications options of the configuration program.

When the MSS Family Client is in this state, you can use the Communications Send option of the Configuration Program to send configuration files from the workstation over the network to the MSS Family Client. When using the version of the Configuration Program that is supported by AIX, you can also use the Communications Retrieve option of the Configuration Program to retrieve configuration files from the MSS Family Client. For more information, see *IBM Multiprotocol Switched Services Client Configuration Program User's Guide for Nways Multiprotocol and Access Services Products*, GC30-3830.

Web browser Hypertext Markup Language (HTML) interface

The Web browser interface is a configurator that is a home page and is accessed by a Web browser from a workstation that is connected to the MSS Family Client. You need a Web browser that can display clickable images and tables. The Web browser interface can be accessed using IP.

If you supply the Web browser one of the configured IP addresses of the MSS Family Client, or its name (when using an IP name server), the Web browser interface will come up.

Command line interface

The command line interface is a teletypewriter (TTY) text interface that requires you to enter commands to use it. The workstation that accesses it must be either an ASCII terminal, a personal computer (PC), a telnet connection to the LAN Switch, or other intelligent programmable workstation emulating an ASCII terminal.

After the MSS Family Client is operational in the network, you can Telnet into the MSS Family Client over IP to bring up this interface. If one connection to the MSS Family Client is a Telnet session, the MSS Family Client can support two connections at one time.

The command line interface is marked by an asterisk (*) prompt.Refer to the *IBM Multiprotocol Switched Services Client Interface Configuration and Software User's Guide* for a full description of this interface.

File Transfer

Table 4 defines the ways in which configuration files and operational software files can be transferred to and from the MSS Family Client.

Table 4. File Transfer

File Transfer Method	Type of Connection
TFTP Get command from the MSS Family Client to the workstation that has the binary configuration file, to download operational software images and configuration files to the MSS Family Client. Files sent using TFTP must be binary, or the MSS Family Client cannot use them. You should use the Create command of the Configuration Program to save configuration files in binary format before downloading them to the MSS Family Client. After the MSS Family Client is operational in the network, you can use the TFTP Put command over IP to upload a file from the MSS Family Client to a workstation. The file will be uploaded in binary format. Both operational software and configuration files can be uploaded. You should use the Read router configuration option of the Configuration Program to make an uploaded configuration file usable by the Configuration Program so that you can change some parameter values in it. **Note:** Using TFTP Put is a way to retrieve files from the MSS Family Client if the Retrieve option of the Configuration Program is not available.	• IP connection of operational MSS Family Client over functioning network (using the TFTP Get and Put commands to download and upload files).
The Communications Option of the Configuration Program (actually, the protocol for this is SNMP). This method cannot be used until the MSS Family Client is operational in the network. The files are not binary, but are in a format that is internal to the Configuration Program. This function can send configuration files to the MSS Family Client and retrieve them from the server.	IP connection of operational MSS Family Client over functioning network.

Initial Configuration

After the MSS Family Client has passed its hardware diagnostics, it is in a ready state for configuration.

Performing an Initial Configuration

1. Perform a minmial configuration using one of the following methods:
   - Use a TTY connection to access the IBM MSS Family Client.
   - Bring up the Web browser interface or the command line interface.
   - Use quick configuration to do a minimal configuration of the IBM MSS Family Client, including IP address and SNMP. See “Quick Configuration”.
2. Restart the IBM MSS Family Client to activate the quick configuration.
3. Next, make and save a configuration file using the Configuration Program. Use the TFTP Get command over IP or use the Communications Options Send command of the Configuration Program to download the configuration file.

   When using TFTP, you must use the Create option of the Configuration Program to create binary files and then TFTP them to the IBM MSS Family Client.
4. Restart the IBM MSS Family Client to make the configuration active. If the configuration file included all the necessary parameters, the IBM MSS Family Client should now be completely operational in the network.

Tips for Managing Configuration Problems

Important: After the IBM MSS Family Client is configured and operational, ***always*** back up the active configuration file. Keeping this file enables you to re-establish the IBM MSS Family Client on the network should the active configuration become corrupted.

Back up the active configuration file by retrieving it and storing it in the workstation. See “File Transfer” on page 54 for more information.

Reconfiguring

You may find it hard to detect problems caused by configuration errors. A configuration error can initially appear to be a hardware problem because the IBM MSS Family Client will not start or data will not flow through a port. In addition, problems with configuration may not result in an error initially; an error may occur only when specific conditions are encountered or when heavy network traffic occurs.

If you cannot resolve a problem after making a few changes to the configuration or after restoring the active configuration file, it is recommended that you generate a new configuration. Too many changes to a configuration often compound the problem, whereas you can usually generate and test a new configuration within a few hours.

Quick Configuration

Quick configuration is a process for initial configuration that is available either from the Web browser interface or from the command line interface. It produces a simple configuration that will enable the IBM MSS Family Client to run in the network. The Web browser interface, which is the more usable of the two interfaces, is recommended. See “Quick Configuration Using the Web Browser Interface” on page 66 for a description of quick configuration using the Web interface.

Completing the Configuration After Quick Configuration

After completing quick configuration, reload the IBM MSS Family Client to activate the configuration. Then, you can access the IBM MSS Family Client over the network, if you have configured an IP address for it.

The configuration provided by QCONFIG depends upon many default values for parameters, some of which may not be appropriate to your installation. You may need to modify the configuration created using QCONFIG to customize the IBM MSS Family Client to work in your network. Do this using any of these methods:

- Configuration Program
- Web browser HTML interface
- Command line interface

However, the Configuration Program is the preferred configuration method for these reasons:

1. It enables you to keep a number of copies of configuration files on a server for uploading to the appropriate IBM MSS Family Client.
2. It does not alter any configuration parameters dynamically. This feature helps control changes to the IBM MSS Family Client configurations.
3. It performs more input validation and cross-checking of the configuration parameters than the other methods.

The command line interface and the Web browser interface cause certain parameters to be altered dynamically. The binary files that they create are saved on the IBM MSS Family Client, not in the workstation. These characteristics make them more difficult to use for managing the configuration of the IBM MSS Family Client. However, they can be used to monitor the operations of the IBM MSS Family Client, whereas the Configuration Program cannot. They are also useful when you want to change one of the parameters that can be dynamically altered.

How Software Files Are Managed

To help manage operational software upgrades and configurations, the IBM MSS Family Client has a software change management feature. This utility enables you to determine which configuration file is active while the IBM MSS Family Client is running. In addition to storing the active configuration file, the IBM MSS Family Client stores up to 4 configuration files in non-volatile memory.

How to View the Files

To use the change management tool in the command line interface to view the operational software image and the configuration files, follow these steps:

1. From the prompt for OPCON, which is an asterisk (*), type **talk 6**. The prompt `Config>` appears.
2. Enter **boot**. You will see the prompt `Boot config>`.
3. Enter **list** to display information about which load images and configuration files are available and active.

   See “List” on page 110 for sample list output and a description of file statuses.

How to Reset the IBM MSS Family Client

Note: A reset interrupts the function of the IBM MSS Family Client for up to 90 seconds. Be sure that the network is prepared for the interruption.

As previously stated, PENDING and LOCAL files are not loaded into active memory until you reset the IBM MSS Family Client.

You can reset the IBM MSS Family Client using any one of these methods:

- At the `Config only>` prompt, type **reload**.

  Note: The `Config only>` prompt appears when no configuration file is active. Lack of an active configuration file indicates that an active configuration has become corrupted or that the IBM MSS Family Client is not configured.
- At the OPCON prompt (*), type **reload**.
- Through the LAN switch.

File Transfer Using TFTP

See “TFTP” on page 112 for a sequence of commands to transfer a file from a workstation or server to the IBM MSS Family Client using TFTP. You will need to substitute your own values for the IP address and path, which are given as examples.

Storing Configuration Files Using the Command Line Interface or the Web Browser Interface

To store a configuration file created using the command line interface, type **write** at the `Config>` prompt. When using the Web browser interface, select **Write.** The Write command creates a binary configuration file that contains the most current value of each of the configuration parameters.

This file is stored in the ACTIVE bank and is given PENDING status. If the status of the file is not changed by a Set command, it becomes the ACTIVE configuration when the IBM MSS Family Client is reset.

Changing the Statuses of Files

These are the ways to change the statuses of image and configuration files:

- You can cause the IBM MSS Family Client to perform a reset by using the Send command from the Communications Option of the Configuration Program. When you do this, the file sent can arrive as a PENDING file or as an AVAIL file. If it is a PENDING file, it becomes the ACTIVE configuration and the previously ACTIVE file becomes AVAIL when the IBM MSS Family Client is reset.

  If it is an AVAIL file, resetting the IBM MSS Family Client does not change its status.
- Use the Set config (set config) commands from the `Boot config>` prompt manually to change the status of any files except the ACTIVE files. If you set a file to PENDING, it becomes ACTIVE and the ACTIVE file becomes AVAIL when a reset is performed.

- Use the Write command to store a configuration file that you have created using the command line interface or the Web browser interface, it is stored with a PENDING status.
- If you copy a file from one location to another, the file receives the status of the file that was there before it and that it overwrites. For example, copying a file with the status of AVAIL over a file that has the status of PENDING, the new file will keep the status of the original file, which is PENDING.

Using the Configuration Program to Manage the Configuration Files

For optimal configuration management, it is recommended that you use the Configuration Program and its configuration database to manage all IBM MSS Family Client configuration files.

The design of change management facilitates good control of the configuration files. Keeping the ACTIVE file and the file that is stored in the configuration database the same assures that a copy of the ACTIVE file is always available.

Use the Send option to send a new configuration to the IBM MSS Family Client, the new configuration is written to the ACTIVE bank and overwrites the file located in the position just below the currently ACTIVE configuration. The new configuration is PENDING if a time is set for a reset. If the configuration file is sent without a specified time for the reset to occur, it gets AVAIL status.

For example, suppose that CONFIG 2 is ACTIVE. The new configuration file is written to CONFIG 3. It has a status of PENDING if a reset time is associated with it; if not, it has a status of AVAIL.

If the file has a status of PENDING, CONFIG 2 becomes AVAIL and CONFIG 3 becomes ACTIVE when a reset occurs. The next file that is sent from the Configuration Program will be placed in CONFIG 4. If a reset time is associated with the file, it will have the PENDING status and will become ACTIVE when the next reset occurs. If another file is then sent, it is placed in CONFIG 1 because the currently ACTIVE file is now in CONFIG 4. This arrangement results in a circular queue.

If the downloaded file has a status of AVAIL, a reset does not change its status. If another file is sent down, it overwrites that file because the ACTIVE file has not changed and the newly downloaded file always occupies the location just behind the ACTIVE file.

Using the Set Commands

See “Set” on page 111 for information about the **set** command.

Other Change Management Functions

These are the other change management commands:

- Describe load images
- Describe config images
- Disable dumping
- Enable dumping
- Erase files

Describe

See “Describe” on page 109 for information about the **Describe** function.

Disable Dumping

The MSS Family Client can be setup to dump the contents of memory to permanent storage in the unlikely event of a complete system failure. Only enable the dumping feature when directed by IBM Service. The default mode for dumping is disabled. If dumping is enabled, using this selection will cause the MSS Family Client *not* to dump to permanent storage.

To disable dumping, type **t 6** at the *, press **Enter** and then type **disable dump** or **dis du** at the `Config>` prompt. You will see the message:

```
Config> Automatic memory dump disabled
```

Enable Dumping

Note: Only enable dumping when directed by an IBM service representative.

This command enables the dumping of memory in the event that the MSS Family Client has a catastrophic error. When enabling dumping, the system’s state is frozen so you can retrieve the memory dump using tftp to a permanent storage device. Retreiving the dump file requires operator intervention and the system will remain frozen until this action is performed or the LAN switch is reset.

The system memory dump must be retreived through a restricted diagnostics menu of the LAN Switch console. IBM Service will provide special instructions for accessing this menu, if needed.

To enable dumping, type **t 6** at the *, press **Enter** and then type **enable dump** or **ena du** at the `Config>` prompt. You will see the message:

```
Config> Automatic memory dump enabled
```

The default state is to have dumping enabled.

Erase Files

See “Erase” on page 109 for information about the **erase** command.

Using the Copy Command

The Copy command moves a file from one location in the storage area to another. This command allows you to change the status as well. The file moved always receives the status of the storage area that it is moved to. For example, suppose that you have this scenario:

- The configuration file in BANK F CONFIG 1 is AVAIL. The configuration file in BANK F CONFIG 2 is PENDING.
- You copy the configuration in BANK F CONFIG 1 to BANK F CONFIG 2.

In this case, the original configuration file in BANK F CONFIG 1 remains unchanged and AVAIL. The configuration that was in BANK F CONFIG 2 is overwritten by a copy of the configuration file that is in BANK F CONFIG 1. This copy retains the status of the file that it overwrote, in this case, PENDING.

See “Copy” on page 108 for additional information about the **copy** command.

Using the Lock Command

The **lock** command prevents the client from overwriting the selected configuration with any other configuration.

See “Lock” on page 110 for additional information about the **lock** command.

Using the Unlock Command

The **unlock** command removes the lock from a configuration allowing the configuration to be updated.

See “Unlock” on page 114 for additional information about the **unlock** command.

Chapter 5. Using the World Wide Web Interface

The MSS Family Client provide a World Wide Web interface to monitor and configure the product. The Web browser interface performs all of the functionality of the command line interface, but in a graphical, more user-friendly manner.

Connecting to the World Wide Web Interface

Use any web browser that supports HyperText Markup Language (HTML) tables and clickable images. Examples of browsers that support this feature are WebExplorer Version 1.03 or higher, Netscape Navigator Version 1.1N or higher, and Mosaic Version 2.1.1 or higher.

Access the MSS Family Client using the Web interface through any connection on an MSS Family Client that has been configured and is operational in the network. To use this connection, provide the browser with the IP address of any interface in the LAN switch. Use any web browser that supports HyperText Markup Language (HTML) tables and clickable images. Examples of browsers that support this feature are WebExplorer Version 1.03 or higher, Netscape Navigator Version 1.1N or higher, and Mosaic Version 2.1.1 or higher.

To access the Home Page of the IBM MSS Family Client, point your browser to the Universal Resource Locator (URL) `http://<machine>/`, where <machine> is either the name or one of the configured IP addresses of the IBM MSS Family Client.

You will be shown the Home Page that is described in the next section.

Note: Before using the Web browser, the IBM MSS Family Client must have been configured with an IP address.

Use this source IP address to identify the workstation:

```
10.1.1.x
```

The letter *x* stands for any value.

Rules for Using the Web Interface

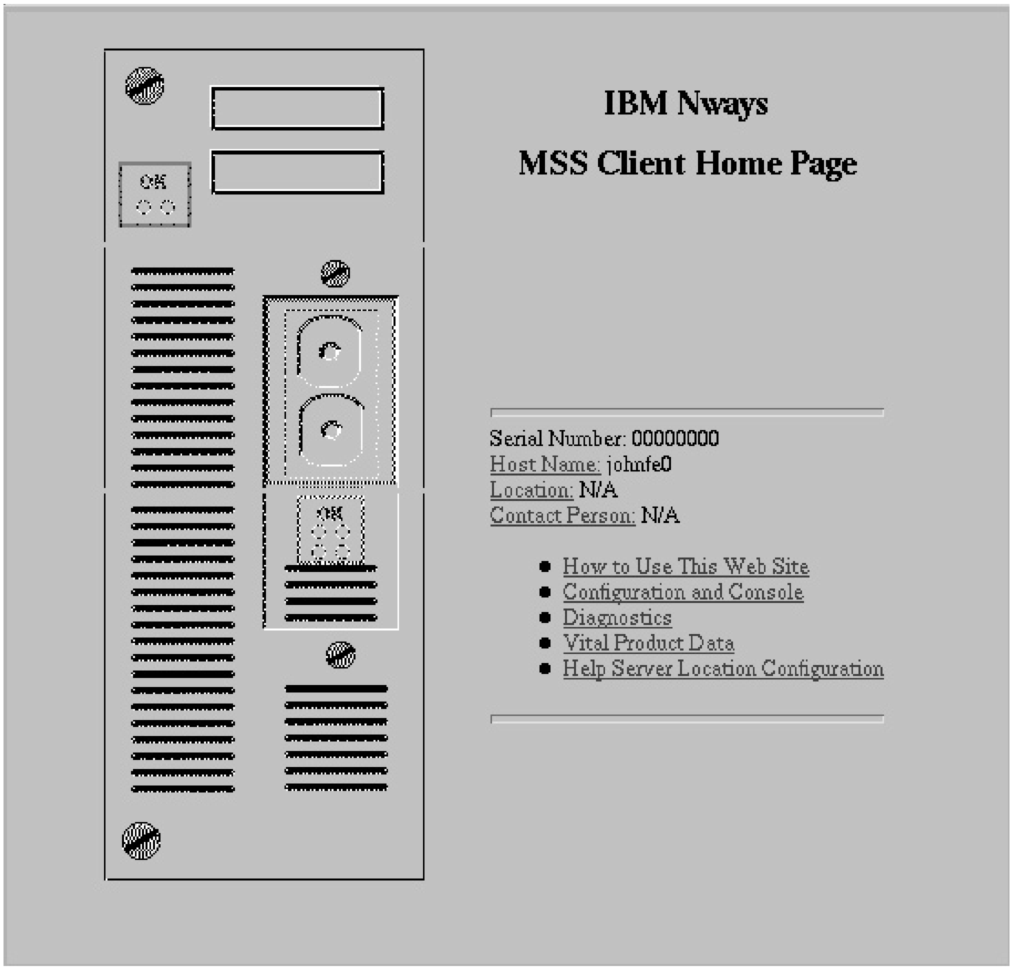
When configuring using the Web browser interface, observe the following guidelines:

- Many configuration options require you to enter data on two or more Web pages (or forms). If you fill in and submit the first form in a series, be sure to complete the remaining forms. If you do not fill in and submit all the forms, the configuration parameter could be left in an unknown state.
- More than one person should not perform configuration at the same time. They can interfere with one another. For example, one person could delete an interface while the other person is in the middle of configuring a protocol on that interface.
- Disable the caching feature of the browser. If you do not do this, the browser may pull a page out of memory instead of going to the IBM MSS Family Client to get the latest information. The browser will display old data. This problem is more likely to occur when you use the *Back* button on the browser.
- Do not use your web browser's reload, back, or forward navigation buttons when using the Web browser interface. Using these buttons could cause problems

during configuration. Instead, use the command history list or any of the navigation buttons on the web pages themselves.

Home Page Structure

Figure 19 shows the IBM MSS Family Client Home Page.



IBM Nways

MSS Client Home Page

Serial Number: 00000000
Host Name: johnfe0
Location: N/A
Contact Person: N/A

- How to Use This Web Site
- Configuration and Console
- Diagnostics
- Vital Product Data
- Help Server Location Configuration

Figure 19. IBM MSS Family Client Home Page

This Home Page provides a graphic that shows the status of the IBM MSS Family Client. It indicates the current network interfaces installed and shows the status of each port (for example, installed, enabled, or disabled). The current state of each LED is also shown. If the Web browser supports dynamic refresh, then this page will automatically refresh itself approximately every 80 seconds. If you click any of these ports or interfaces, a more detailed description of its status will be shown on a separate Web page.

Click **How to use this Web Site** for instructions about using this site.

Click **Configuration and Console** to bring up the menu shown in Figure Figure 20 on page 63.

Click **Diagnostics** to bring up the menu shown in Figure Figure 21 on page 63.

Click **Vital Product Data** for information about the hardware and operational software. This panel, which is usually used for diagnostics, is not displayed here.

Click **Help Server Location Configuration** to set the path for the optional Help Server. You will need to set this path if you want to use the optional help files for the Web Browser interface.

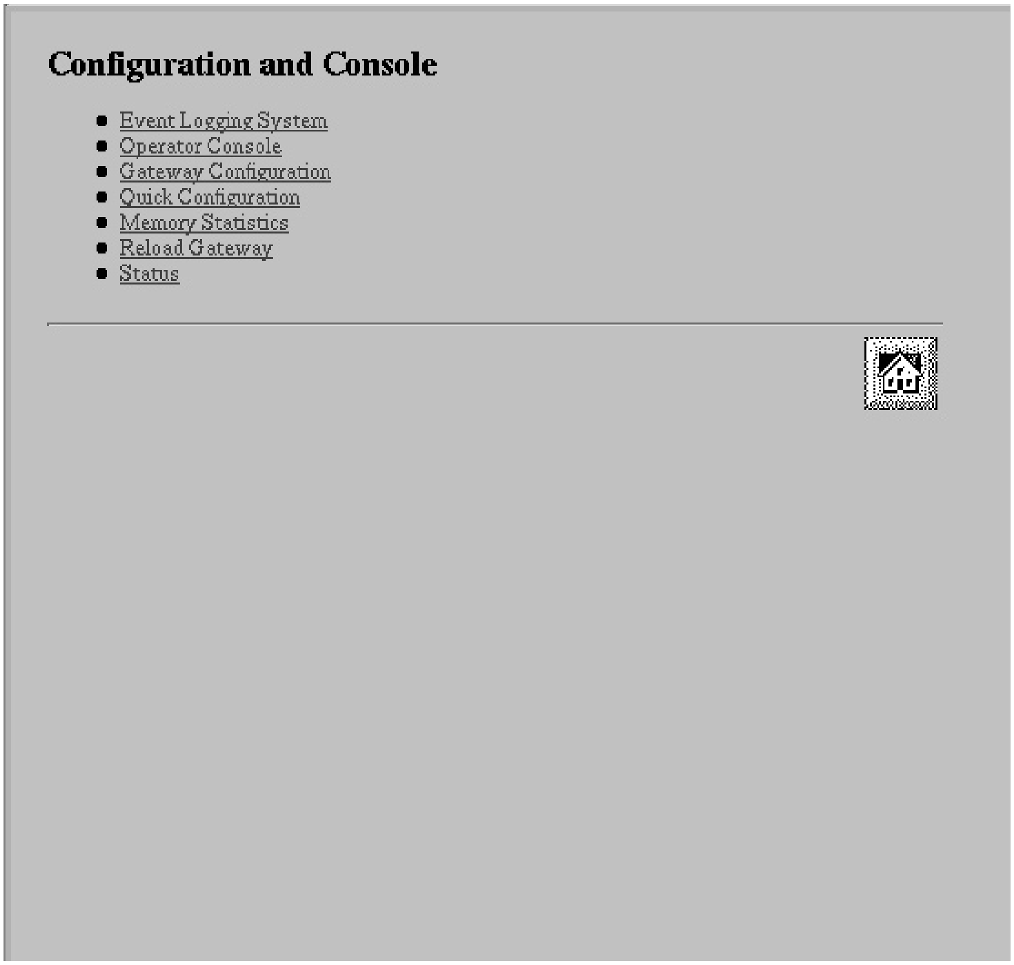


Figure 20. Configuration and Console Page 1

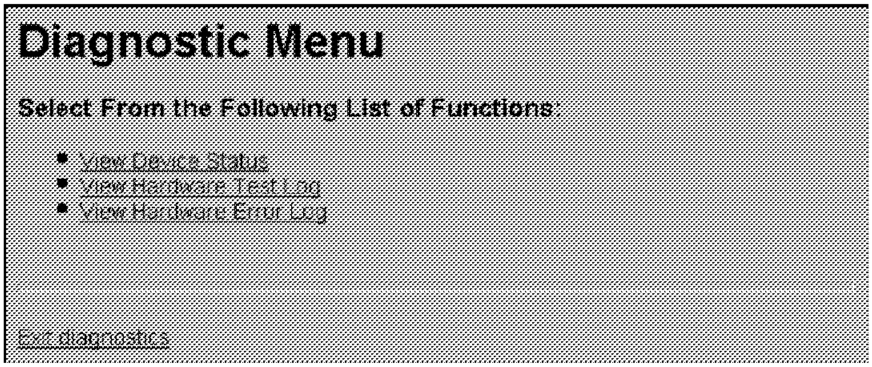
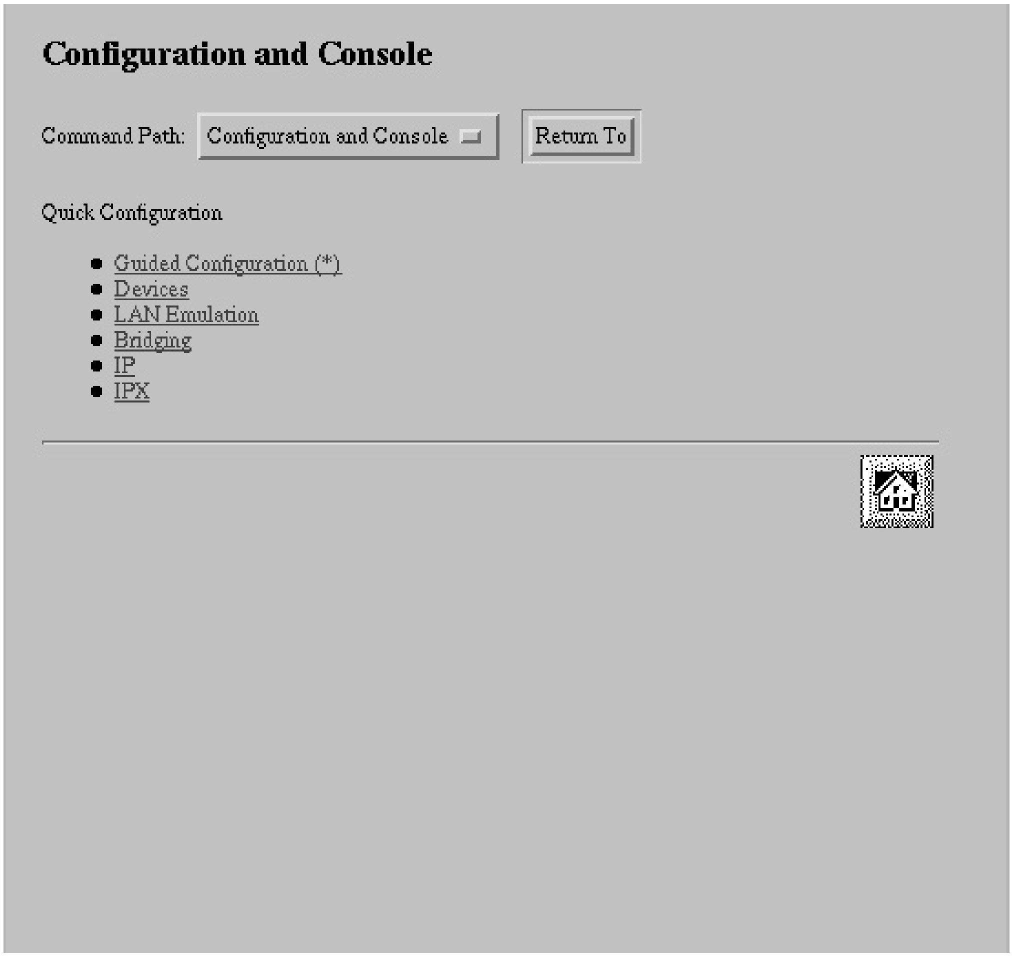


Figure 21. Diagnostic Menu

Configuration and Console Menu

This menu can lead you into various aspects of configuration. To start with quick configuration, click **Quick Configuration**. Figure 22 shows the quick configuration menu. See “Quick Configuration Using the Web Browser Interface” on page 66 for information about quick configuration and guided configuration.



Configuration and Console

Command Path: Configuration and Console

Figure 22. Configuration and Console Page 2

Event Logging System

One of the links on the Configuration and Console page 1 is to the Event Logging System (ELS). The ELS display is similar to the one provided on the command line interface. On the Web interface, going into the ELS will display the most recent events stored in the system memory. In order to get future updates, press the Reload button on your browser. For more details about the ELS message facility, refer to the *Event Logging System Messages Guide*.

Operator Console

The console monitoring interface provides real-time status information very similar to that offered in the command line interface. The menus from the command line interface are presented as a hierarchy of Web links that can easily be traversed with the click of a mouse button. It is possible to jump back several levels in the hierarchy with a single push of a button.

Device Configuration

Important: Exercise caution when using the Web browser to change configuration parameters. Changes to the configuration that are made using the Web browser are written directly to static random access memory (SRAM). You can make unintentional configuration changes that do not take effect until you reset the IBM MSS Family Client. To check that you have the correct parameters, look over the settings for any parameters that you have configured before submitting them.

The Web interface greatly simplifies the configuration of network and protocol parameters. In many cases where it is necessary to remember the individual network numbers on the command line interface, those options are now all presented as menu options on the Web. Also, the Web interface uses the graphical features available to it, such as pick lists, selection lists, radio buttons, and check boxes.

If a particular configuration option needs to prompt you for answers to several questions, those questions are now presented on a single Web page. After all of the questions are filled in, you should press the *Submit* button to send the data back to the IBM MSS Family Client for validation.

The hierarchy of the Web browser interface is very similar to that of the command line interface.

History Function

The Web Configurator uses a selection list and a *Return to* button to provide an advanced history function. Depending upon your choice of HTML browser, a pick list, choice box or pull-down list box will be displayed. This list of selections contains the names of the pages visited under the current branch of the software structure. To return to a previously visited page within the current command pathway, select that entry from the list and click the *Return To* button.

Help System for the Web Browser Interface

Optional, free-of-charge, help files for the Web Browser interface can be downloaded from the Web. Use of the help button located at the bottom of Web Browser configuration panels requires the installation of these help files.

For download instructions and additional information about the help files, point your browser to URL `http://www.networking.ibm.com/nes/neshome.html`.

Quick Configuration Using the Web Browser Interface

Note: This section is most helpful when it is used while you are viewing the IBM MSS Family Client Web interface.

Quick Configuration for the IBM MSS Family Client using the Web interface is divided into the following steps:

- Guided configuration
- Devices
- Bridging - For Token-Ring LAN switches only
- IP
- IPX
- LAN Emulation (MSS Client only)

Guided Configuration

To view the individual steps that are required for quick configuration, select **Guided Configuration** from the menu on Configuration and Console page 2, shown in Figure 22 on page 64. On each step, you will be presented with a link that allows you to skip to the next step. When you submit the form for a step, the results page will contain a link that takes you to the next step in the guided configuration. The results page in the last step of the guided configuration contains a link to take you back to the home page.

If you complete the guided configuration, you will have been through every step of a quick configuration. If you want to change only certain aspects of a quick configuration, use each of the separate steps. For example, to change only LAN emulation parameters, select that step.

Devices

Selecting **Devices** presents a list of the currently configured devices, which are the ATM, Ethernet, or Token-Ring devices. Select an interface and click on the **Submit** button to add the device using the next available network and slot numbers, for example. A **Submit** button is included on the results page if there is still room to add more devices. A **Submit** will not be included on the results page once all the available slots have been filled, so it is impossible to attempt to add too many devices.

Bridging

Selecting **Bridging** presents a form that allows bridging to be configured on each network interface that can support bridging.

IP

Selecting **IP** presents a form that allows IP to be configured on each network interface. For each interface, enable IP by selecting the associated check box. When enabling IP, provide an IP address and mask using the dotted decimal format. The IP address and the subnet mask are the only parameters required to enable IP on an ELAN.

When enabling IP on an ATM device, you are actually configuring Classical IP (RFC 1577). In this case, select a radio button to choose between a *client-only* configuration or a *client and server* configuration. If you select *client-only*, specify the 20-byte ATM address of the remote ARP server that the client will use. If you select *client and server*, specify the selector. The burned-in ESI and the specified selector make up the portion of the ATM address that can be configured.

Note: For quick configuration, the burned-in ESI is the only choice. You are required to set the selector.

When the form is submitted by clicking on the Submit button, IP is configured according to the submitted data and the results are displayed on a new page.

IPX

Selecting **IPX** presents a form that allows IPX to be configured on each network interface that can support IPX. Each eligible interface can be enabled for IPX by selecting the associated check box. If you enable IPX, configure a network number and select the encapsulation type to be used by choosing the appropriate value from the select list presented for each interface.

When you submit the form by clicking the Submit button, IPX is configured according to the submitted data and the results are displayed on a new page.

An Example of Quick Configuration Using the Web Browser Interface

The following procedure shows how to use Quick Configuration to configure LAN emulation using the Web Browser interface:

1. Open the following URL: http://10.1.1.2/
2. From the MSS home page, click **Configuration and Console**.
3. From Configuration and Console click **Quick Configuration**.
   a. Click **LAN Emulation**.

      Change ELAN names if desired, and then click **Submit**.

      LEC is now configured for one Token-Ring and one Ethernet ELAN. Either or both ELANs can be omitted if desired.

      Select **Quick Configuration** from the Command History and click **Return to**.

   b. Click **IP**.

      Enable IP on the desired interfaces. IP must be enabled on at least one interface.

      Change the IP addresses and masks to appropriate values for your network.

      Click **Submit**.

      IP is now configured on the specified interfaces.

      Click the home icon at the bottom of the screen.
4. From the MSS home page, click **Configuration and Console**.

   From Configuration and Console click **Router Configuration**

   Click **RELOAD**.

   Select **Yes** and click the **Submit** button to restart the IBM MSS Family Client.

The IBM MSS Family Client will now be accessible from the network using the IP addresses that were specified in step 3.b.

Chapter 6. The OPCON Process and Commands

This chapter describes the OPCON interface configuration and operational commands. It includes the following sections:

- "What is the OPCON Process?"
- "Accessing the OPCON Process"
- "OPCON Commands"

What is the OPCON Process?

The Operator Console process (OPCON) is the root-level process of the router software user interface. The main function of OPCON is to communicate with processes at the secondary level, such as Configuration, Console, and Event Logging. Using OPCON commands, you may also:

- Display information about device memory usage
- Reload the device software (reboot)
- Telnet or ping to other routers or hosts
- Display status information about all router processes
- Manipulate the output from a process
- Change the OPCON intercept character
- Return to the Base LAN Switch console

Accessing the OPCON Process

When the router starts for the first time, a boot message appears on the console. Then the OPCON prompt (*) appears on the console, indicating that the OPCON process is active and ready to accept commands.

The OPCON process allows you to configure, change, and monitor all of the router's operating parameters. While in the OPCON process, the router is forwarding data traffic. When the router is booted and enters OPCON, a copyright logo and an asterisk (*) prompt appears on the locally attached console terminal. This is the OPCON (OPerator's CONsole) prompt, the main user interface that allows access to second-level processes.

Some changes to the router's operating parameters made while in OPCON take effect immediately without requiring reinitializing of the router. If the changes do not take effect, use the **reload** command at the * prompt.

At the * prompt, an extensive set of commands enables you to check the status of various internal software processes, monitor the performance of the router's interfaces and packet forwarders, and configure various operational parameters.

OPCON Commands

This section describes the OPCON commands. Commands that are needed more often appear before the "- - - - -" separator. Each command includes a description, syntax requirements, and an example. The OPCON commands are summarized in Table 5 on page 70. To use them, access the OPCON process and enter the appropriate command at the OPCON prompt (*).

Table 5. OPCON Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Configuration*	Accesses the device’s configuration process. (`talk 6`)
Console*	Accesses the device’s console process. (`talk 5`)
Event Logging System*	Accesses the device’s event logging process. (`talk 2`)
ELS Console*	Accesses the device’s secondary ELS Console process. (`talk 7`)
Logout	Logs off a remote console.
Ping	Pings a specified IP address.
Reload	Reloads the device.
Telnet	Connects to another device.
- - - - - -	- -
Diags	Displays device status and the contents of the hardware test log and the hardware error log.
Divert	Sends the output from a process to a console or other terminal.
Flush	Discards the output from a process.
Halt	Suspends the output from a process.
Intercept	Sets the OPCON default intercept character.
Memory	Reports the router’s memory usage.
Return	Returns to the LAN switch console when you are configuring through the LAN switch.
Status	Shows information about all router processes.
Talk	Connects to another router process and enables the use of its commands.

***:** When you use this command for the first time, you will be reminded that you can use **Ctrl-P** to return to the MOS Operator Console prompt (*).

Configuration

Use the **configuration** command to access the device’s configuration process (`talk 6`). See “Chapter 7. The CONFIG Process (CONFIG - Talk 6) and Commands” on page 81 for more information.

Syntax:

configuration

Example:

```
* configuration

(To return to the MOS Operator Console prompt (*), press Control-P)

Gateway user configuration
Config>
```

Console

Use the **console** command to access the device’s console and monitoring process (`talk 5`). See “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 117 for more information.

Syntax:

console

Example:

```
* console

CGW Operator Console

+
```

Diags

Use the **diags** command to display the Diagnostic Main Menu. The diagnostic menus allow you to enable, disable and test hardware adapters or ports. Diagnostic menus have on-screen help for the various options and status information that is available.

You can use the “b” (back) key to return to any previous menu. Use the “e” (exit) key to exit the diagnostics and return to the OPCON command prompt.

Syntax:

diags

Divert

Use the **divert** command to send the output from a specified process to a specified terminal. This command allows you to divert the output of several processes to the same terminal to simultaneously view the output. The **divert** command is commonly used to redirect MONITR output messages to a specific terminal. The router allows only certain processes to be redirected.

The **divert** command requires the PID and tty# (number of the output terminal). To obtain these values, use the OPCON **status** command. The terminal number can be the number of either the local console (tty0) or one of the remote consoles (tty1, tty2). The following example shows Event Logging System messages generated by the MONITR process (2) being sent to a remote console *tty1* (1).

Event messages are displayed immediately even though you may be in the middle of typing a command. The display and keyboard have separate buffers to prevent command confusion. The following example shows the MONITR process connected to TTY0 after executing the **divert 2 0** command. If you want to stop the output, enter **halt 2**. The **halt** command is described in “Halt” on page 73.

Syntax:

divert *pid tty#*

Example:

```
* divert 2 0
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL    TTY0
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
```

```
 7    ELSCon    DET     --
 8    ROpCon    IDL    TTY1
 9    ROpCon    RDY    TTY2 jlg@128.185.40.40
 10   WEBCon    IDL    --
```

Els

Use the **els** command to access the device’s secondary ELS console process, (`talk 7`). See “Accessing the Secondary ELS Console Process, ELSCon (Talk 7)” on page 28 for more information.

Syntax:

els

Event

Use the **event** command to access the device’s event logging process, (`talk 2`). See “Chapter 12. Using the Event Logging System (ELS)” on page 137 for more information.

Syntax:

event

Flush

Use the **flush** command to clear the output buffers of a process. This command is generally used before displaying the contents of the MONITR’s FIFO buffer to prevent messages from scrolling off the screen. Accumulated messages are discarded.

The router allows only certain processes to be flushed. To obtain the *pid* and *tty#*, use the OPCON **status** command. In the following example, after executing the **flush 2** command, the output of the MONITR process is sent to the Sink (it has been flushed).

Syntax:

flush *pid*

Example:

```
* flush 2
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL    Sink
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCon    IDL    TTY1
9    ROpCon    RDY    TTY2 jlg@128.185.40.40
10   WEBCon    IDL    --
*
```

Halt

Use the **halt** command to suspend all subsequent output from a specified process until the **divert**, **flush**, or **talk** OPCON command is issued to the process. The router cannot redirect all processes. **Halt** is the default state for output from a process. To obtain the PID for this command, use the OPCON **status** command. In the following example, after executing the **halt 2** command, the MONITR process is no longer connected to TTY0. Event messages no longer appear.

Syntax:

halt *pid*

Example:

```
* halt 2
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCon    IDL    TTY1
9    ROpCon    RDY    TTY2 jlg@128.185.40.40
10   WEBCon    IDL    --
```

Intercept

Use the **intercept** command to change the OPCON intercept character. The intercept character is what you enter from other processes to get back to the OPCON process. The default intercept key combination is **Ctrl-P**.

The intercept character ***must*** be a control character. Enter the ˆ (shift 6) character followed by the letter character you want for the intercept character.

Syntax:

intercept ˆ *character*

Example:

```
* intercept ˆa
```

From this example, the intercept character is now **Ctrl-A**.

Logout

Use the **logout** command to terminate the current session for the user who enters the logout command. If the console login is enabled, this command will require the next user to log in using an authorized userid/password combination. If the console login is not enabled, the OPCON prompt appears again.

Syntax:

logout

Memory

Use the **memory** command to obtain and display information about the router’s global heap memory usage. The display helps you to determine if the router is being utilized efficiently. For an example of memory utilization, see Figure 23.

See “Memory” on page 124 for memory usage via talk 5.

Syntax:

memory

Example:

```
* memory
Number of bytes:  Busy = 319544, Idle = 1936, Free = 1592
```

Busy Specifies the number of bytes currently allocated.

Idle Specifies the number of bytes previously allocated but freed and available for reuse.

Free Specifies the number of bytes that were never allocated from the initial free storage area.

Note: The sum of the Idle and Free memory equals the total available heap memory.

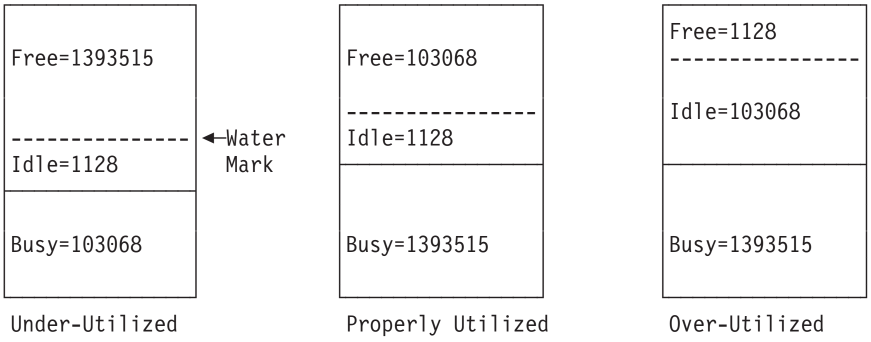


Figure 23. Memory Utilization

Ping

Use the **ping** command to have the router send ICMP Echo messages to a given destination (that is, “pinging”) and watch for a response. This command can be used to isolate trouble in the internetwork.

Syntax:

ping *dest-addr [src-addr data-size ttl rate tos data-value]*

The ping process is done continuously, incrementing the ICMP sequence number with each additional packet. Each matching received ICMP Echo response is reported with its sequence number and the round-trip time. The granularity (time resolution) of the round-trip time calculation is usually around 20 milliseconds, depending on the platform.

To stop the ping process, type any character at the console. At that time, a summary of packet loss, round-trip time, and number of unreachable ICMP destinations will be displayed.

When a broadcast or multicast address is given as destination, there may be multiple responses printed for each packet sent, one for each group member. Each returned response is displayed with the source address of the responder.

You can specify the size of the ping (number of data bytes in the ICMP message, excluding the ICMP header), value of the data, time-to-live (TTL) value, rate of pinging, and TOS bits to set. You can also specify the source IP address. If you do not specify the source IP address, the router uses its local address on the outgoing interface to the specified destination. If you are validating connectivity from any of the router’s other interfaces to the destination, enter the IP address for that interface as the source address.

Only the destination parameter is required; all other parameters are optional. By default the size is 56 bytes, the TTL is 64, the rate is 1 ping per second, and the TOS setting is 0. The first 4 bytes of the ICMP data are used for a timestamp. By default the remaining data is a series of bytes with values that are incremented by 1, starting at X'04', and rolling over from X'FF' to X'00' (for example, X'04 05 06 07 . . . FC FD FE FF 00 01 02 03 . . .'). These values are incremented only when the default is used; if the data byte value is specified, all of the ICMP data (except for the first 4 bytes) is set to that value and that value is not incremented. For example, if you set the data byte value to X'FF', the ICMP data is a series of bytes with the value X'FF FF FF . . .'.

Example:

```
* ping
Destination IP address [0.0.0.0]? 192.9.200.1
Source IP address [192.9.200.77]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
Ping TOS (00-FF) [0]? e0
Ping data byte value (00-FF) [ ]?
PING 192.9.200.77-> 192.9.200.1:56 data bytes,ttl=64,every 1 sec.
56 data bytes from 192.9.200.1:icmp_seq=0.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=1.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=2.ttl=255.time=0.ms


----192.9.200.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=0/0/0 ms
```

Reload

Use the **reload** command to reboot the router by loading in a new copy of the router software. When you use this command from a remote console, you install a new software load without going to the router. This command executes the same functions as pressing the reset button except that the router will not dump (if so configured). Before the reload takes effect, you are prompted to confirm the reload. You are also prompted if you have not saved the configuration changes.

Syntax:

reload

Example:

```
* reload
Are you sure you want to reload the gateway (Yes or No)?
```

Return

Use the **return** command to return to the LAN switch interface when accessing the MSS Family Client through the LAN switch.

Note: If you use **Ctrl-B** instead of return when attached through a Telnet session, the Telnet session will end.

Syntax:

return

Status

Use the **status** command to display information about all router processes. By entering the PID after the **status** command, you can look at the status of only the desired process. The following example shows the total status display.

Syntax:

status *pid*

Example:

```
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    IOW     --
6    Config    IOW    TTY1
7    ELSCon    DET     --
8    ROpCon    IOW    TTY1 128.185.46.101
9    ROpCon    RDY    TTY2 128.185.46.104
10   WEBCon    IDL    --
```

Pid Specifies the PID. This is the process to talk to from OPCON, or it can be an argument to the STATUS command to request status information about a specific process.

Name Specifies the process name. It usually corresponds to the name of the program that is running in the process.

Status
Specifies one of the following:

- **IDL** Specifies that the process is idle and waiting for completion of some external event, such as asynchronous I/O.
- **RDY** Specifies that the process is ready to run and is waiting to use the CPU.
- **IOW** Specifies that the process is waiting for synchronous I/O, usually its expected standard input, to complete.
- **DET** Specifies that the process has output ready to be displayed and it is either waiting to be attached to a display console or waiting to have its output diverted to a specified console.

FZN Specifies that the process is frozen due to an error. This usually means the process is trying to use a device which is faulty or incorrectly configured.

TTY*n* Specifies the output terminal, if any, to which the process is currently connected.

TTY0 Local console

TTY1 or TTY2
Telnet consoles.

Sink Process has been flushed.

Two dashes (--)
Process has been halted.

Comments
Specifies the user's login IP address provided during login when a user is logged in using Telnet (ROpCon).

Talk

You can use the **configuration**, **console**, or **event** comands to connect to other processes, such as CONFIG, GWCON, or MONITR, or use the **talk** command. After connecting to a new process, you can send specific commands to and receive output from that process. You cannot talk to the TASKER or OPCON processes.

To obtain the PID, use the OPCON **status** command. Once you are connected to the second-level process, such as CONFIG, use the intercept character, **Ctrl-P**, to return to the * prompt.

Syntax:

talk *pid*

Example:

```
* talk 5

CGW Operator Console

+
```

When using third-level processes, such as `SNMP Config>` or `SNMP>`, use the **exit** command to return to the second level.

Telnet

Use the **telnet** command to remotely attach to another router or to a remote host. The only optional parameter is the terminal type that you want to emulate.

You can use the **telnet** command with IPv4 or with IPv6 addresses.

A router has a maximum of five Telnet sessions: two servers (inbound to the router), and three clients (outbound from the router).

Note: To use Telnet in a pure bridging environment, enable Host Services.

Syntax:

telnet *ip-address terminal-type*

Example 1: `telnet 128.185.10.30` or **`telnet 128.185.10.30 23`** or **`telnet 128.185.10.30 vt100`**

```
Trying 128.185.10.30  ...
Connected to 128.185.10.30
Escape character is '^]'
```

When telneting to a non-existent IP address, the router displays:

```
Trying 128.185.10.30  ...
```

To enter the Telnet command mode, type the escape character-sequence, which is **Ctrl-]**, at any prompt.

```
telnet>
```

If you Telnet into a router,

- Press ← **Backspace** to delete the last character typed on the command line.

  Note: When using a VT100 terminal, do not press ← **Backspace** because it inserts invisible characters. Press **Delete** to delete the last character.
- Press **Ctrl-U** at the `telnet>` prompt to delete the whole command line entry so that you can reenter a command.

The Telnet command mode consists of the following subcommands:

close Close current connection

display
Display operating parameters

mode Try to enter line-by-line or character-at-a-time mode

open Connect to a site

quit Exit Telnet

send Transmit special characters ('send ?' for more)

set Set operating parameters ('set ?' for more)

status Print status information

toggle Toggle operating parameters ('toggle ?' for more)

z Suspend Telnet

? Print help information

The **status** and **send** subcommands have one of two responses depending on whether or not the user is connected to another host. For example:

Connected to a host:

```
   telnet>    status
Connected to 128.185.10.30    Operating in character-at-a-time mode.    Escape character is ^].

   telnet>    send ayt
```

Note: The send command currently supports only ayt.

Not connected to a host:

```
 telnet>    status
 Need to be connected first.

 telnet>    send ayt

 Need to be connected first.
```

Use the **close** subcommand to close a connection to a remote host and terminate the Telnet session. Use the **quit** subcommand to exit the **telnet** command mode, close a connection, and terminate a Telnet session.

```
telnet>    close
```

or

```
telnet>    quit

logout
*
```

Chapter 7. The CONFIG Process (CONFIG - Talk 6) and Commands

This chapter describes the CONFIG process configuration and operational commands. It includes the following sections:

- "What is CONFIG?"
- "Entering and Exiting CONFIG" on page 87
- "CONFIG Commands" on page 88

What is CONFIG?

The Configuration process (CONFIG) is a second-level process of the router user interface. Using CONFIG commands, you can:

- Set or change various configuration parameters
- Add or delete an interface to the hardware configuration
- Enter the Boot CONFIG command mode
- Enter the Quick Configuration mode
- Clear, list, or update configuration information
- Enable or disable console login
- Communicate with third-level processes, including protocol environments

CONFIG lets you display or change the configuration information stored in the router's nonvolatile configuration memory. Changes to system and protocol parameters do not take effect until you reload the router software. (For more information, refer to the OPCON **reload** command in "What is the OPCON Process?" on page 69).

Note: You must enter the **write** command to save the changes in the device's flash memory.

The CONFIG command interface is made up of levels that are called modes. Each mode has its own prompt. For example, the prompt for the SNMP protocol is `SNMP config>`.

If you want to know the process and mode you are communicating with, press **Enter** to display the prompt. Some commands in this chapter, such as the **network** and **protocol** commands, allow you to access and exit the various levels in CONFIG. See Table 6 on page 88 for a list of the commands you can issue from the CONFIG process.

Config-Only Mode

Config-Only mode is entered if the configuration file that you are using is empty or no protocols are configured. Config-Only mode can also be entered manually to recover from an invalid configuration that is causing the router to crash during start-up.

Automatic Entry Into Config-Only Mode

Config-Only mode is entered if the router detects a problem during operation or during router initialization.

The following conditions cause the router to enter Config-Only mode:

- The software load does not match the device configuration. Specifically, an attempt is made to configure a device or data link that is not supported by the software load.
- Deletion of all router interface information.

If the router enters Config-Only mode because an unsupported device is configured:

- Change the device information to match the hardware installed in (and supported by) the router, or change the unsupported device to “null device”.
- Enter the **Reload** command from the `Config (only)>` prompt.
- The router will automatically enter OPCON (*).

Manual Entry Into Config-Only Mode

To enter Config-Only mode, do one of the following:

- Reload the router with no configuration.
- Reload the router with no interfaces configured.
- Reload the router with no protocols configured.

See “Chapter 3. Using MSS Family Client Firmware” on page 39 for more information.

Quick Configuration

Quick Configuration (Quick Config) provides a minimal set of commands that allow you to configure bridging protocols and routing protocols present in the router load. You can also configure an SNMP community with WRITE_READ_TRAP access. This is useful during initial setup because the configuration program uses SNMP SET commands to transfer the configuration.

Important: At least one network device must be configured before using quick config. To add a device, use the **add device** command at the `config(only)>` or `config>` prompt.

Quick Config complements the existing configuration process by offering a shortcut. This shortcut allows you to configure the minimum number of parameters for these bridging protocols and routing protocols without having to exit and enter the different configuration processes. The other parameters are set to selected defaults.

Situations that call for the router to be quickly configured are:

- Blank or corrupted configuration memory, such as when one of the following situations occurs:
  - The router is configured for the first time.
  - Voltage fluctuations caused corruption of configuration memory.
- Demonstration purposes, for which the router needs to be quickly configured to demonstrate its capabilities.

- Bench-marking tests to get the tests going without having to learn the router’s operating system commands.

Quick Config operates as follows:

- It asks a series of questions with default values.
- It offers a short-cut to the detailed configuration of the normal mode command set.

Quick Config sets a number of default parameters based upon how you answer the configuration questions. What cannot be configured with Quick Config can be configured using Config after exiting Quick Config.

You cannot delete Quick Config information from within Quick Config. However, you can correct information either by exiting and returning to Quick Config, or by entering the **reload** command as a response to some Quick Config questions.

For complete information on using the Quick Config software, see “Appendix A. Quick Configuration Reference” on page 329.

Manual Entry Into Quick Config Mode

You might want to run Quick Config manually to demonstrate the router’s capabilities or to reconfigure dynamically to perform benchmark tests without having to learn the router’s operating system commands.

To enter Quick Config, type **qconfig** at the `Config>` prompt.

Exiting from Quick Config Mode

To exit Quick Config, restart by entering **r** from any prompt. Follow the queries until you enter **no** and then enter **q** to quit. The router returns to either the `Config (only)>` or the `Config>` prompt.

Configuring User Access

The router configuration process allows for a maximum of 50 user names, passwords, and levels of permission. Each user needs to be assigned a password and level of permission. There are three levels of permission: *Administration, Operation,* and *Monitoring*.

For more information, see 89.

Technical Support Access

If you are the system administrator, when you add a new user for the first time, you are asked if you want to add Technical Support access. If you answer yes, Technical Support is granted the same access privileges that you have as system administrator.

The password for this account is automatically selected by the software and is known by your service representative. This password can be changed using the **change user** command; however, if you do change the password, customer service cannot provide remote support. For additional information on the use of the **change user** command, see “Change” on page 90.

Configuring Spare Interfaces

Occasionally, you may need to configure a new interface along with its routing protocols without having to restart the device. You can accomplish this by configuring a number of ***spare interfaces*** on your device. Spare interfaces are useful if:

- You are adding ATM LAN Emulation clients.

  Use spare interfaces to add Token-Ring or Ethernet ATM LAN Emulation clients to an existing ATM interface.
- Adding router interfaces to new domains.

To configure a spare interface:

1. Access the CONFIG process by entering **configuration**.
2. Configure the number of spare interfaces for the device using the **set spare-interfaces** command.
3. Exit the CONFIG process by pressing **Ctrl-P**.
4. Reload the device.

Example:

```
* configuration
Config> set spare 2
Config>
*reload
Are you sure you want to reload the gateway? (Yes or [No]) yes
```

When the device reloads, the spare interfaces are installed as null devices.

To use one of the spare interfaces:

1. Access the CONFIG process by entering **configuration**.
2. Configure the spare interface by using the **net** command to configure the interface or add ATM LAN Emulation clients.
3. Configure the various protocols and features using the **protocol** and **feature** commands.
4. Exit the CONFIG process by pressing **Ctrl-P**.
5. Access the GWCON process by entering **console**.
6. Bring the new interface online to the network using the **activate** command.

The following example shows how to configure and activate a new ATM LAN Emulation Client on which the IP protocol is configured. The ATM LAN Emulation Client and IP configurations are not shown.

```
* configuration
Config> net 0
ATM User Configuration
ATM Config> le-client
ATM LAN Emulation Clients Configuration
LE Client config> add token-ring
Added Emulated LAN as interface 6
LE Client config> config 6
ATM LAN Emulation Client configuration
⋮
(Here you would configure the ATM LAN Emulation Client)
⋮
Token Ring Forum Compliant LEC Config> exit
LE Client config> exit
ATM Config> exit
Config> protocol ip
IP Conifg>
⋮
(Here you would configure IP on the ATM LAN Emulation Client)
⋮
```

```
.
IP Config> exit
Config> write
ctrl-p
* console
+ activate 6
Interface 6 activated successfully
```

Restrictions for Spare Interfaces

The **activate** command cannot be used to activate a new interface on the network under the following conditions:

- You have already entered a **delete interface** command. The device must be restarted if ***any*** interface has been deleted. You cannot delete a spare interface (indicated by ***null*** in list displays).
- The spare interface is the only interface that enables a protocol or feature. The protocol or feature must already be enabled on an existing interface before it can be used by a spare interface.
- The new spare interface has a header size or trailer size greater than the sizes for other interfaces.
- There is not enough memory to allocate receive buffers for the new interface.
- SRB is added on the spare interface.

In these cases, you must restart the device to bring the new interface or SRB online.

Note: When using the configuration program, use the following to work with spare interfaces:

1. Make the configuration changes for the spare interface on the device
2. Enter the **activate** command on the device to bring the spare interface, protocols, and features online
3. Retrieve the configuration using the configuration program
4. Save the retrieved configuration into the configuration program database

There are requirements for certain functions. These are:

BGP Use the BGP **reset neighbor** command to activate new neighbors.

IPX Use the **reset** command to activate static routes, static services, and filter lists on the spare interface.

Bridging

- Bridging was not already active.
- NetBIOS filters are defined on the spare interface.
- The spare interface caused a change to the bridge personality or behavior.

IP Use the reset IP command to bring configuration changes online for access-controls and packet-filters.

Resetting Interfaces

Occasionally, you might need to change the configuration of a network interface along with its bridging and routing protocols without restarting the device. The **reset** command allows you to disable a network interface and then enable it using new interface, bridging and routing configuration parameters.

Using the CONFIG Process

The interface, protocols and features configuration parameters are changed using the CONFIG process (talk 6) commands. The talk 6 commands affect the contents of the configuration memory. The configuration changes are activated by issuing the GWCON process (talk 5) **reset** command.

To reset an interface:

1. Access the CONFIG process (talk 6).
2. Use the **net** command and other commands to change configuration parameters.
3. Use the **protocol** and **feature** commands to change the interface-based configuration parameters.
4. Exit the CONFIG process by pressing **Ctrl-P**.
5. Access the GWCON process (talk 5).
6. Use the **reset** command to reset the interface and the protocols and features on the interface.

Example:

```
* configuration
Config> net 0
ATM User Configuration
ATM Config> le-client
ATM LAN Emulation Clients Configuration
LE Client config> config 6

. . . change ATM LAN Emulation Client parameters . . .

Ethernet Forum Compliant LEC Config> exit
LE Client config> exit
ATM Config> exit

Config> protocol ipx
IPX Config>

. . . change IPX parameters on the ATM LAN Emulation Client . . .

IPX Config> exit
Config>
*console
+reset 6
Resetting net 6 Eth/1...successful
```

Note: When using the configuration program, do the following to make configuration changes to existing interfaces:

1. Make the configuration changes for the interface on the device
2. Enter the **reset** command to reset interface, protocol and feature parameters
3. Retrieve the configuration using the configuration program
4. Save the retrieved configuration into the configuration program database

Restrictions for Resetting Interfaces

The **reset** command cannot be used to reset a network interface if:

- You have already entered a **delete interface** command. The device must be reloadedif any interface has been deleted.
- You have configured a larger MTU.

- You have configured a routing protocol or bridging on the interface, but that routing protocol or bridging is not currently active in the device.

In these situations, you must reload the device to activate the configuration changes.

You can change the configuration parameters of the following types of interfaces, but you cannot activate the changes using the **reset** command:

- ATM

You must reload the device to activate these configuration changes.

You can change the configuration parameters of the following protocols and features, but you cannot activate the changes using the **reset** command:

- AppleTalk
- Vines
- MARS

You must reload the device to activate these configuration changes.

There are also requirements for certain functions. They are:

Bridging
- Bridging was not already active.
- NetBIOS filters are defined on the interface you are resetting.
- The reset interface caused a change to the bridge personality or behavior.

BGP
Use the BGP **reset neighbor** command to activate neighbor configuration changes.

APPN
Use the **activate_new_config** command to activate configuration changes.

IPX
Use the IPX **reset** command to activate configuration changes for static routes, static services, and filter-lists.

SNMP
Use the SNMP **revert** command to activate configuration changes.

Entering and Exiting CONFIG

To enter the CONFIG process from OPCON and obtain the CONFIG prompt, enter the **configuration** command. Alternatively, you can enter the OPCON **talk** command and the PID for CONFIG. The PID for CONFIG is 6.

```
* configuration
```

or

```
* talk 6
```

The console displays the CONFIG prompt (`Config>`). If the prompt does not appear, press the **Enter** key again.

To exit CONFIG and return to the OPCON prompt (*), enter the intercept character. (The default is **Ctrl-P** .)

CONFIG Commands

This section describes each of the CONFIG commands. Each command includes a description, syntax requirements, and an example. The CONFIG commands are summarized in Table 6.

After accessing the CONFIG environment, enter the configuration commands at the `Config>` prompt.

Table 6. CONFIG Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Add	Adds an interface to the router configuration, or a user to the router.
Boot	Enters Boot CONFIG command mode.
Change	Changes a user’s password or a user’s parameter values associated with this interface. Also changes a slot/port of an interface.
Clear	Clears configuration information.
Delete	Deletes an interface from the router configuration or deletes a configured user.
Disable	Disables command completion, login from a remote console, system memory dumping and rebooting, or a specified interface.
Enable	Enables command completion, login from a remote console, system memory dumping and rebooting, or enables a specified interface.
Event	Enters the Event Logging System configuration environment.
Feature	Provides access to configuration commands for independent router features outside the usual protocol and network interface configuration processes.
List	Displays system parameters, hardware configuration, a complete user list.
Network	Enters the configuration environment of the specified network.
Patch	Modifies the router’s global configuration.
Performance	Provides a snapshot of the main processor utilization statistics.
Protocol	Enters the command environment of the specified protocol.
Qconfig	Initiates the Quick Config process.
Set	Sets system-wide parameters for buffers, host name, inactivity timer, packet size, prompt level, number of spare interfaces, location, and contact person.
Time	Keeps track of system time and displays it on the console.
Unpatch	Restores patch variables to default values.
Write	Writes the current configuration information to the nonvolatile memory.

Add

Use the **add** command to add an interface to the configuration, or user-access. This command also recreates device records if the configuration is inadvertently lost.

Syntax:

add	device
	user . . .

device *device_type additional-config-info*

With the **add device** command, you must enter the interface device type (*device_type*). You are prompted for additional configuration parameters. This additional information varies by device and platform. Refer to

"Accessing Network Interface Configuration and Operating Processes" on page 28 for additional information about device type and configuration parameters.

Note: If you are adding more than one interface, the order in which you add them is important because the router assigns a sequential interface number to the device when it is added. This interface number is an index number in the device list; it links the device with other protocol configuration information, such as the IP addresses associated with the device. (For more information, refer to the **list devices** command, "List" on page 95.)

All device and protocol configuration information related to network interfaces is stored by interface number. Any changes made to interface numbers will invalidate much of the device configuration information in the protocols.

Example:

```
add device atm
Device Slot x(0-3) 0?
Adding CHARM ATM Adapter device in slot 0 port 1 as interface x
(where x is the interface number assigned)
```

To determine which devices you can add, use the **add devices ?** command.

user *user_name*

Gives a user access to the device. You can authorize up to 50 users to access the device. Each *user_name* is eight characters and is case-sensitive.

When the first user is added, console login is automatically enabled. Each user added must be assigned one of the permission levels defined in Table 7.

When users are added, set login authentication to local. Otherwise a remote server must be used.

Table 7. Access Permission

Permission Level	Description
Administrator (A)	Displays configuration and user information, adds/modifies/deletes configuration and user information. The Administrator can access any router function.
Operator (O)	Views router configuration, views statistics, runs potentially disruptive tests, dynamically changes router operation, and restarts the router. Operators cannot modify the permanent router configuration. All actions can be undone with a system restart.
Monitor (M)	Views router configuration and statistics but cannot modify or disrupt the operation of the router.
Tech Support	Allows your service representative to gain access to the router if a password is forgotten. Cannot be assigned to users.

Note: To add a user, you must have administrative permission. You do not have to reinitialize the router after adding a user.

Example:

```
add user John
Enter password:
Enter password again:
Enter permission (A)dmin, (O)perations, (M)onitor [A]?
Do you want to add Technical Support access? (Yes or [No]):
```

Enter password
Specifies the access password for the user. Limited to 80 alphanumeric characters and is case-sensitive.

Enter password again
Confirms the access password for the user.

Enter permission
Specifies the permission level for the user: A, O, or M (see Table 7 on page 89).

Boot

Use the **boot** command to enter the Boot CONFIG command environment. For Boot CONFIG information, see “Chapter 8. Using BOOT Config to Perform Change Management” on page 105.

Syntax:

boot

Change

Use the **change** command to modify an interface in the configuration,change your own password, or change user information.

Syntax:

change device . . .
user

Example:

```
MSS Client Config>change device
Device Interface #(0-8) [0]? 2
Device Domain #(0-15) [0]? 15
Changing Token Ring device interface #2 to domain 15
```

device *device_type*
With the **change device** command you can:

- Change the slot of an existing interface. (Change slot x in interface record n to y where slot y is unoccupied.)
- Replace the slot in an existing interface with the slot in another. (Interface configuration for slot x will become interface configuration for slot y. Interface records for slot y will be deleted.)

When the target slot is occupied:

1. If you select the “replace” option is selected, the interface configuration for slot x will become the interface configuration for slot y. Interface records for slot y will be deleted.

You cannot use the **change device** command on an ATM device.

```
MSS Client Config>list dev
Ifc 0   ATM                             Slot: 1  Port: 1
Ifc 1   NHRP LANE Shortcut Interface
Ifc 2   Token Ring                      Domain: 0
Ifc 3   Token Ring                      Domain: 1
Ifc 4   Token Ring                      Domain: 2
Ifc 5   Token Ring                      Domain: 3
Ifc 6   ATM Token Ring LAN Emulation
Ifc 7   ATM Token Ring LAN Emulation
Ifc 8   ATM Virtual Net
MSS Client Config>cha dev
Device Interface #(0-8) [0]?
Device domain change not supported for ATM devices.
```

user Modifies the user information that was previously configured with the **add user** command.

Note: To change a user, you must have administrative permission.

Example:

```
change user
User name: []
Change password? (Yes or No)
Change permission? (Yes or [No])
```

Clear

Use the **clear** command to delete the router’s configuration information from nonvolatile configuration memory.

Attention: Use this command only after calling your service representative.

Syntax:

clear

all

ap2 (AppleTalk 2)

arp (ARP)

asrt (Adaptive Source Route Protocol)

atm (Asynchronous Transfer Mode)

bgp (Border Gateway Protocol)

boot

device

dn (DECnet)

els (Event Logging System Information)

hostname

ip (IP)

ipx (Novell IPX)

lnm

mcf

named-profiles

ospf (OSPF routing protocol)

prompt

snmp

tcp/ip-host

time (Time of day information)

user

vines (Banyan VINES)

To clear a process from nonvolatile configuration memory, enter the **clear** command and the process name. To clear all information from configuration memory, except for device information, use the **clear all** command. To clear all information, including the device information, use the **clear all** command and then the **clear device** command.

The **clear user** command clears all user information except the router console login information. This is left as enabled (if it was configured as enabled) even though the default value is “disabled”.

Notes:

1. To clear user information, you must have administrative permission.
2. There may be other items in the list, depending upon what is included in the software load.

Example: **`clear els`**

```
You are about to clear all Event Logging configuration information
Are you sure you want to do this (Yes or No):
```

Note: The previous message appears for any parameter configuration you are clearing.

Delete

Use the **delete** command to remove an interface from the list of devices stored in the configuration, or to remove a user. To use the **delete** command, you must have administrative permission.

Syntax:

delete interface . . .

user . . .

interface [*intfc#*]
To delete an interface, enter the interface or network number as part of the command. (Only devices that were added with the **add device** command can be deleted.) To obtain the interface number that the router assigns, use the **list device** command.

The delete interface command deletes the device configuration and any protocol information for that interface. However, the router will continue to run the previous configuration until it is .

user *user_name*
Removes user access to the router for the specified user.

Disable

Use the **disable** command to disable command completion, login from a remote console, system memory dumping, rebooting, or a specified interface.

Syntax:

disable command-completion

console-login

interface . . .

reboot-system . . .

command-completion

Use the **disable command-completion** command to disable the automatic command completion function. See “Command Completion” on page 33 for a discussion of the automatic command completion function.

console-login
Disables the user from being prompted for a user ID and password on the physical console. The default is disabled.

interface *interface#*
Causes the specified interface to be disabled after issuing the **reload** command. The default is enabled.

reboot-system
Disables the rebooting of the system when a serious error occurs. This may be desirable if the network service personnel wish to troubleshoot the error on-line. System rebooting cannot be disabled unless memory dumping is also disabled. If you attempt to disable system rebooting while memory dumping is enabled, system rebooting is aborted and the following message is displayed:

```
System reboot not disabled:  memory dumping must be disabled first
```

Enable

Use the **enable** command to enable command completion, login from a remote console, system memory dumping, rebooting, or a specified interface.

Syntax:

enable command-completion

console-login

interface . . .

reboot-system . . .

command-completion

Use the **enable command-completion** command to enable the automatic command completion function, which assists with the command syntax. See “Command Completion” on page 33 for a discussion of the automatic command completion function.

console-login
Enables the user to be prompted for a user ID and password on the physical console. This is useful for security situations. If you do not configure any administrative users and you enable this feature, the following message appears:

```
Warning: Console login is disabled until an
administrative user is added.
```

Attention: Before enabling console login, save the configuration with console login disabled. If login authentication is set to a remote server using Radius or Tacacs+ and the router is unable to reach the authentication server, then access to the router is denied. By disabling the console login, a lock-out situation is prevented.

interface *interface#*

Causes the interface to be enabled after issuing the **reload** command.

modem-control [carrier-wait or ring-wait] [service1 or service2]

Sets up the router for login on the physical console, if the physical console is connected to the router through a modem. Before using this command, be sure to:

- Set your modem for auto-answer.
- Verify that the console baud rate is equal to the modem baud rate.
- Verify that the cable connecting the modem to the router is configured correctly.
- Turn echo off by using the ATE0 command.
- Run in quiet mode by using the ATQ1 command.
- Verify that any necessary jumpers are set. Refer to your router's *User's Guide* more information.

The router automatically hangs up the modem when you log out. Also, if your modem becomes disconnected from the router while you are using it, the router logs you out.

Specify the service port for both the **enable modem-control carrier-wait** and the **enable modem-control ring-wait** commands. For routers with two service ports, also specify to which service port you connected the modem, either **service1** or **service2**. To enable *both* service ports, enable them separately.

Note: No console connection can be made with the router after enabling modem control unless you clear all configuration and restart the router.

You can tell the router to wait for the carrier-detect signal from the modem before sending Request to Send. This is the standard method of modem control.

You can tell the router to wait for the ring-indication signal before raising Request to Send or Data Terminal Ready. This is provided for countries requiring an earlier handshake.

Example:

```
Config> enable modem-control carrier-wait service1
```

reboot-system

Enables the rebooting of the system when a serious error occurs.

Event

Use the **event** command to enter the Event Logging System (ELS) environment so that you can define the messages that will appear on the console. Refer to "Chapter 12. Using the Event Logging System (ELS)" on page 137 for information about ELS.

Syntax:

event

Feature

Use the **feature** command to access configuration commands for specific router features outside of the protocol and network interface configuration processes.

Syntax:

feature [*feature#* or *feature-short-name*]

All IBM MSS Family Client features have commands that are executed by:

- Accessing the configuration process to initially configure and enable the feature, as well as perform later configuration changes.
- Accessing the console process to monitor information about each feature, or make temporary configuration changes.

The procedure for accessing these processes is the same for all features. The following information describes the procedure.

Enter a question mark after the **feature** command to obtain a listing of the features available for your software release.

To access a feature's configuration prompt, enter the **feature** command followed by the feature number or short name. Table 8 lists available feature numbers and names.

Table 8. IBM MSS Family Client Feature Numbers and Names

Feature Number	Feature Short Name	Accesses the following feature configuration process
2	MCF	MAC Filtering
6	QoS	Quality of Service

Once you access the configuration prompt for a feature, you can begin entering specific configuration commands for the feature. To return to the CONFIG prompt, enter the **exit** command at the feature's configuration prompt.

List

Use the **list** command to display configuration information for all network interfaces, or configuration information for the router.

Syntax:

list configuration

devices

named-profile

patches . . .

users . . .

vpd

configuration

Displays configuration information about the router.

Example: `list configuration`

devices

Displays the relationship between an interface number and the hardware interface. You can also use this command to check that a device was added correctly issuing the **add** command.

Example: `list devices`

```
Ifc 0   ATM                              Slot: 1  Port: 1
Ifc 1   NHRP LANE Shortcut Interface
Ifc 2   Token Ring                       Domain: 0
Ifc 3   Token Ring                       Domain: 1
Ifc 4   Token Ring                       Domain: 2
Ifc 5   Token Ring                       Domain: 3
Ifc 6   ATM Token Ring LAN Emulation
Ifc 7   ATM Token Ring LAN Emulation
Ifc 8   ATM Virtual Net
```

patches

Displays the values of patch variables that have been entered using the **patch** command.

Example:

```
list patches
Patched variable            Value

mosheap-lowmark             20
```

vpd Displays the hardware and software vital product data.

Network

Use the **network** command to enter the network interface configuration environment for supported networks. Enter the interface or network number as part of the command. (To obtain the interface number, use the CONFIG **list device** command.) The appropriate configuration prompt (for example, `TKR Config>`) will be displayed. See the network interface configuration chapters in this book for complete information on configuring your types of network interfaces.

Syntax:

network *interface#*

Notes:

1. If you change a user-configurable parameter, you may use the GWCON **reset interface** command, or you may **reload** the router for the change to take effect. To do so, enter the **reload** command at the OPCON prompt (*).
2. Not all network interfaces are user-configurable. For interfaces that you cannot configure, you receive the message: `That network is not configurable`.

Patch

Use the **patch** command for modifying the router's global configuration. Patch variables are recorded in nonvolatile configuration memory and take effect immediately; you do not have to wait for the next restart of the router. This command should be used only for handling uncommon configurations. Anything that you commonly configure should still be handled by using the specific configuration commands. The following is a list of the current patch variables documented and supported for this release.

Syntax:

patch	bgp-subnets
	ip-default-ttl
	ip-mtu
	more-lines
	mosheap-lowmark
	ospf-import-rate
	ping-size
	ping-ttl
	rip-static-suppress

bgp-subnets *new value*
If you want the BGP speaker to advertise subnet routes to its neighbors, set *new value* to 1. The default is 0.

dls-ignore-lfs *new value*
When set to 1, DLSw ignores the "largest frame" size bits in source-routed frames when setting up a circuit. This avoids circuit setup problems with some older LAN products that do not set these bits correctly. The default is 0.

ip-default-ttl *#_of_packets*
The TTL used in packets that are originated by the router. The default is 64.

Note: It is preferable to set this parameter with the **set ttl** IP configuration command. (See the "Set" section of the "Using and Configuring IP" chapter of *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide* .) This patch variable remains for compatibility with configurations from older releases.

ip-mtu *bytes*
This parameter limits the IP MTU size to the specified value. When this parameter is set, the IP MTU size on a given network interface is set to the lesser of the ip-mtu value and the largest value that network interface's configured frame size can accommodate.

more-lines *#_of_lines*
The number of lines to display on the console when listing long output.

mosheap-lowmark *new value*
This parameter specifies the percentage of free MOS heap memory, at which the device notifies the operator that an out-of-memory error is imminent. This notification allows the operator to take action to free up MOS heap memory before the device receives an error and stops.

When the operator receives notification, the operator can reconfigure the router and then reboot, minimizing the outage to the network. Specifying 0 for this parameter suppresses this warning.

Valid Values: 0 to 100

Default Value: 10

ospf-import-rate *rate*
Number of routes imported per second.

ping-size *bytes*
The size of the data portion (that is, excluding IP and ICMP headers) of the ICMP PING packet that is sent via the `IP>`**ping** command. Default: 56 bytes. (The size of the PING data can also be entered as a parameter of the **ping** command as described in the “Ping” section of the “Monitoring IP” chapter of *Multiprotocol Switched Services (MSS) Interface Configuration and Software User’s Guide* .)

ping-ttl *seconds*
The TTL (time-to-live) sent in PINGs by the `IP>`**ping** command. Default: 64. (The TTL can also be entered as a parameter of the **ping** command as described in the “Ping” section of the “Monitoring IP” chapter of *Multiprotocol Switched Services (MSS) Interface Configuration and Software User’s Guide*.

rip-static-suppress *new value*
When set to a non-zero value, static routes will not be advertised by RIP over a given interface unless the `IP config>` **enable send static** command is given for the interface. This changes the semantics of the **enable send static** command. When rip-static-suppress is equal to 0 (the default), the list of the routes advertised via RIP is the union of those specified by the interface’s RIP flags.

Note: You must specify the complete name of the patch variable that you want to change. You cannot use an abbreviated syntax for the patch name.

Performance

Use the **performance** command at the `Config>` prompt to enter the configuration environment for performance. See “Chapter 14. Configuring and Monitoring Performance” on page 201 for more information.

performance

Protocol

Use the **protocol** command at the `Config>` prompt to enter the configuration environment for the protocol software installed in the router.

Syntax:

protocol [*prot#* or *prot_name*]

The **protocol** command followed by the desired protocol number *or* short name lets you enter a protocol’s command environment. After you enter this command, the prompt of the specified protocol appears. From the prompt, you can enter commands specific to that protocol. To return to `Config>`, enter the **exit** command.

Notes:

1. To see the names and numbers of the protocols in your software load, at the `Config>` prompt, enter **list configuration**.
2. When you change a user-configurable parameter, you may be able to use the protocol's GWCON **reset** command, or you may have to restart the router for the change to take effect. To do so, enter the **reload** command at the OPCON prompt (*).

   The changes you make through CONFIG are kept in a configuration database in nonvolatile memory and are recalled when you restart the router.

Qconfig

Use the **qconfig** command to initiate Quick Config. Quick Config allows you to configure parameters for bridging and routing protocols without entering separate configuration environments.

Syntax:

qconfig

Note: For complete information on using the Quick Config software provided with your router, see "Appendix A. Quick Configuration Reference" on page 329.

Set

Use the **set** command to configure various system-wide parameters.

Syntax:

set	contact-person . . .
	down-notify . . .
	global-buffers
	hostname
	inactivity-timer
	input-low-water
	location . . .
	logging disposition
	packet-size
	prompt
	receive-buffers
	spare-interfaces

contact-person *sysContact*

Sets the name or identification of the contact person for this managed SNMP node. There is a limit of 80 characters for the *sysContact* name length.

This variable is for information purposes only and has no effect on router operation. It is useful for SNMP management identification of the system.

down-notify *interface# # of seconds*
Allows the user to specify the number of seconds before declaring an interface as being down. The normal maintenance packet interval is 3 seconds, and it takes four maintenance failures to declare the interface as down.

The **set down-notify** command is used primarily when tunneling LLC traffic over an IP network using OSPF. If an interface goes down, OSPF cannot detect it fast enough because of the length of time that it takes for an interface to be declared down. Therefore, LLC sessions would begin to timeout. You can set the down-notify timer to a lower value, allowing OSPF to sense that an interface is down quicker. This enables an alternate route to be chosen more quickly, which will prevent the LLC sessions from timing out.

Note: If the **set down-notify** command is executed on one end of a serial link, the same command must be performed at the other end of the link or the link may not come up and stay up.

Interface#
The number of the interface you are configuring.

# of seconds
The down notification time value that specifies the maximum time that will elapse before a down interface is marked as such. Large values will cause the router to ignore transient connection problems, and smaller values will cause the router to react more quickly. The range of values is 1 to 300 seconds and the default is 0, which sets the 3-second period. Setting the down notification time to 0 will restore the default time for that interface.

The **list devices** command will show the down notification time setting for any interface that has the default value overridden.

global-buffers *max#*
Sets the maximum number of global packet buffers, which are the packet buffers used for locally originated packets. The default is to autoconfigure for the maximum number of buffers (up to 1000). To restore the default, set the value to 0. To display the setting for global-buffers, use the **list configuration** command.

hostname *name*
Adds or changes the router name. The router name is for identification only; it does not affect any router addresses. The *name* must be less than 78 characters and is case sensitive.

inactivity-timer *#_of_min*
Changes the setting of the Inactivity Timer. The Inactivity Timer logs out a user if the remote or physical console is inactive for the period of time specified in this command. This command affects only consoles that require login. The default setting of 0 turns the inactivity timer off, indicating that no logoff is performed, no matter how long a console remains inactive.

input-low-water *interface# low_ #_of_receive_buffers*
Allows you to configure the value of the low number of receive buffers, or packets, on a per-interface basis, thus overriding the default values.

The memory allocation strategy changes to conserve buffers when the number of free buffers is equal to or less than the low or low-water mark value. When a packet is received, and the current value of the interface is less than the low water value, then that packet is eligible for flow control (dropping).

The range of values is 1 to 255. The default is both platform and device specific. Setting the value to 0 restores the autoconfigured default.

Interface# is the number of the interface you are configuring. *Low_#_of_receive_buffers* is the low water value.

Lowering the value will make it less likely that packets from this interface will be dropped when sent on congested networks. However, lowering the value may negatively affect performance if it drops packets to the extent that the receive queue is frequently empty. Raising the value has the opposite effect.

Type the **QUEUE** or **BUFFER** command at the GWCON prompt (**+**) to show the low setting.

location *sysLocation*

Sets the physical location of an SNMP node. There is a limit of 80 characters for the *sysLocation* name length. This variable is for information purposes only and has no effect on router operation. It is useful for SNMP management identification of the system.

logging disposition *setting*

Changes the SRAM record for the default logging disposition. This command affects the MONITR process (that is, it changes the default setting at startup).

The logging disposition *settings* are as follows:

- **console** writes to the console (equivalent to the OPCON **divert 2 0** command).
- **detached** holds the data and does not print it (equivalent to the OPCON **halt 2** command).
- **flush** discards the data (equivalent to the OPCON **flush 2** command).

If you have a printing terminal attached to the router’s console port, you can obtain a hard copy of the startup messages by setting the logging disposition to **console**, and restarting the router.

packet-size *max_packet_size_in_bytes*

Establishes or changes the maximum size for global buffers and receive buffers. If you specify a value of 0 as the maximum packet size, the size of receive buffers for an interface is based on that interface’s configured packet size and the packet size of global buffers are autoconfigured. If you specify a non-zero value, the configured value is used as the global buffer packet size and any interfaces that have a configured packet size that is larger than the maximum packet size will use the maximum packet size for their receive buffers. A value of 0 (for autoconfigure) is the default.

Attention: Use this command only under direct instructions from your service representative. ***Never*** use it to reduce packet size – ***only*** to increase it.

prompt *user-defined-name*

Adds a user-defined name as a prefix to all operator prompts, replacing the hostname.

The user-defined-name can be any combination of characters, numbers, and spaces up to 80 characters. Special characters may be used to request additional functions as described in Table 9.

Example:

```
set prompt
What is the new MOS prompt [y]? AnyHost 99
AnyHost 99 Config>
```

Table 9. Additional Functions Provided by the Set Prompt Level Command

Special Characters	Function Provided by the Set Prompt Level Command
$n	Displays the hostname. This is useful when you want the hostname included in the prompt. For example: Config> **set prompt** What is the new MOS prompt [y]? **$n** hostname:: Config>
$t	Displays the time. For example: Config> **set prompt**. What is the new MOS prompt [y]? **$t** 02:51:08[GMT-300] Config>
$d	Displays the current date-month-year. For example: Config> **set prompt**. What is the new MOS prompt [y]? **$d** 26-Feb-1997 Config>
$v	Displays the software VPD information in the following format: program-product-name Feature xxxx Vx.x PTFx RPQx
$e	Erases one character *after* this combination within the user-defined prompt.
$h	Erases one character *before* this combination within the user-defined prompt.
$_	Adds a carriage return to the user-defined prompt.
$$	Displays the $.
Note: You can combine these commands. For example: Config> **set prompt** What is the new MOS prompt [y]? **$n::$d** hostname::26-Feb-1997 Config>	

receive-buffers *interface# max#*

Adjusts the number of private receive buffers for most interfaces.

The range is 5 to 1000.

Table 10. Default and Maximum Settings for Interfaces

Interface	Default	Maximum
ATM	80	1000
TKR	40	250

spare-interfaces ***n***

Defines ***n***, the number of spare interfaces, for this device. See “Configuring Spare Interfaces” on page 84 for additional information.

Time

Use the **time** command to set the IBM MSS Family Client system clock and date, and to display the values on the user console. These values can then be used to time-stamp ELS messages.

Note: The IBM MSS Family Client has a hardware clock that maintains the date and time after router reinitialization.

Syntax:

time host . . .
list
offset
set . . .
sync . . .

host *IP_address*

Sets the IP address of the RFC 868-compliant host that will be used as the time source. This is the address of a host which will respond to an empty datagram on UDP port 37 with a datagram containing the current time.

list Displays all configured time-related parameters. This includes the current time (if set) and the source of the time (operator or IP address from which time was last received).

```
Example: time list
05:20:27  Wednesday December 7, 1994
Set by: operator
Time Host:  131.210.4.1
Sync Interval: 10 seconds GMT
Offset:  -300 minutes
```

offset *minutes*

Defines the time zone, in minutes, offset from GMT (Greenwich Mean Time). Note that values west of GMT are negative. For example, EST is 5 hours earlier than GMT, so the command would be **time offset -300**.

Valid values: -720 to 720

Default value: 0

set <*year month date hour minute second***>**

Prompts you to set the current time. If you do not specify the entire time in the command, you are prompted for the remaining values. You can change the date as shown in the following example.

```
Example: time set
year [1996] 1997
month [12]?
date [6]? 7
hour [11]? 12
minute [3]?
second [2]?
```

sync *seconds*

Sets the period, in seconds, at which the router will poll the time host for the current time.

Unpatch

Use the **unpatch** command to restore the values of the patch variables entered with the **patch** command to their default values. See the **patch** command in “Patch” on page 97 for details.

Syntax:

unpatch	*variable_name*

Note: You ***must*** specify the complete name of the patch variable to be restored.

Update

Use the **update** command to update the configuration memory when you receive a new software load.

Syntax:

update	version-of-SRAM

Follow the instructions on the release notice sent with the software. The **update** command is the last command that you enter when loading new software. After you enter this command, the console displays a message indicating configuration memory is being updated.

Write

Use the **write** command to save a configuration to the device before reloading.

Syntax:

write

If you fail to issue the write command and try to reload the device, you will be asked if you want to save the configuration. The configuration is saved in the next CONFIG on the hard disk in the bank you are currently using.

Chapter 8. Using BOOT Config to Perform Change Management

This chapter describes how to use the Boot Configuration process. This chapter includes the following sections:

- “Understanding Change Management”
- “Using the Trivial File Transfer Protocol (TFTP)”
- “Loading an Image at a Specific Time” on page 106

Understanding Change Management

Change management is the handling of software and configuration data for an IBM MSS Family Client. This involves:

1. Moving code and configuration data to and from the IBM MSS Family Client
2.
3. Selecting and activating specific combinations of software and configuration.

The change management functions are available by entering the **boot** command at the `Boot config>` prompt (talk 6), or the firmware should the box be in a condition where the flash memory does not contain viable software (that is, you cannot access talk 6).

The IBM MSS Family Client code and configuration data storage resource is divided into areas called “system banks” (banks for short), each containing a single version of the operational code and any other files pertinent to that release of the code. Up to four configuration files are associated with each bank’s software.

Using the Trivial File Transfer Protocol (TFTP)

TFTP is a file transfer protocol that runs over the Internet UDP protocol. This implementation provides multiple, simultaneous TFTP file transfers between an IBM MSS Family Client’s non-volatile configuration memory, image bank, and remote hosts.

TFTP allows you to:

- Get a configuration file from a server to an IBM MSS Family Client
- Put a configuration file from an IBM MSS Family Client to a server
- Get operational code.

TFTP transfers involve a *client* node and a *server* node. The client node generates a TFTP Get or Put request onto the network. The IBM MSS Family Client acts as a client node by generating TFTP requests from the IBM MSS Family Client console using the `Boot config>` process **tftp** command.

The client can transfer a copy of a configuration file or image file stored in the image bank of a server.

The server is any device (for example, a personal computer or workstation) that receives and services the TFTP requests. Use the ELS subsystem TFTP message log to view the transfer in progress.

Loading an Image at a Specific Time

There may be occasions when you may want to load a device on a specific day and time when you will be unavailable. You can configure the device to perform a timed load using the **timedload activate** command. Other commands allow you to view a device’s scheduled load information or cancel a scheduled load. See “Change Management Configuration Commands” on page 107 for information on these commands.

Chapter 9. Configuring Change Management

This chapter describe the Change management configuration commands. It includes the following sections:

- "Accessing the Change Management Configuration Environment"
- "Change Management Configuration Commands"

Accessing the Change Management Configuration Environment

To enter the change management configuration command environment, use the CONFIG **boot** command. When the router's software is initially loaded, it is running in the OPCON process, signified by the * prompt. From the * prompt:

1. Enter **talk 6**.
2. At the `Config>` prompt, type **boot**.

To return to the CONFIG process, type **exit**.

Change Management Configuration Commands

This section describes the Change Management Configuration commands. Each command includes a description, syntax requirements, and an example. Table 11 summarizes the Change Management Configuration commands.

After accessing the Change Management Configuration environment, enter the configuration commands at the `Boot config>` prompt.

Table 11. Change Management Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 22.
Add	Adds an optional description to a configuration file.
Copy	Copies configuration files to or from banks.
Describe	Displays information about the stored loadfile images.
Erase	Erases a stored image or a configuration file.
List	Displays information about configuration files and scheduled load information.
Lock	Prevents the device from overwriting the selected configuration with any other configuration.
Set	Selects code bank and configuration to be used.
TFTP	Initiates TFTP file transfers between the IBM MSS Family Client and remote servers.
Timedload	Schedules a load into the device on a specific day and time, cancels a scheduled load, or displays scheduled load information.
Unlock	Removes the lock from a configuration allowing the configuration to be updated by the device.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 23.

Add

Use the **add** command to add an optional description to a configuration file.

Syntax:

add configuration *file description*

load *image description*

Example: `Boot config>` **`add`**

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:30 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (F): [F]
Select the source configuration:  (1, 2, 3, 4): [1] 3
Enter the description of the file: () New config for today

Attempting to set description for bank F configuration 3.

Operation completed successfully.


Boot config>list
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

Copy

Use the **copy** command to copy configuration files to and from banks.

Syntax:

copy configuration *file*

Example: `Boot config>`**`copy configuration`**

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:37 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (F): [F]
Select the source configuration:  (1, 2, 3, 4): [1]
Select the destination bank:  (F): [F]

Select the destination configuration:  (1, 2, 3, 4): [3]
Copy SW configuration from: bank F, configuration 1
                         to: bank F, configuration 3.

Operation completed successfully.
```

If the copy fails you may receive one of the following messages:

Error: File copy failed.

This condition occurs when the copy operation fails for reasons other than copying to the active configuration. The most common cause is specifying the same source and destination configurations. When you list (see “List” on page 110) the configurations, CORRUPT appears next to the bank that is damaged.

Describe

Use the **describe** command to display information about a stored image.

Syntax: describe

Example: Boot config>**describe**

```
+-------------------------+
|          BANK F         |
| Product ID -   MSSC     |
| Version   2.1           |
| Mod       0 PTF       0 |
| Feat.  0000 RPQ       0 |
| Date        31 Mar 1998 |
+-------------------------+
```

Erase

Use the **erase** command to erase a stored image or a configuration file.

Syntax:

erase	configuration [file]
	load [image]

config

Erases a configuration file. Enter the config number to be erased after the **erase** command.

Example: Boot config>**erase configuration**

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (F): [F]
Select the configuration to erase:  (1, 2, 3, 4): [1] 3
Erase SW configuration file from bank F, configuration 3.

Operation completed successfully.


Boot config>list
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - NONE        |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

If the erasure fails, a message indicating the failure appears on the console with the banks that failed.

List

Use the **list** command to display information about the load image and configuration files are available and active. This command may also be used to display boot options and scheduled load information.

Syntax:

list

Example: `Boot config>`**`list`**

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

 Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date:  June 26, 1997
Time:  16:30
The load modules are in bank F.
The configuration is CONFIG 1 in bank F.
Boot config>
```

The possible file status descriptors are:

ACTIVE
The file is currently loaded and is running on the MSS Family Client

AVAIL This is a valid file that can be made ACTIVE.

CORRUPT
The file was damaged or not loaded into the MSS Family Client completely. The file must be replaced.

LOCAL
The file will be used only on the next reload or reset. After the file is used, it will be placed in AVAIL state.

PENDING
This file will be loaded on the next reload, reset, or power-up of the MSS Family Client.

Lock

Use the **lock** command to prevent the device from overwriting the selected configuration with any other configuration.

Syntax:

lock

Example: `Boot config>`**`lock`**

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Select the source bank:  (F): [F]
Select the source configuration:  (1, 2, 3, 4): [1] 4
Attempting to lock bank F and configuration 4.

Operation completed successfully.


Boot config>list
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                |                   |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL   L   |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

Note: Note that config 4 is marked with an “L.”

Set

Use the **set** command to select the code bank, the configuration to use, and the duration of use. The valid durations are:

once The configuration is active for the next boot only.

always
The configuration is active for all subsequent boots until changed again.

Syntax:

set

Example: `Boot config>set`

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (F): [F] f
Select the source configuration:  (1, 2, 3, 4): [1] 4
Select the duration to use for booting:  (once, always): [always]
Set SW to boot using bank F and configuration 4, always.

Operation completed successfully.


Boot config>list
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

TFTP

Use the **tftp** command to initiate TFTP file transfers between the MSS Family Client and remote servers.

Syntax:

tftp get	config
tftp put	config
	load single *image*

Example: Boot config>**tftp get load single**

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE  *   |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote file name: : (/u/bin) /usr/MSS Family Clientload/nce.img
Select the destination bank:  (F): [F] f
  TFTP SW load image
  get:   /usr/MSS Family Clientload/nce.img
  from:  192.9.200.1
  to:    bank F.

Operation completed successfully.
```

Notes:
When putting files to a server:

1. Make sure that the files on the target server have the appropriate permissions that would allow anyone to write to those files. If not, the put operation will fail.
2. You must be aware of the files you are putting to the target server.

Timedload

Use the **timedload** command to schedule a load on a device, cancel a scheduled load, or view scheduled load information.

This command allows you to load the device outside peak network traffic periods when support personnel may not be present.

Note: You may also use the Configuration Program to schedule a reload for a device, which is not affected by reloads or power outages. These circumstances would normally cause the reload to be lost. See the chapter “Using the Configuration Program” in *Configuration Program User’s Guide* for details.

Syntax:

timedload	activate
	deactivate
	view

activate

Schedules a load on the device. You will be prompted for information for a time-activated load similar to the **tftp get load** and **tftp get config** commands. See “TFTP” on page 112 for information about the parameters.

Time of day to load the device

Specifies the date and time to load the device. Specify the value as *YYYYMMDDHHMM*, where:

YYYY is the four-digit year

Note: If the current month on the device is December, the year data must be the current year or the following year. Otherwise, if the current month on the device is January through November, the year data must be the current year.

MM is the two digit month.

MM Valid Values: 01 to 12 with 01 representing January.

DD is the two-digit day of the month.

DD Valid Values: 01 to 31, depending on the value of MM.

HH is the two-digit hour in 24-hour time.

HH Valid Values: 00 to 23

MM is the two-digit minute of the hour.

MM Valid Values: 00 to 59

The following are examples of scheduling a load from different sources.

Example 1. Load modules and configuration source is a remote host:

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Time Activated Load Processing...

Select the bank to use:  (F): [F] f
Do you want to put load modules into the bank? (Yes, No, Quit): [Yes] yes

Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote modules directory: : (/u/bin) /usr/601bin/205img
The destination bank is bank F
TFTP SW load image
  get:   /usr/601bin/205img/
  from:  192.9.200.1
  to:    bank F.
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'
tftp: connect to '192.9.200.1'

Operation completed successfully.

Do you want to put a configuration into the bank? (Yes, No, Quit): [Yes] yes

Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote file name: : (config.dat) /tftpboot/192.9.200.6.config
The destination bank is bank F
Select the destination configuration:  (1, 2, 3, 4): [1] 1
TFTP SW configuration file
```

```
  get:   /tftpboot/192.9.200.6.config
  from:  192.9.200.1
  to:    bank F, configuration 1.
tftp: connect to '192.9.200.1'

Operation completed successfully.

Time of day to load the router (YYYYMMDDHHMM) []? 199706261630
The load timer has been activated.
Boot config>
```

Example 2. Load modules and configuration source is a bank:

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL       |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Time Activated Load Processing...

Select the bank to use:  (F): [F] f
Do you want to put load modules into the bank? (Yes, No, Quit): [Yes] no

Do you want to put a configuration into the bank? (Yes, No, Quit): [Yes] no

Select the configuration to use:  (1, 2, 3, 4): [1] 1

Time of day to load the router (YYYYMMDDHHMM) []? 199706261630
The load timer has been activated.
Boot config>
```

deactivate

Cancels a scheduled load.

Example 1: Deactivate the time activated load

```
Boot config>timedload deactivate
Deactivate Load Timer Processing...

Do you want to deactivate the load timer? (Yes, No, Quit): [No] yes
The load timer has been deactivated.
Boot config>
```

view Displays scheduled load information.

```
Boot Config> timedload view
Time Activated Load Schedule Information...

The router is scheduled to reload as follows.

Date:  June 26, 1997
Time:  16:30
The load modules are in bank F.
The configuration is CONFIG 1 in bank F.
Boot config>
```

Unlock

Use the **unlock** command to allow the device to overwrite the selected configuration that was previously locked.

Syntax:

unlock

Example: `Boot config>unlock`

```
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL   L   |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

```
Select the source bank:  (F): [F]
Select the source configuration:  (1, 2, 3, 4): [1] 4
Attempting to unlock bank F and configuration 4.

Operation completed successfully.
Boot config>list
+------ BankF -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                                | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE      |                                | 01 Jan 1970 00:24 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

Note: Note that config 4 is no longer marked with an “L.”

Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands

This chapter describes the GWCON process and includes the following sections:

- “What is GWCON?”
- “Entering and Exiting GWCON”
- “GWCON Commands” on page 118

What is GWCON?

The Gateway Console (monitoring) process, GWCON (also referred to as CGWCON), is a second-level process of the router user interface.

Using GWCON commands, you can:

- List the protocols and interfaces currently configured in the router.
- Display memory and network statistics.
- Set current Event Logging System (ELS) parameters.
- Test a specified network interface.
- Communicate with third-level processes, including protocol environments.
- Enable and disable interfaces.
- Activate dynamically configured devices.

The GWCON command interface is made up of levels called modes. Each mode has its own prompt. For example, the prompt for the SNMP protocol is `SNMP>`.

If you want to know the process and mode you are communicating with, press **enter** to display the prompt. Some commands in this chapter, such as the **network** and **protocol** commands, allow you to access the various modes in GWCON.

Entering and Exiting GWCON

To enter GWCON from OPCON (*), choose one of the following methods:

1. Enter the OPCON **console** command:

   ```
   * console
   ```

2. At the OPCON prompt, enter the **status** command to find the PID of GWCON. (See page 21 for a sample output of the **status** command.)

   ```
   * status
   ```

   Then, enter the **talk** command followed by the PID number for GWCON:

   ```
   * talk 5
   ```

The console displays the GWCON prompt (+). If the prompt does not appear, press **enter**. Now, you can enter GWCON commands.

To return to OPCON, enter the OPCON intercept character. (The default is **Ctrl-P**.)

GWCON Commands

This section contains the GWCON commands. Each command includes a description, syntax requirements, and an example. The GWCON commands are summarized in Table 12.

To use the GWCON commands, access the GWCON process by entering **talk 5** and enter the GWCON commands at the (+) prompt.

Table 12. GWCON Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 22.
Activate	Enables a newly configured spare interface.
Buffer	Displays information about packet buffers assigned to each interface.
Clear	Clears network statistics.
Configuration	Lists status of the current protocols and interfaces.
Disable	Takes the specified interface off line.
Error	Displays error counts.
Event	Enters the Event Logging System environment.
Feature	Provides access to console commands for independent router features outside the usual protocol and network interface console processes.
Interface	Displays network hardware statistics or statistics for the specified interface.
Memory	Displays memory, buffer, and packet data.
Network	Enters the console environment of the specified network.
Performance	Provides a snapshot of the main processor utilization statistics.
Protocol	Enters the command environment of the specified protocol.
Queue	Displays buffer statistics for a specified interface.
Reset	Disables the specified interface and then re-enables it using new interface, protocol and feature configuration parameters.
Statistics	Displays statistics for a specified interface.
Switch-Interface	Enters the console environment of the LAN Switch Interface which allows you to display hardware bridging statistics.
Test	Enables a disabled interface or tests the specified interface.
Uptime	Displays time statistics for the router.

Activate

Use the **activate** command to enable a spare interface and its protocols on this device. See "Configuring Spare Interfaces" on page 84 for more information.

Syntax:

activate *interface#*

Buffer

Use the **buffer** command to display information about packet buffers assigned to each interface.

Note: Each buffer on a device is the same size and is dynamically built. Buffers vary in size from one device to another.

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

buffer [*network#* or]

Example:

```
buffer
                  Input Buffers        Buffer sizes                   Bytes
Nt  Interface   Req Alloc Low Curr   Hdr  Wrap  Data Trail Total    Alloc
0   ATM/0        80    80  20   80    84    94  9234    32  9444   755520
1   NHRPL/0       0     0   0    0    82    94  9188     0  9364        0
2   TKR/0         0     0   0    0    83    94  2052     7  2236        0
3   TKR/1         0     0   0    0    83    94  2052     7  2236        0
4   TKR/2         0     0   0    0    83    94  2052     7  2236        0
5   TKR/3         0     0   0    0    83    94  2052     7  2236        0
6   TKR/4         0     0   0    0   198    94  4384     0  4676        0
7   TKR/5         0     0   0    0   198    94  4384     0  4676        0
8   ATM/1         0     0   0    0    84    94  9234     0  9412        0
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Buffers:

Req Number of buffers requested.

Alloc Number of buffers allocated.

Low Low water mark (flow control).

Curr Current number of buffers on this device. The value will be 0 if the device is disabled. When a packet is received, if the value of *Curr* is below *Low*, then the packet is eligible for flow control. (See the **queue** command for conditions.)

Buffer Sizes:

Hdr Sum of the maximum hardware, MAC, and data link headers.

Wrap Allowance given for MAC, LLC, or Network layer headers due to protocol wrapping.

Data Maximum data link layer packet size.

Trail Sum of the largest MAC and hardware trailers.

Total Overall size of each packet buffer.

Bytes Alloc
Amount of buffer memory for this device. This value is determined by multiplying the values of *Alloc x Total*.

Clear

Use the **clear** command to delete statistical information about one or all of the router’s network interfaces. This command is useful when tracking changes in large counters. Using this command does not save space or speed up the router.

GWCON Commands

Enter the interface (or net) number as part of the command. To get the interface number, use the GWCON **configuration** command.

Syntax:

clear *interface#*

Configuration

Use the **configuration** command to display information about the protocols and network interfaces. The output is displayed in three sections, the first section lists the router identification, software version, boot ROM version, and the state of the auto-boot switch. The second and third sections list the protocol and interface information.

Syntax:

configuration

Example:

```
IBM MSS Client
Host name: MSS Client
Version: MSSC Feature 0 V2.1 Mod 0 PTF 0 RPQ 0

Num Name  Protocol
0   IP     DOD-IP
3   ARP    Address Resolution
7   IPX    NetWare IPX
11  SNMP   Simple Network Management Protocol
12  OSPF   Open SPF-Based Routing Protocol
23  ASRT   Adaptive Source Routing Transparent Enhanced Bridge
25  LNM    LAN Network Manager
29  NHRP   Next Hop Resolution Protocol

Num Name  Feature
2   MCF    MAC Filtering
6   QOS    Quality of Service

9 Networks:
Net Interface  MAC/Data-Link        Hardware                     State
0   ATM/0      ATM                  ATM                          Up
1   NHRPL/0    NHRP LANE Shortcut   ATM                          Up
2   TKR/0      Token-Ring/802.5     Token-Ring                   Up
3   TKR/1      Token-Ring/802.5     Token-Ring                   Up
4   TKR/2      Token-Ring/802.5     Token-Ring                   Up
5   TKR/3      Token-Ring/802.5     Token-Ring                   Up
6   TKR/4      Token-Ring/802.5     ATM                          Up
7   TKR/5      Token-Ring/802.5     ATM                          Up
8   ATM/1      ATM                  Virtual ATM interface        Up
```

- The first line gives the product name.
- The second line indicates whether a host name is configured.
- The third line lists the program/product number, Feature Number, Version, Release, PTF and RPQ information.
- The remaining lines list the configured protocols, followed by the configured features.

The following information is displayed for protocols:

Num Number that is associated with the protocol.

Name Abbreviated name of the protocol.

Protocol
Full name of the protocol.

The following information is displayed for features:

Num Number associated with the feature.

Name Abbreviated name of the feature.

Feature
Full name of the feature.

The following information is displayed for networks:

Net Network number that the software assigns to the interface. Networks are numbered starting at 0. These numbers correspond to the interface numbers discussed under the CONFIG process.

Interface
Name of the interface and instance of this type of interface.

MAC/Data Link
Type of MAC/Data link configured for the interface.

Hardware
Specific kind of interface by hardware type.

State Current state of the network interface.

Testing
Indicates that the interface is undergoing a self-test. Occurs when the router is first started, when a problem is detected on the interface, or when the **test command** is used.

When an interface is operational, the interface periodically sends out maintenance packets and/or checks the physical state of the port or line to ensure that the interface is still functioning correctly. If the maintenance fails, the interface is declared down and a self-test is scheduled to run in 5 seconds. If a self-test fails, the interface transitions to the down state and the interval until the next self-test is increased up to a maximum of 2 minutes. If the self-test is successful, the network is declared up.

Up Indicates the interface is operational.

Down Indicates that the interface is not operational and has failed a self-test. The network will periodically transition to the testing state to determine if the interface can become operational again.

Disabled
Indicates that the interface is disabled. An interface can be disabled by the following methods:

- An interface can be configured as disabled using the CONFIG **disable** command. Each time the router is reinitialized, the interface's initial state will be disabled. It will remain in the disabled state until an action is taken to enable it.
- An interface can be disabled using the GWCON **disable** command. This method is temporary because the interface will revert to its configured state (enabled or disabled) when the router is reinitialized.

- The network manager can disable the interface through SNMP. This method is temporary because the interface will revert to its configured state (enabled or disabled) when the router is reinitialized.

When an interface is disabled, it remains disabled until one of the following methods is used to enable it:

- The GWCON **test** command is used to start a self-test of the interface.
- The network manager initiates a self-test of the interface through SNMP.

Not Present
Indicates that the interface's adapter is not plugged in.

Not Present is also used as the state for a null device. Spare interfaces are displayed as null devices until they are activated.

HW Mismatch
Indicates that the configured adapter type does not match the adapter type that is actually present in the slot.

Disable

Use the **disable** command to take a network interface off-line, making the interface unavailable. This command immediately disables the interface. You are not prompted to confirm, and no verification message displays. If you disable an interface with this command, it remains disabled until you use the GWCON **test** command or an OPCON **reload** command to enable it.

Enter the interface, or net number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

disable *interface#*

Error

Use the **error** command to display error statistics for the network. This command provides a group of error counters.

Syntax:

error

Example:

```
error
                      Input      Input      Input      Input     Output     Output
Nt  Interface      Discards     Errors  Unk Proto  Flow Drop   Discards     Errors
0   ATM/0                 0          0          0          0          0          0
1   NHRPL/0               0          0          0          0          0          0
2   TKR/0                 0          0          0          0          0          0
3   TKR/1                 0          0          0          0          0          1
4   TKR/2                 0          0          1          0          0          3
5   TKR/3                 0          0          4          0          0          3
6   TKR/4                 0          0          0          0          0          0
7   TKR/5                 0          0          0          0          0          0
8   ATM/1                 0          0          0          0          0          0
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Discards
Number of inbound packets which were discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. The packets may have been discarded to free buffer space.

Input Errors
Number of packets that were found to be defective at the data link.

Input Unk Proto
Number of packets received for an unknown protocol.

Input Flow Drop
Number of packets received that are flow controlled on output.

Output Discards
Number of packets that the router chose to discard rather than transmit due to flow control.

Output Errors
Number of output errors, such as attempts to send over a network that is down or over a network that went down during transmission.

Note: The sum of the discarded output packets is not the same as input flow drops over all networks. Discarded output may indicate locally originated packets.

Event

Use the **event** command to access the Event Logging System (ELS) console environment. This environment is used to set up temporary message filters for troubleshooting purposes. All changes made in the ELS console environment will take effect immediately, but will go away when the router is reinitialized. See "Chapter 12. Using the Event Logging System (ELS)" on page 137 for information about the Event Logging System and its commands. Use the **exit** command to return to the GWCON process.

Syntax:

event

Feature

Use the **feature** command to access console commands for specific IBM MSS Family Client features outside of the protocol and network interface console processes.

Enter a question mark after the **feature** command to obtain a listing of the features available for your software release.

To access that feature's console prompt, enter the **feature** command at the GWCON prompt followed by the feature number or short name. Table 8 on page 95 lists available feature numbers and names.

Once you access the prompt for that feature, you can begin entering specific commands to monitor that feature. To return to the GWCON prompt, enter the **exit** command at the feature's console prompt.

Syntax:

feature *feature#* or *feature-short-name*

Interface

Use the **interface** command to display statistical information about the network interfaces (for example, Ethernet). This command can be used without a qualifier to provide a summary of all the interfaces (shown in the following output) or with a qualifier to reveal detailed information about one specific interface.

Descriptions of detailed output for each type of interface are provided in the specific interface *Monitoring* chapters found in this guide. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

interface [*interface#*]

Example: **`interface`**

```
                                             Self-Test  Self-Test Maintenance
Nt  Nt'  Interface Slot-Port                    Passed     Failed      Failed
0   0    ATM/0     Slot: 1   Port: 1                 1          0           0
1   1    NHRPL/0                                     1          0           0
2   2    TKR/0     Domain: 0                         1          0           0
3   3    TKR/1     Domain: 1                         1          0           0
4   4    TKR/2     Domain: 2                         1          0           0
5   5    TKR/3     Domain: 3                         1          0           0
6   6    TKR/4                                       8        114           0
7   7    TKR/5                                       1          1           0
8   8    ATM/1                                       1          0           0
```

Note: The display varies depending on the device.

Nt Global interface number.

Interface
Interface name.

Slot-Port
Slot number and port number of the interface.

Port Name
Port number, if applicable on the slot.

Self-Test Passed
Number of times self-test succeeded (state of interface changes from down to up).

Self-Test Failed
Number of times self-test failed (state of interface changes from up to down).

Maintenance Failed
Number of maintenance failures.

Memory

Use the **memory** command to display the current CPU memory usage in bytes, the number of buffers, and the packet sizes.

To use this command, free memory must be available. The number of free packet buffers may drop to zero, resulting in the loss of some incoming packets; however, this does not adversely affect router operations. The number of free buffers should remain constant when the router is idle. If it does not, contact your service representative.

Syntax:

memory

Example:

```
memory
Physical installed memory:        16 MB
Total routing (heap) memory:      12 MB
Routing memory in use:            13 %

                  Total  Reserve    Never     Perm     Temp     Prev
                                    Alloc    Alloc    Alloc    Alloc
Heap memory    12231155    26488 10687312  1438487   104924      432

Number of global buffers: Total = 300, Free = 300, Fair = 77, Low = 60
Global buff size: Data = 2048, Hdr = 17, Wrap = 72, Trail = 65, Total = 2208
```

Physical installed memory
The total amount of physical RAM installed in the router.

Total routing memory
The amount of memory available to the routing function, not including that allocated to the base operating system, system extensions, or options such as APPN. This is also called ″heap″ memory, and matches the ″Total″ heap memory size given in bytes shortly thereafter.

Routing memory in use
The percentage of total routing memory that is currently being used by the routing function. Heap memory currently in use is counted under the following headings **Perm Alloc** and **Temp Alloc**.

Heap memory:
Amount of memory used to dynamically allocate data structures.

Total Total amount of space available for allocation for memory.

Reserve
Minimum amount of memory needed by the currently configured protocols and features.

Never Alloc
Memory that has never been allocated.

Perm Alloc
Memory requested permanently by router tasks.

Temp Alloc
Memory allocated temporarily to router tasks.

Prev Alloc
Memory allocated temporarily and returned.
Number of global buffers:

Total Total number of global buffers in the system.

Free Number of global buffers available.

Fair Fair number of buffers for each interface. (See “Low”.)

Low The number of free buffers at which the allocation strategy changes to conserve buffers. If the value of *Free* is less than *Low*, then buffers will not be placed on any queue that has more than the *Fair* number of buffers in it.

Global buff size:
Global buffer size.

Data Maximum data link packet size of any interface.

Header
Sum of the maximum hardware, MAC, and data link headers.

Wrap Allowance given for MAC, LLC, or Network layer headers due to protocol wrapping.

Trailer Sum of the largest MAC and hardware trailers.

Total Overall size of each packet buffer

Network

Use the **network** command to enter the console environment for supported networks. This command obtains the console prompt for the specified interface.

Syntax:

network *interface#*

At the GWCON prompt (+), enter the **configuration** command to see the protocols and networks for which the router is configured. See "Configuration" on page 120 for more information on the configuration command.

Enter **interface** at the + prompt for a display of the networks for which the router is configured.

Enter the GWCON **network** command and the number of the interface you want to monitor or change. For example:

```
+network 0
ATM+
```

In the example, the ATM+ prompt is displayed. You can then view information about the ATM interface by entering the ATM operating commands.

After identifying the interface number of the interface you want to monitor, for interface-specific information, see the corresponding monitoring chapter in this manual for the specified network or link-layer interface. Console support is offered for the following network and link-layer interfaces:

- ATM
- Token-Ring LECs
- Ethernet LECs

Performance

Use the **performance** command at the GWCON prompt to enter the monitoring environment for performance. See "Chapter 14. Configuring and Monitoring Performance" on page 201 for more information.

Protocol

Use the **protocol** command to communicate with the router software that implements the network protocols installed in your router. The **protocol** command accesses a protocol's command environment. After you enter this command, the prompt of the specified protocol appears. From the prompt, you can enter commands that are specific to that protocol.

Syntax:

protocol *prot#*

Enter the protocol number or short name as part of the command. To obtain the protocol number or short name, enter the CONFIG command environment (`Config>`), and then enter the **list configuration** command. See "Accessing the Configuration Process, CONFIG (Talk 6)" on page 26 for instructions on accessing `Config>`. To return to GWCON, enter **exit**.

See the corresponding monitoring chapter in this manual or in the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for information on a specific protocol's console commands.

Queue

Use the **queue** command to display statistics about the length of input and output queues on the specified interfaces. Information about input and output queues provided by the queue command includes:

- The total number of buffers allocated
- The low-level buffer value
- The number of buffers currently active on the interface.

Syntax:

queue *interface#*

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

```
MSS Client +queue
                Input Queue       Output Queue
Nt  Interface   Alloc Low Curr    Fair Curr
0   ATM/0          80  20   80      20    0
1   NHRPL/0         0   0    0      20    0
2   TKR/0           0   0    0      20    0
3   TKR/1           0   0    0      20    0
4   TKR/2           0   0    0      20    0
5   TKR/3           0   0    0      20    0
6   TKR/4           0   0    0      20    0
7   TKR/5           0   0    0      20    0
8   ATM/1           0   0    0      20    0

MSS Client +queue 2
                Input Queue       Output Queue
Nt  Interface   Alloc Low Curr    Fair Curr
2   TKR/0           0   0    0      20    0
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Queue:

Alloc Number of buffers allocated to this device.

Low Low water mark for flow control on this device.

Curr Current number of buffers on this device. The value will be 0 if the device is disabled.

Output Queue:

Fair Fair level for the length of the output queue on this device.

Curr Number of packets currently waiting to be transmitted on this device. For locally originated packets, the eligibility discard depends on the global low water mark described in the **memory** command.

The router attempts to keep at least the Low value packets available for receiving over an interface. If a packet is received and the value of Curr is less than Low, then the packet will be subject to flow control. If a buffer subject to flow control is to be queued on this device and the Curr level is greater than Fair, then the buffer is dropped instead of queued. The dropped buffer is displayed in the Output Discards column of the **error** command. It will also generate ELS event GW.036 or GW.057.

Due to the scheduling algorithms of the router, the dynamic numbers of Curr (particularly the Input Queue Curr) may not be fully representative of typical values during packet forwarding. The console code runs only when the input queues have been drained. Thus, Input Queue Curr will generally be nonzero only when those packets are waiting on slow transmit queues.

Reset

Use the **reset** command to disable the specified interface and then re-enable it using new interface, protocol and feature configuration parameters. See “Resetting Interfaces” on page 85 for more information.

Syntax:

reset *interface#*

Statistics

Use the **statistics** command to display statistical information about the network software, such as the configuration of the networks in the router.

Syntax:

statistics *interface#*

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Example:

```
statistics
Nt Interface     Unicast  Multicast      Bytes    Packets      Bytes
                Pkts Rcv   Pkts Rcv   Received      Trans      Trans
0   ATM/0       59445857          0 3035044754   28220894 1286421650
1   NHRPL/0            0          0          0          0          0
2   TKR/0          10846      21762    2963771      10847     227787
3   TKR/1          40795   27903331 1492268217      37089    2636231
4   TKR/2          22941   27892772 1547248412   27959282 1326317190
5   TKR/3          22740   27960571 1551981625   27976109 1328606969
```

```
6   TKR/4         64062   31201551 1753679907      33559    3206729
7   TKR/5         59364   27947601 1276965544   27959091 1271582564
8   ATM/1             0          0          0          0          0
```

Nt Network interface number associated with the software.

Interface
Type of interface.

Unicast Pkts Rcv
Number of non-multicast, non-broadcast specifically-addressed packets at the MAC layer.

Multicast Pkts Rcv
Number of multicast or broadcast packets received.

Bytes Received
Number of bytes received at this interface at the MAC layer.

Packets Trans
Number of packets of unicast, multicast, or broadcast type transmitted.

Bytes Trans
Number of bytes transmitted at the MAC layer.

Switch-Interface

Use the **switch-interface** command to access the console environment of the LAN Switch Interface. This environment allows you to display the hardware bridging statistics.

Syntax:

switch-interface

See “Switch-Interface Commands” on page 130 for details about the switch-interface commands.

Test

Use the **test** command to verify the state of an interface or to enable an interface that was previously disabled with the **disable** command. If the interface is enabled and passing traffic, the **test** command will remove the interface from the network and run self-diagnostic tests on the interface.

Syntax:

test *interface#*

Note: For this command to work, you must enter the ***complete*** name of the command followed by the interface number.

Enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command. For example, when testing starts, the console displays the following message:

```
Testing net 0 ATM/0...
```

When testing completes or fails, or when GWCON times out (after 30 seconds), the following possible messages are displayed:

```
Testing net 0 ATM/0 ...successful
   Testing net 0 ATM/0 ...failed
  Testing net 0 ATM/0 ...still testing
   Network is already undergoing test, attempting restart
```

Some interfaces may take more than 30 seconds before testing is done.

Uptime

Use the **uptime** command to display time statistics about the router, including the following:

- Number of restarts.
- Number of known crashes.
- Whether the router was last reloaded or restarted.
- Time elapsed since the last reload.
- Time elapsed since the last restart.

Syntax:

uptime

Switch-Interface Commands

The switch-interface operating environment allows you to display hardware bridging statistics. You access this environment by entering the **switch-interface** command at the GWCON (+) prompt. Table 13 lists the commands available at the `SI>` prompt.

Table 13. Switch-Interface Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Cell	Enables and disables the cell counting function on the interface.
Clear	Clears the frame counters and cell counts for the interface.
Disable	Disables hardware bridging globally or for specific interfaces on the switch interface. Use this command only under the guidance of a service representative.
Enable	Enables hardware bridging globally or for specific networks on the switch interface.
Statistics	Displays the hardware bridging statistics for all of the networks on the switch interface or for a specific network on the switch interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Cell

Use the **cell** command to enable or disable the cell counting function on the interface.

Syntax:

cell off

on

off Disables the cell counting function on the interface. This is the default. When cell counting is off, the cells received and transmitted displayed by the **statistics** command will display as “n/a.”

on Enables the cell counting function on the interface.

Example:

```
SI>cell on
Warning:  Enabling Cell Counts will result in reduced performance.
Are you sure you want to do this? (Yes or [No]): y
Cell counts have been ENABLED.
```

Clear

Use the **clear** command to clear the frame counters and the cell counts, if cell counts are enabled, for the interface.

Syntax:

clear

Disable

Attention: Use this command only under the guidance of a service representative.

Use the **disable** command to disable hardware bridging either globally or for a particular network on the interface.

Syntax:

disable (no parameters)

net#

(no parameters)
Disables hardware bridging globally. The **statistics** command displays that each individual network has the hardware bridge enabled, but hardware bridging does not take place.

net# Disables hardware bridging for the network identified by *net#.* Other networks on the router will continue to use hardware bridging unless bridging is disabled globally.

Example:

```
SI>di 1
Warning:  Disabling Hardware Bridging will result in reduced
performance of the bridge path across this network.
Are you sure you want to do this? (Yes or [No]): y
Hardware Bridging has been DISABLED on the specified network.
```

See “Statistics” on page 132 for a description of the statistics display.

Enable

Use the **enable** command to enable hardware bridging either globally or for a particular network on the interface.

Syntax:

enable (no parameters)

net#

(no parameters)
Enables hardware bridging globally. Hardware bridging takes place over all networks that have been enabled.

net# Enables hardware bridging for the network identified by *net#.* However, if hardware bridging is globally disabled, no hardware bridging takes place.

Example:

```
SI>en 1
Hardware Bridging has been ENABLED on the specified network.
Note:  Hardware Bridging is globally DISABLED.
```

See “Statistics” for a description of the statistics display.

Statistics

Use the **statistics** command to display the hardware bridging statistics for all networks on the interface or a specific network on the interface.

Syntax:

statistics (no parameter)
net#

(no parameters)
Displays the bridging statistics for all of the networks on the interface.

net# Displays the bridging statistics for a specific network on the interface. If you specify a network that cannot use hardware bridging, you will receive the message `Hardware Bridging statistics are not available on this network.` If you specify a network that does not exist, you will receive the message `Bad network number.`

Example:

```
SI>s 1

The Hardware Bridging function is globally ENABLED.

Nt Interface  Dom  TxID    Packets    Packets      Cells      Cells  Hardware
                          Received      Trans   Received      Trans    Bridge
1   TKR/0     15   4094          8          8         16         16   enabled
1   TKR/0     15   4095          0          0          0          0   enabled
                        ------------------------------------------
    TOTALS                       8          8         16         16
```

The parameters are:

Nt The network identifier.

Interface
The type and number of the interface.

Dom The LAN Switch domain to which the interface belongs.

Txid The hardware bridging path identifier.

Packets Received
The number of packets received on this network.

Packets Trans
The number of packets transmitted on this network.

Cells Received
The number of cells received on this network.

Cells Trans
The number of cells transmitted on this network.

Hardware Bridge
Whether hardware bridging in enabled on this interface.

Chapter 11. The Messaging (MONITR - Talk 2) Process

This chapter explains how to collect and display messages. (Refer to “Chapter 12. Using the Event Logging System (ELS)” on page 137 for information about ELS and message formats. Refer also to the *IBM Multiprotocol Switched Services Client Event Logging System Messages Guide* for a description of each message. This chapter includes the following sections:

- “What is Messaging (MONITR)?”
- “Commands Affecting Messaging”
- “Entering and Exiting the Messaging (MONITR) Process”
- “Receiving Messages”

What is Messaging (MONITR)?

The MONITR process provides a view of activity inside the router and the networks. MONITR also displays logging messages from the software.

Commands Affecting Messaging

The following commands affect the messaging process:

- OPCON commands:
  - **divert** temporarily diverts output to a different device.
  - **flush** causes the software to discard the messages it collects.
  - **halt** reverses the action of the divert command.
  - **talk** displays message output.
- CONFIG **set logging disposition** command sets the initial device to which the software sends its output.

Entering and Exiting the Messaging (MONITR) Process

To enter the messaging process from OPCON enter the **event** command or the **talk 2** command.

The console displays the messages the software has accumulated.

To exit messaging and return to OPCON, enter the OPCON intercept character (the default is **Ctrl-P**).

Receiving Messages

To receive messages at your console, enter the messaging process as described in the previous section. The software then displays all the messages it has recorded since it was last invoked. While you are connected to the messaging process, it displays all messages as they arrive.

Use the OPCON **divert** and **halt** commands to view software messages while you are doing something else with the router. Permitted devices divert output to TTY0 (the local console), TTY1, or TTY2 (the remote consoles).

Chapter 12. Using the Event Logging System (ELS)

This chapter describes the Event Logging System (ELS). The ELS continually logs all events, filtering them according to parameters that you select. A combination of operational counters and the ELS provides information for monitoring the health and activity of the system. The information is divided into the following sections:

What is ELS?

ELS is a monitoring system and an integral part of the router operating system. ELS manages the messages logged as a result of router activity. Use ELS commands to set up a configuration that sorts out only those messages you feel are important. You can then display the messages on the console terminal screen, log them to a remote workstation, or send the messages to a network management station using Simple Network Management Protocol (SNMP) traps.

The ELS system and the operational counters are the best troubleshooting tools you have to isolate problems in the router. A quick scan of the event messages will tell you whether the router has a problem and where to start looking for it.

In the ELS configuration environment, the commands are used to establish a default configuration. This default configuration does not take effect until the router reinitializes.

Occasionally, it is helpful to temporarily view messages using parameters other than was set up in the ELS configuration environment, without having to reinitialize the router. The ELS operating and monitoring environment is used to:

- Temporarily change the default ELS display settings
  - Changes made in the ELS console environment take effect immediately
  - Changes made in the operating/monitoring environment are not stored in nonvolatile configuration storage.
- View statistical information regarding ELS uses of dynamic RAM

Note: Specific ELS messages are described in the *IBM Multiprotocol Switched Services Client Event Logging System Messages Guide*.

ELS is a subprocess that you access from the OPCON process.

Entering and Exiting the ELS Configuration Environment

The ELS configuration environment (available from the CONFIG process) is characterized by the `ELS Config>` prompt. Commands entered at this prompt create the ELS default state that takes effect after you restart the router. These commands are described in greater detail later in this chapter.

Configuration commands that have subsystem, group, or event as a parameter are executed in the following order:

- Subsystem
- Group
- Event

To set a basic ELS configuration, enter the **display subsystem all standard** command at the `ELS Config>` prompt. This command configures the ELS to display messages from all subsystems with the STANDARD logging level (that is, all errors and unusual informational comments).

Note: The router does not have a default ELS configuration. You must enter the ELS configuration environment and set the default state.

To enter the ELS configuration environment from OPCON:

1. Enter the **configuration** command. The console displays the CONFIG prompt (`Config>`). If the prompt does not appear when you first enter CONFIG, press **enter**.
2. At the CONFIG prompt, enter the following command to access ELS:

   ```
   Config> eve
   ```

   The console displays the ELS configuration prompt (`ELS config>`). Now, you can enter ELS configuration commands.

To leave the ELS configuration environment, enter the **exit** command.

Event Logging Concepts

This section describes how events are logged and how to interpret messages. Also described are the concepts of subsystem, event number, and logging level. A large part of ELS function is based on commands that accept the subsystem, event number, and logging level as parameters.

Causes of Events

Events occur continuously while the router is operating. They can be caused by any of the following reasons:

- System activity
- Status changes
- Service requests
- Data transmission and reception
- Data and internal errors

When an event occurs, ELS receives data from the system that identifies the source and nature of the event. Then ELS generates a message that uses the data received as part of the message.

Interpreting a Message

This section describes how to interpret a message generated by ELS. Figure 24 shows the message contents.

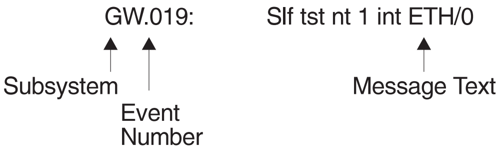


Figure 24. Message Generated by an Event

The information illustrated in Figure 24 as well as the ELS logging level information displayed with the **list subsystem** command is as follows:

Subsystem

Subsystem is a predefined short name for a router component, such as a protocol or interface. In Figure 24, **GW** identifies the subsystem through which this event occurred.

Other examples of subsystems include IP, TKR, and ATM. On a particular router, the actual subsystems present depend on the hardware and software configured for that router. You can use the **list subsystem** command described in this chapter to see a list of the subsystems on your router.

Enter the subsystem as a parameter to an ELS command when you want the command to affect the entire subsystem. For example, the ELS command **display subsystem GW** causes all events (except the events with 'debug' logging level) that occur through the GW subsystem to be displayed.

Event Number

Event Number is a predefined, unique, arbitrary number assigned to each message within a subsystem. In Figure 24, **019** is the event number within the GW subsystem. You can see a list of all the events within a subsystem by using the **list subsystem** command, where *subsystem* is the short name for the subsystem.

The event number always appears with a subsystem identifier, separated by a period. For example: **GW.019**. The subsystem and event number together identify an *individual* event. They are entered as a parameter to certain ELS commands. When you want a command to affect only the specified event, enter the subsystem and event number as a parameter for the ELS command.

Logging Level

Logging level is a predefined setting that classifies each message by the type of event that generated it. Use the **list subsystem** ELS console command to display the setting of the logging level. Table 14 on page 140 lists the logging levels and types. ERROR, INFO, TRACE, STANDARD, and ALL are aggregates of other logging level types. STANDARD is the recommended default.

Table 14. Logging Levels

Logging Level	Type
UI ERROR	Unusual internal errors
CI ERROR	Common internal errors
UE ERROR	Unusual external errors
CE ERROR	Common external errors
ERROR	Includes all error levels above
UINFO	Unusual informational comment
CINFO	Common informational comment
INFO	Includes all comment levels above
STANDARD	Includes all error levels and all informational comment levels (default)
PTRACE	Per packet trace
UTRACE	Unusual operation Trace message
CTRACE	Common operation Trace message
TRACE	Includes all trace levels above
DEBUG	Message for debugging
ALL	Includes all logging levels

The logging level setting affects the operation of the following commands:

- **Display subsystem**
- **Nodisplay subsystem**
- **Trap subsystem**
- **Notrap subsystem**
- **Remote subsystem**
- **Noremote subsystem**

The logging level is set for a particular command when you specify it as a parameter to one of the above commands. For example:

```
display subsystem IP ERROR
```

Including the logging level on the command line modifies the **display** command so that whenever an event with a logging level of either UI-ERROR or CI-ERROR occurs through subsystem TKR, the console displays the resulting message.

You cannot specify the logging level for operations affecting groups or events.

Message Text

Message Text appears in short form. In Figure 24 on page 139, `Slf tst nt 1 int ETH/0` is the message generated by this event. Variables, such as *source_address* or *network*, are replaced with actual data when the message displays on the console.

The variable *error_code* is referred to by some of the Event Logging System message descriptions (usually preceded by rsn or reason). They indicate the type of packet error detected. Table 15 on page 141 describes the error or packet completion codes. Packet completion codes indicate the disposition of the packets received by the router.

Table 15. Packet Completion Codes (Error Codes)

Code	Meaning
0	Packet successfully queued for output
1	Random, unidentified error
2	Packet not queued for output due to flow control reasons
3	Packet not queued because network is down
4	Packet not queued to avoid looping or bad broadcast
5	Packet not queued because destination host is down (only on networks where this can be detected)

ELS displays network information as follows:

`nt 1 int Eth/0` (or) `network 1, interface Eth/0,`

where:

- 1 is the network number (each network on the router is numbered sequentially from zero).
- 0 is the unit number (the interfaces of each hardware type are numbered sequentially from zero).

Ethernet and 802.5 hardware addresses appear as a long hexadecimal number.

IP (Internet Protocol) addresses are printed as 4 decimal bytes separated by periods, such as 18.123.0.16.

Groups

Groups are user-defined collections of events that are given a name, the group name. Like the subsystem, subsystem and event number, and logging level, use the group name as a parameter to ELS commands. However, there are no predefined group names. You must create a group before you can specify its name on the command line.

To create a group, use the **add** configuration command, specify the name you want to call the group, and then specify the events you want to be part of the group. The events you add to the group can be from different subsystems and have different logging levels.

After creating a group, use the group name to manipulate the events in the group as a whole. For example, to turn off display of all messages from events that have been added to a group named grouptwo, include the group name on the command line, as follows:

```
nodisplay group grouptwo
```

To delete a group, use the **delete** command.

Using ELS

To use ELS effectively, do the following:

- Know what you want before using the ELS system. Clearly define the problem or events that you want to see before using the MONITR process.
- Execute the command **nodisplay subsystem all all** to turn off all ELS messages.

- Turn on only those messages that relate to the problem you are experiencing.
- Use the *IBM Multiprotocol Switched Services Client Event Logging System Messages Guide* to determine which messages are not normal.

When initially viewing ELS from the MONITR process, you will see a considerable amount of information. Because the router cannot buffer and display every packet under moderate to heavy loads the buffers are flushed. When this occurs the following message is displayed:

```
xx messages flushed
```

The router does not save these messages. When this message appears, tailor the ELS output to display only that information that is important to the current task you are monitoring, or use the advanced ELS commands to establish a message buffer. See “Using ELS Message Buffering” on page 153.

Managing ELS Message Rotation

It is also important to note that the ELS messages continually rotate through the router’s buffers. To stop and restart the displaying of ELS messages, use the following key combinations:

Ctrl-S to pause scrolling

Ctrl-Q to resume scrolling

Ctrl-P to go back to the last process

You may also want to capture the ELS output to a file. You can do this by starting a script file or log file from your location when Telneting to a router. You can also do this by attaching a PC to the router’s console port and starting a log file from within the terminal emulation package. This information is needed to help Customer Service diagnose a problem.

Capturing ELS Output Using a Telnet Connection on a UNIX Host

Use a Telnet connection on an AIX or UNIX host to capture the ELS messages on your screen to a file on the host. Before beginning, set up ELS for the messages you want to capture using the ELS console commands in “Chapter 13. Configuring and Monitoring the Event Logging System (ELS)” on page 157.

To capture the ELS output to a file on an AIX or UNIX host, follow these steps:

1. From the host, enter **telnet** *router_ip_addr* **| tee** *local_file_name*

   router_ip_addr is the IP address of the router

   local_file_name is the name of the file on the host where you want the ELS messages to be saved.

   The **tee** command displays the ELS messages on your screen and, at the same time, copies them to the local file.
2. From the OPCON prompt (*****), enter **t 2**. This accesses the MONITR process, which is the process that displays ELS messages on your screen. Depending on which ELS messages you configured, you should see ELS messages appearing on the screen.

   As long as you are in the MONITR process, all ELS messages will be written to the local file. When you exit the MONITR process (by entering **Ctrl-P**) or terminate the Telnet session, the logging of messages to the local file will stop.

You can also use remote logging instead of capturing ELS output on a UNIX Host. For more information about remote logging, see “Using and Configuring ELS Remote Logging” on page 145.

Configuring ELS So Event Messages Are Sent In SNMP Traps

ELS can be configured so that event messages are sent to a network management workstation in an SNMP enterprise-specific trap. These traps are useful for reporting status and diagnostic results, and are often used for remote monitoring of a IBM MSS Family Client. When ELS is configured appropriately, an SNMP trap will be generated each time the selected event occurs. For more information about SNMP, see *Multiprotocol Switched Services (MSS) Configuring Protocols and Features*.

To tell ELS that a specific event should be activated to be sent as an SNMP trap, at the `ELS config>` prompt or at the `ELS>` prompt, using IP as an example, type:

```
trap event ip.007
```

Note: If you are at the `ELS config>` prompt, you will need to reboot.

To enable the ELS enterprise-specific trap, follow these steps:

1. At the `SNMP config>` prompt, using **public** as an example, type:

   ```
   SNMP config> add address public <network manager IP address>
   SNMP config> enable trap enterprise public
   SNMP config> set community access read_trap public
   ```

   Note: You need to reboot to activate these changes.
2. Enable your network management station to receive and properly display the enterprise-specific traps.

Follow these steps to trap groups, subsystems, and events.

Using ELS to Troubleshoot a Problem

If you are trying to troubleshoot a particular problem, display the messages related to the problem. For example, if experiencing a problem with bridging, turn on the bridging messages:

display subsystem srt all

display subsystem br all

Initially, because of the rapid pace of messages scrolling across the screen, you may want to record the numbers you see and look them up in the *Event Logging System Messages Guide* manual. Once you become familiar with different types of messages being displayed for a particular protocol, you can turn on and turn off only those messages that contain the information that you require to troubleshoot a problem. The following sections list specific ELS examples. Keep in mind that different problems may require different steps.

ELS Example 1

You are interested in looking at the frequency of polling on a Token-Ring interface, and finding out whether the polls are successful.

```
ELS> nodisplay subsystem all all
ELS> display subsystem tkr all
Ctrl-P
* t 2
```

As the messages begin to scroll by, look for ELS message tkr.031.

ELS Example 2

SRB bridging is not working.

1. Check the configuration.
2. Use the GWCON bridging console to verify that the bridging interfaces are enabled.
3. Enter:

   ```
   * t 6
   config> event
   ELS config> nodisplay subsystem all all
   ELS config> display subsystem srb all
   ELS config> exit
   config> Ctrl-P
   ```

4. Restart the routing subsystem. When the subsystem has restarted, enter the following:

   ```
   * t 2
   ```

ELS Example 3

Router cannot communicate with an IPX server on an Ethernet.

1. Enter the **talk** command and the PID for GWCON.

   ```
   * talk 5
   ```

   The console displays the GWCON prompt (+). If the prompt does not appear when you first enter GWCON, press **Return**.

2. At the GWCON prompt (+), enter **IPX** to access the IPX console prompt (`IPX>`).
3. At the IPX console prompt, enter the **slist** command to verify that the server is listed. (See the section on monitoring IPX in the *Multiprotocol Switched Services (MSS) Configuring Protocols and Features* for information on the **slist** command.)
4. Check the IPX configuration.
5. Enter the following:

   ```
   * t 5
   + event
   ELS> nodisplay subsystem all all
   ELS> display subsystem IPX all
   ELS> display subsystem eth all
   ELS> Ctrl-P
   * t 2
   ```

As the messages begin to scroll by, look for ELS message eth.001. This indicates that the server has a bad Ethernet type field.

Using and Configuring ELS Remote Logging

The remotely-logged ELS message contains all of the information that is contained in ELS messages found in the monitor queue, as viewed under `talk 2`, and also contains additional information as shown in Figure 25.

```
Date/Time         IP address      Sequence Number      Local Name      ELS Subsystem Name, &
                  assigned        used for detecting   assigned        Formatted message
                  by the user     missing messages     by the user

Nov 20 12:13:47   5.1.1.1         Msg [0444] from      ** IBM/MSS Family Client **  :els: MPC.011 Del ent ...
```

Figure 25. Syslog Message Description

Note the following differences in the remote log display:

- The month and day of month in addition to the time, which is always displayed as the time-of-day.
- An IP address, which is the user-specified source IP address. If a DNS server resolves the source IP address to a hostname, then the hostname will be displayed instead of the IP address.
- A Sequence number is added to the message by the source device to assist in detecting dropped messages. See “Remote Logging Output” on page 149 for an explanation of dropped messages. When the sequence number of the message reaches 9999, the next sequence number is 0001.
- A “Local Name” for the source router, to assist in distinguishing between messages from multiple sources. If you do not configure a local name, this field is blank.

Syslog Facility and Level

Remotely-logged ELS messages are transmitted over the network in UDP packets with the destination port number in the UDP header always equal to 514, the syslog port. To receive and process the UDP packets, the *syslog daemon* (syslogd) must be running in the remote workstation that is receiving and logging the ELS messages. See “Remote Workstation Configuration” for details.

Although it is not displayed in the remotely-logged ELS message, every ELS message sent on the network in a UDP packet must be assigned a *syslog_facility* and a *syslog_level*. The syslog daemon uses the combination of facility and level to determine where to route the message. Typically, you want the ELS messages to be written to one or more files in the remote host. Other options include displaying the message on the console, sending the message to one or more users, or sending the message to another workstation.

The commands you use to specify the *syslog_facility* and *syslog_level* values, along with other remote-logging related console commands, are described in “ELS Monitoring Commands” on page 175 and “ELS Configuration Commands” on page 157. Review these commands before reading through the next section.

Remote Workstation Configuration

The following configuration assumes that a single MSS Family Client is remote-logging to a single remote workstation. You can configure multiple MSS

Family Clients to remote-log to the same remote workstation. However, a particular MSS Family Client can log to one and only one remote workstation. The operating system used in this example is AIX 4.2. Your environment may be slightly different. For more information on syslog, refer to the documentation for your operating system.

To perform the configuration on an AIX workstation, you must log in as **root**. To configure the workstation:

1. Create or edit a syslog.conf file to specify where ELS messages with particular *syslog_facility* and *syslog_level* values are to be written. See the bottom of Figure 26 on page 147 for an example of how to specify the message destination. Note that the full pathname of the log files must be specified. The default location for the syslog configuration file is /etc/syslog.conf.
2. Create the files for logging syslog messages that you specified in the syslog.conf file.
3. Start the syslog daemon by entering **syslogd**. To start the syslog daemon from SRC (System Resource Controller), enter **startsrc -s syslogd**. If the pathname of the configuration file is not /etc/syslog.conf, then enter **syslogd -f** *pathname*. To start the syslog daemon in debug mode, enter **syslogd -d**.

   Note: Running multiple instances of the syslog daemon is not supported.
4. If the syslog daemon is already running when you create or modify the syslog.conf file, it must be restarted so that the daemon reinitializes the configuration from syslog.conf.
5. Verify the setup by using the **logger** command as follows:

   ```
   logger -p user.alert  THIS IS A TEST MESSAGE (user.alert)
   logger -p news.info  THIS IS A TEST MESSAGE (news.info)
   ```

   If the setup is correct, `THIS IS A TEST MESSAGE...` will be written to the files specified in syslog.conf.

```
# @(#)34       1.9 src/bos/etc/syslog/syslog.conf, cmdnet, bos411, 9428A410j 6/13/93 14:52:39
#
# COMPONENT_NAME: (CMDNET) Network commands.
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1988, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# /etc/syslog.conf - control output of syslogd
#
# Each line must consist of two parts:-
#
# 1) A selector to determine the message priorities to which the
#    line applies
# 2) An action.
#
# The two fields must be separated by one or more tabs or spaces.
#
# format:
#
# <msg_src_list>               <destination>
#
# where <msg_src_list> is a semicolon separated list of <facility>.<priority>
# where:
#
# <facility> is:
#      * - all (except mark)
#      kern,user,mail,daemon, auth, syslog, lpr, news, uucp, cron, authpriv, local0 - local7
#
# <priority or level> is one of (from high to low):
#      emerg,alert,crit,err(or),warn(ing),notice,info,debug
#      (meaning all messages of this priority or higher)
#
# <destination> is:
#      /filename - log to this file
#      username[,username2...] - write to user(s)
#      @hostname - send to syslogd on this machine
#      * - send to all logged in users
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
#  mail.debug          /usr/spool/mqueue/syslog
#  *.debug             /dev/console
#  *.crit                      *

#   syslog messages with facilty / priority values of LOG_USER,   LOG_ALERT
user.alert            /tmp/syslog_user_alert

#   syslog messages with facilty / priority values of LOG_NEWS,  LOG_INFO
news.info           /tmp/syslog_news_info
```

Figure 26. syslog.conf Configuration File

Configuring the MSS Family Client for Remote Logging

To configure a MSS Family Client:

1. In talk 6, configure the remote-logging facility as shown in Figure 27 on page 148. The IP address specified as the *source-ip-addr* should be an IP address that is configured in the MSS Family Client for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address resolves quickly into a hostname by the name server or that the name server at least responds quickly

with “address not found.” To determine whether this happens, issue the **host** command on your workstation as follows:

```
workstation> host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address which resolves more quickly.

2. In talk 6 configure events and subsystems for remote-logging, as shown in Figure 28 on page 149.
3. Write the configuration and reload the MSS Family Client.

```
ELS config>set remote source-ip-addr 5.1.1.1
Source IP Addr = 5.1.1.1

ELS config>set remote remote-ip-addr 192.9.200.1
Remote Log IP Addr = 192.9.200.1

ELS config>set remote local-id ** IBM/MSS Family Client **
Remote Log Local ID = ** IBM/MSS Family Client **

ELS config>set remote no-msgs-in-buffer 100
Number of messages in Remote Log Buffer must be 100-512
Number of Messages in Remote Buffer = 100

ELS config><B>set remote facility log_news
Default Syslog Facility = LOG_NEWS

ELS config>set remote level log_info
Default Syslog Level = LOG_INFO

ELS config>set remote on
Remote Logging is ON

ELS config>list remote

------------------   Remote Log Status  -----------------

Remote Logging is ON
Source IP Address = 5.1.1.1
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_NEWS
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log =  100
Remote Logging Local ID = ** IBM / MSS Family Client **
ELS config>
```

Figure 27. Configuring the MSS Family Client for Remote Logging

```
ELS config>display sub snmp all
ELS config>remote sub snmp all log_news log_info

ELS config>display event srt.017
ELS config>remote event srt.017 log_news log_info

ELS config>display event stp.016
ELS config>remote event stp.016 log_user log_info

ELS config>display event stp.026
ELS config>remote event stp.026 log_news log_info

ELS config>display event stp.024
ELS config>remote event stp.024 log_news log_info

ELS config>display event ip.068
ELS config>remote event ip.068 log_news log_info

ELS config>display event ip.058
ELS config>remote event ip.058 log_news log_info

ELS config>display event ip.022
ELS config>remote event ip.022 log_news log_info

ELS config>display event gw.022
ELS config>remote event gw.22 log_news log_info

ELS config>display event arp.011
ELS config>remote event arp.011 log_user log_alert

ELS config>display event arp.002
ELS config>remote event arp.022 log_user log_alert

ELS config>list status
Subsystem:    SNMP
Disp levels:  ERROR INFO TRACE
Trap levels:  none
Trace levels: none
Remote levels:  ERROR INFO TRACE
        Syslog Facility/Level: LOG_NEWS LOG_INFO

Event     Display Trap    Trace     Remote
SRT.017   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.016   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.026   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.024   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.068    On      Unset   Unset
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.058    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.022    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
GW.022    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
ARP.011   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_USER LOG_ALERT
ARP.002   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_USER LOG_ALERT
```

Figure 28. Configuring Subsystems and Events for Remote Logging

Remote Logging Output

Figure 29 on page 150 shows a sample from the /tmp/syslog_news_info file. Notice that the first message has a sequence number of 310. This means that the first 309 ELS messages were not sent from the source MSS Family Client. There are several reasons for this:

- The remote-logging facility had not completed initialization when the messages were first passed to ELS

- A route from the source MSS Family Client to the remote workstation was not in the routing table
- The interface for the outbound UDP packet containing the ELS messages was not in the “Up” state

Notice in 1 that messages 311-313 did not get remote-logged. This is because an ARP request was outstanding and until the ARP response is received, all but the first packet is dropped in the source MSS Family Client. Additionally, the ARP cache is cleared at a user-configured refresh rate, and a new ARP request is issued. To determine when this is occurring, you can remote log events ARP.002 and ARP.011 in addition to the primary ELS events of interest. Figure 31 on page 151 shows ARP events logged to the *syslog_user_alert* file that account for events 445 and 446, which were indicated as missing in Figure 29.

```
Nov 20 12:03:16 worksta01 root:  THIS IS A TEST MESSAGE  (news.info)
Nov 20 12:08:48 5.1.1.1 Msg [0310] from ** IBM / MSS Family Client **: els:  IP.022: add nt 192.9.200.0 int 192.9.200.20
nt 0 int Eth/0

 1  ( messages 311, 312, and 313 did not get remote-logged due to ARP request outstanding - see
  explanation in the text)

 2  (messages 314 and 315 were logged to a separate
file - see explanation in the text)

Nov 20 12:08:48 5.1.1.1 Msg [0316] from ** IBM / MSS Family Client **: els:  IP.068: routing cache cleared
Nov 20 12:08:48 5.1.1.1 Msg [0317] from ** IBM / MSS Family Client **: els:  IP.022: add nt 5.0.0.0 int 5.1.1.1 nt 5 int Eth/4
Nov 20 12:08:48 5.1.1.1 Msg [0318] from ** IBM / MSS Family Client **: els: SRT.017: Enabling SRT on port 5 nt 5 int Eth/4


(message 319 was logged to a separate file)

Nov 20 12:08:48 5.1.1.1 Msg [0320] from ** IBM / MSS Family Client **: els:  IP.068: routing cache cleared

(120 messages not shown)

Nov 20 12:13:33 5.1.1.1 Msg [0441] from ** IBM / MSS Family Client **: els:  GW.022: Nt fld slf tst nt 3 int Eth/3
Nov 20 12:13:33 5.1.1.1 Msg [0442] from ** IBM / MSS Family Client **: els:  GW.022: Nt fld slf tst nt 6 int Eth/5
Nov 20 12:13:38 5.1.1.1 Msg [0443] from ** IBM / MSS Family Client **: els:  GW.022: Nt fld slf tst nt 11 int ISDN/0


(messages 444 and 447 were logged to a separate file)


(messages 445 and 446 did not get remote-logged due to ARP request outstanding)

Nov 20 12:13:50 5.1.1.1 Msg [0448] from ** IBM / MSS Family Client **: els:  GW.022: Nt fld slf tst nt 4 int PPP/0
Nov 20 12:13:50 5.1.1.1 Msg [0449] from ** IBM / MSS Family Client **: els:  IP.068: routing cache cleared
Nov 20 12:13:50 5.1.1.1 Msg [0450] from ** IBM / MSS Family Client **: els:  IP.058: del nt 4.0.0.0 rt via 0.0.0.4 nt 4 int PPP/0
```

Figure 29. Sample Contents from Syslog News Info File

If the initial ELS messages that are generated during and immediately after booting are of particular interest, then it is recommended that these messages also be displayed in the monitor queue, which is viewed with talk 2. Figure 30 on page 151 shows the talk 2 output including the initial messages that did not get remote-logged. Note that there is a message in the talk 2 output that indicates that the remote-logging facility is available. This does not indicate that a route exists to the remote workstation, nor that the associated interface is in the “Up” state. It simply provides a reference point before which no messages can be successfully remote-logged.

Also notice that you can account for the messages that were missing (indicated in Figure 29 with 2) in the talk 2 output.

```
12:08:17 SNMP.024: generic trc (P2) at snmp_mg.c(766): Now 0 trap destinations
12:08:17 SNMP.012: comm public added
12:08:17 SNMP.012: comm public added
12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_router_if_info(): sr
rdrec failed

12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_router_if_info(): sr
rdrec failed

12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:28   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:28   IP.022: add nt 4.0.0.0 int 4.1.1.1 nt 4 int PPP/0

     ( 297 messages not shown )                                         Corresponding Sequence
                                                                        Numbers in
12:08:43   GW.022: Nt fld slf tst nt 12 int PPP/2                       Remote-Logging Files :
12:08:43   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:48   IP.022: add nt 192.9.200.0 int 192.9.200.20 nt 0 int Eth/0   [0310] first message logged
12:08:48  SRT.017: Enabling SRT on port 1 nt 0 int Eth/0                -- not logged (ARP request) --
12:08:48  STP.016: Select as root TB-1, det topol chg                   -- not logged (ARP request)--
12:08:48  STP.026: Root TB-1, strt hello tmr                            -- not logged (ARP request)--
12:08:48  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0                        [0314]
12:08:48  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                        [0315]
12:08:48   IP.068: routing cache cleared                                [0316]


     ( 126 messages not shown )

12:13:38   GW.022: Nt fld slf tst nt 11 int ISDN/0                      [0443]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                           [0444]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                           -- not logged (ARP request) --
12:13:47  ARP.002: Pkt in 1 1 800 nt 5 int Eth/4                        -- not logged (ARP request)--
12:13:47  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                        [0447]
12:13:50   GW.022: Nt fld slf tst nt 4 int PPP/0                        [0448]
```

Figure 30. Output from Talk 2

You can use the timestamp, which appears in both the remote-logging output file and the talk 2 output, to determine when the first ELS message is successfully remote-logged. To use the timestamp for this purpose, configure ELS such that the timestamp in the monitor queue displays the time-of-day.

Also notice in Figure 29 on page 150 that messages 311-313 did not get remote-logged. This is because an ARP request was outstanding and until the ARP response is received, all but the first packet is dropped in the source IBM MSS Family Client. The ARP cache is cleared at a user-configured refresh rate, and the device issues a new ARP request. To determine when ARP requests are occurring, events ARP.002 and ARP.011 can be remote-logged, in addition to the ELS events of interest. Figure 31 shows ARP events logged to the *syslog_user_alert* file that account for events 445 and 446, which were indicated as missing in Figure 29 on page 150.

```
Nov 20 12:02:53 worksta01 root: THIS IS A TEST MESSAGE (user.alert)
Nov 20 12:08:48 5.1.1.1 Msg [0314] from ** IBM / MSS Family Client **: els:  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0315] from ** IBM / MSS Family Client **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0319] from ** IBM / MSS Family Client **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0444] from ** IBM / MSS Family Client **: els:  ARP.011: Del ent 1 3 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0447] from ** IBM / MSS Family Client **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
```

Figure 31. Sample Contents from Syslog_user_alert File

You can prevent the loss of ELS messages caused by this ARP sequence by establishing a static relationship between the IP address and the MAC address. The basic steps are outlined below and are illustrated in Figure 32 on page 152.

1. In talk 5, “ping” the remote workstation’s IP address
2. In talk 5, determine the interface (net) number used to send messages to the remote-workstation’s IP address

3. Use the net number from the previous step to determine the associated MAC address
4. In talk 6, add an ARP entry to establish a static IP address to MAC address relationship

```
*t 5
+p ip

IP>ping 192.9.200.1
PING 192.9.200.20 -> 192.9.200.1: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.9.200.1: icmp_seq=0. ttl=64. time=0. ms
----192.9.200.1 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms

IP>dump

  Type   Dest net            Mask          Cost    Age       Next hop(s)
.
   Dir*  192.9.200.0         FFFFFF00      1       102305    Eth/0
.
IP>exit
+int
                                                     Self-Test  Self-Test   Maintenance
Net   Net'   Interface  Slot-Port                    Passed     Failed      Failed
0     0      Eth/0      Slot: 1   Port: 1                 1          0            0
.
+p arp
ARP>dump
Network number to dump [0]? 0
Hardware Address        IP Address        Refresh
02-60-8C-2D-69-5D       192.9.200.1       2

Ctrl-P
*t 6
config>p arp
ARP config>add entry
Interface Number [0]? 0
Protocol [IP]? IP
IP Address [0.0.0.0]? 192.9.200.1
Mac Address []? 02608C2D695D
ARP config> list entry

Mac address translation configuration

IF #      Prot #  Protocol -> Mac address
   0           0  192.9.200.1 -> 02608C2D695D
ARP config>exit
Config>write

Ctrl-P

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

 (after reload, static ARP entry is active)
```

Figure 32. Example of Setting Up a Static ARP Entry

Additional Considerations

ELS Messages Containing IP Addresses

ELS messages containing an IP address which matches the IP address of the remote workstation will not be remote-logged, even if configured for remote-logging, and may appear under talk 2. These messages are discarded instead of being remote-logged in order to prevent excessive UDP packets from being sent on the network.

Duplicate Logging

If a facility value is repeated in *syslog.conf*, for example:

```
user.debug       /tmp/syslog_user_debug
user.alert       /tmp/syslog_user_alert
```

The syslog daemon will log *user.debug* messages only to the */tmp/syslog_user_debug* file while user.alert messages will be logged to both the */tmp/syslog_user_debug* file and the */tmp/syslog_user_alert* file. This is consistent with the syslog design that logs the more severe conditions in multiple places.

To prevent this duplicate logging, it is recommended that different facility values be specified in the *syslog.conf* file. A total of 19 facility values are available.

Recurring Sequence Numbers in Syslog Output Files

Depending upon the configuration of your network, it is possible for duplicate UDP packets containing ELS messages to arrive at the remote host. It is also possible for the packets to arrive in a different order than they were transmitted. An example of this phenomenon is shown in Figure 33. Notice that the messages with sequence numbers 628 through 633 are logged twice. Also notice that after the first occurrence of sequence number 0630, sequence number 0629 occurs again, followed by the second occurrence of 0630.

```
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
```

Figure 33. Example of Recurring Sequence Numbers in Syslog Output

Because neither Syslog nor UDP has the ability to handle duplicate or out of sequence packets, it is important to recognize the possibility of duplicate sequence numbers occurring.

Using ELS Message Buffering

Message buffering is an advanced feature of ELS that can help you with problem determination. You can set up defaults that ELS will use for message buffering or change how messages are buffered while the router is operating. Message buffering can minimize the information lost because messages have wrapped in the default message buffers. Message buffering is accessible through the **advanced** configuration or monitoring command. It enables you to:

- Specify whether buffering is active.
- Specify what events are written to the message buffer.
- Stop buffering and free the memory allocated for buffering.
- Display the status of the message buffer.

- Specify an event that stops message buffering and what action the system takes when the event occurs.
- Send a formatted version of the buffer to a file at a remote server.
- View a specific number or all of the ELS messages in the buffer.
- Write the buffer to a hard drive if a hard drive is present.
- Read a file that contains a formatted ELS message buffer from the hard drive , if a hard drive is present.
- Send a file that contains a formatted ELS message buffer from the hard drive , if a hard drive is present.

For specifics about the commands, see “ELS Message Buffering Configuration Commands” on page 171 and “ELS Message Buffering Monitoring Commands” on page 196.

The following example shows how to configure ELS message buffering.

```
 MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

 *t 5 :Enter t 5 at the * prompt.

 CGW Operator Console

 +ev :Enter ev at the + prompt.
 Event Logging System user console
 ELS>a :Enter a for advanced at the ELS prompt.
 Advanced ELS Console
 ELS Advanced>li s :Enter li s to list status at the > prompt.
 ------------------Advanced ELS Configuration------------------------
 Logging Status:  OFF  Wrap Mode:  ON   Logging Buffer Size: 0 KB
 Stop-Event:  NONE   Stop-String:   NONE
 Additional Stop-Action:  NONE
 ------------------------Run-Time Status-----------------------------
 Has Stop Condition Occurred?   NO   Messages currently in buffer:  0

 ELS Advanced>s b :Enter s b to set buffer size.
 Enter buffer size of 0 KB or between 148 and 593 KB [148]?
 Buffer size set to 148 KB
 ELS Advanced>s s e gw.26 :Enter s s e to set stop event eg. gw.26
 Stop Event "GW.026" has been set
 ELS Advanced>ex :Enter ex to exit Advanced to list gw.26
 ELS>list ev gw.26
 Level: C-TRACE
 Message: Mnt nt %n int %s/%d
 Active:         Count: 742

 ELS>a :Enter a to get back to advanced.
 Advanced ELS Console
 ELS Advanced>s s s Mnt nt 5 :Enter s s s to set the stop string.
 Stop String set to "Mnt nt 5"
 ELS Advanced>s s a ? :Enter s s a ? to query available stop actions.
 NONE
 APPN-DUMP  :Only available if APPN active and in the load image.
 SYSTEM-DUMP
 ELS Advanced>s s a s :Enter s s a s to set SYSTEM-DUMP stop action.
 Stop Action has been set to SYSTEM-DUMP
 ELS Advanced>s w off to :Enter s w on to set wrap mode off.
 Advanced Wrap Mode set to OFF.

 ELS Advanced>log sub gw all :Enter to enable the whole gw subsystem
 ELS Advanced>s l on :Enter s l on to start the logging process.
 Advanced Logging set to ON.
 ELS Advanced>li s :Enter to list status of logging.
 ------------------Advanced ELS Configuration------------------------
 Logging Status:  OFF  Wrap Mode: OFF  Logging Buffer Size: 148 KB
 Stop-Event:     GW.026   Stop-String:  Mnt nt 5
 Additional Stop-Action:  SYSTEM-DUMP


------------------------Run-Time Status-----------------------------
 Has Stop Condition Occurred?   YES  Messages currently in buffer:  7
```

```
ELS Advanced>v a n :Enter to view all messages in buffer. For this
                    trivial example any viewing command suffices.

 1  10:52:10   GW.026: Mnt nt 0 int Eth/0
 2  10:52:10   GW.026: Mnt nt 5 int Eth/1->This triggers stop action
 3  10:52:14   GW.026: Mnt nt 0 int Eth/0  Note that 5 more events
 4  10:52:14   GW.026: Mnt nt 5 int Eth/1  get logged before
 5  10:52:18   GW.026: Mnt nt 0 int Eth/0  logging stops and
 6  10:52:18   GW.026: Mnt nt 5 int Eth/1  the stop action occurs.
 7  10:52:22   GW.026: Mnt nt 0 int Eth/0

Bughlt: Dump initiated by ELS Stop Action.

BUGHLT+80; Dump initiated by ELS Stop Action.

Note:
In reality if the stop action is the SYSTEM-DUMP you will not be
able to list the final status as above nor view the buffer because
the router will be attempting to reload.
```

Chapter 13. Configuring and Monitoring the Event Logging System (ELS)

This chapter describes how to configure events logged by ELS and how to use the ELS commands. The information includes the following sections:

- "Accessing the ELS Configuration Environment"
- "ELS Configuration Commands"
- "Entering and Exiting the ELS Operating Environment" on page 175
- "ELS Monitoring Commands" on page 175

For more information on the Event Logging System and how to interpret ELS event messages, refer to "Chapter 12. Using the Event Logging System (ELS)" on page 137.

Accessing the ELS Configuration Environment

The ELS configuration environment is characterized by the `ELS config>` prompt. Commands entered at this prompt are described "Chapter 13. Configuring and Monitoring the Event Logging System (ELS)".

To enter the ELS configuration environment:

1. Enter **configuration**.

   The monitoring displays the `Config>` prompt. If the prompt does not appear, press **enter**.
2. At the `Config>` prompt, enter the following command to access ELS:

   ```
   event
   ```

   The monitoring displays the ELS configuration prompt (`ELS config>`). Now, you can enter ELS configuration commands.

To leave the ELS configuration environment, enter the **exit** command.

ELS Configuration Commands

Table 16 summarizes the ELS configuration commands. The remainder of this section describes each one in detail. After accessing the ELS configuration environment, you can enter ELS Configuration commands at the `ELS Config>` prompt.

Table 16. ELS Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 22.
Add	Adds an event to an existing group or creates a new group.
Advanced	Places you in the advanced configuration environment in which you can configure message buffering.
Clear	Clears all ELS configuration information.
Default	Resets the display or trap setting of an event, group, or subsystem.

Table 16. ELS Configuration Command Summary (continued)

Command	Function
Delete	Deletes an event number from an existing group or deletes an entire group.
Display	Enables message display on the console monitor.
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Noremote	Disables remote logging to a remote workstation.
Notrace	Controls disablement of packet trace events.
Notrap	Keeps messages from being sent out in SNMP traps.
Remote	Allows messages to be logged to a remote workstation.
Set	Sets the pin parameter and the timestamp feature options.
Trace	Controls enablement of packet trace events.
Trap	Allows messages to be sent to a network management workstation in SNMP traps.
View	Allows viewing of traced packets.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Add

Use the **add** command to add an individual event to an existing group or to create a new group. Group names must start with a letter and are case sensitive. You cannot append an entire subsystem to a group.

Syntax:

add *group_name subsystem.event_number*

Note: If the specified group does not exist, the following prompt asks you to confirm the creation of a new group:

```
Group not found. Create new group? (yes or no)
```

Advanced

Use the **advanced** command to enter the advanced configuration environment. In this environment you configure message buffering.

Syntax:

advanced

Clear

Use the **clear** command to clear all of the ELS configuration information.

Syntax:

clear

Example:

```
clear

You are about to clear all ELS configuration information
Are you sure you want to do this (Yes or No):
```

Default

Resets the display or trap setting of an event, group, or subsystem back to a disabled state.

Syntax:

default	display
	trap
	remote

display *event* **OR** *group* **OR** *subsystem*
Controls the output of the display of messages to the monitoring.

trap *event* **OR** *group* **OR** *subsystem*
Controls the generation of traps to the network management station.

remote *event* **OR** *group* **OR** *subsystem*
Controls the generation of traps to the remote station.

Delete

Use the **delete** command to delete an event number from an existing group or to delete the entire group. If the specified event is the last event to be deleted in a group, you will be notified. If *all* is specified instead of *subsystem.event_number*, a prompt asks you to confirm the deletion of the entire group.

Syntax:

delete	*group_name subsystem.event_number*

Display

Use the **display** command to enable message displaying on the monitoring monitor for specific events, a range of events for a subsystem, groups, or subsystems.

Syntax:

display	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Displays messages of the specified event (*subsystem.event#*).

group *groupname*
Displays messages of a specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event in the specified event range.

Displays a range of messages for the specified subsystem.

Example:

```
display range gw 19 22
```

Displays events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Displays messages associated with the specified subsystem. To find out which subsystems are on the router, type **list subsystems**.

Note: Although ELS supports all subsystems on the router, not all devices support all subsystems. See *Event Logging System Messages Guide* for a list of currently supported subsystems.

List

Use the **list** command to get updated information regarding ELS settings and listings of selected messages.

Syntax:

list
all
groups
pin
remote-log status
status
subsystem . . .
subsystems all
trace-status

all Lists information from all the **list** categories.

groups
Lists the user-defined group names and contents.

pin Lists the current number of ELS event messages sent in SNMP traps (per second).

remote-log status
Lists the current values of remote logging options.

Example:

```
list r

Remote Logging is ON
Source IP Address = 192.67.38.2
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_DAEMON
Default Syslog Priority Level = LOG_CRIT
Number of Messages in Remote Log = 256
Remote Logging Local ID = MYHOSTNAME
```

status Lists the subsystems, groups, and events that have been modified by the **display**, **nodisplay**, **trap**, **notrap**, **trace**, **notrace**, **remote**, and **noremote** commands.

Example:

```
list status

Subsystem:              TKR
Disp Levels:            STANDARD
Trap levels:            none
Trace levels:           none
Remote levels:          ERROR INFO TRACE
```

```
Syslog Facility/Level: LOG_USER LOG_INFO

Group        Disp     Trap    Trace  Remote
Mygroup     Unset    Unset    Unset    On
                                       Syslog Facilty/Level: LOG_DAEMON LOG_CRIT

Event        Disp     Trap    Trace  Remote
IP.007      Unset    Unset    Unset    On
                                       Syslog Facility/Level: LOG_CRON LOG_NOTICE
```

Note: Not only is remote logging enabled, but the display includes the Syslog Facility/Level values for each subsystem, group, and event. Ranges of events are listed as individual events.

subsystem

Lists names, events, and descriptions of all subsystems.

(Example output from a **list subsystem** command can be found beginning on page 178.)

subsystem *subsystem*

Lists all events in a specified subsystem.

Example:

```
list subsystem gw


Event      Level      Message

GW.001     ALWAYS   Copyright 1984 Mass Institute of Technology
GW.002     ALWAYS   Portable CGW %s Rel %s strtd
GW.003     ALWAYS   Unus pkt len %d nt %d int %s/%d
GW.004     ALWAYS   Sys %s q adv alloc %d excd %d
GW.005     ALWAYS   Bffrs: %d avail %d idle   fair %d low %d
GW.006     C-INFO    Pkt frm nt %d int %s/%d for uninit prt, disc
GW.007     C-INFO    Ip err %x nt %d int %s/%d
GW.008     U-INFO    Ip ovfl nt %d int %s/%d, disc
GW.009     UI-ERROR  Nt dwn ip rstrt nt %d int %s/%d
GW.010     UI-ERROR  Ip q len %d no ip buf nt %d int %s/%d
GW.011     U-INFO    Op err %x hst %wo nt %d int %s/%d
GW.012     U-INFO    Op err cnt excd hst %wo nt %d int %s/%d
GW.013     U-INFO    Rtrns cnt excd hst %wo nt %d int %s/%d
GW.014     UI-ERROR  Nt dwn op rstrt nt %d int %s/%d
GW.015     UI-ERROR  Nt dwn to hst %wo nt %d int %s/%d
GW.016     U-INFO    Op ovfl to hst %wo nt %d int %s/%d
GW.017     UE-ERROR  Intfc hdw mssng nt %d int %s/%d
GW.018     U-TRACE   Strt nt slf tst nt %d int %s/%d
GW.019     C-INFO    Slf tst nt %d int %s/%d
GW.020     U-TRACE   Nt pss slf tst nt %d int %s/%d
GW.021     UE-ERROR  Nt up nt %d int %s/%d
GW.022     U-TRACE   Nt fld slf tst nt %d int %s/%d
```

subsystems all

Lists all events in all subsystems.

trace-status

Displays information on the status of packet tracing, including configuration and run-time information.

Example:

```
list trace-status

------------------------- Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
```

Nodisplay

Use the **nodisplay** command to select and turn off messages displaying on the console.

Syntax:

nodisplay	event. . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Suppresses the displaying of a specified event (*subsystem.event#*).

group *groupname*
Suppresses the displaying of messages that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the displaying of a range of messages for the specified subsystem.

Example:

```
nodisplay range gw 19 22
```

Suppresses the display of events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Suppresses the displaying of messages associated with the specified subsystem.

Noremote

Use the **noremote** command to suppress the logging of events to a remote workstation based on event number, group, range of events, or subsystem.

Note: With the **noremote** command, there is usually no need to specify a *syslog_facility* and *syslog_level*, such as there is with the **remote** command. However, for **noremote subsystem** command, there exists the option of selectively suppressing specific message levels (for example, “error” only or “trace” only) rather than turning them all off. (If you do not specify any particular message level, “all” is assumed). Additionally, with the **noremote subsystem** command, you can set a *syslog_facility* and *syslog_level* for any remaining message levels that have not been turned off.

Syntax:

noremote	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Suppresses the remote logging of messages for the specified event.

group *group.name*
Suppresses the remote logging of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the remote logging of a range of messages for the specified subsystem.

Example:

```
noremote range gw 19 22
```

Suppresses the remote logging of events gw.019, gw.020, gw.021, and gw.022

subsystem *subsystem.name [syslog_facility syslog_level]*
Suppresses the remote logging of messages associated with the specified subsystem (*subsystem.name*).

Example 1:

```
noremote subsystem tkr
```

Suppresses the remote logging of all “tkr” messages.

Example 2:

```
ELS config> noremote subsystem tkr info
ELS config> SYSLOG FACILITY[LOG_USER]?
ELS config> SYSLOG LEVEL[LOG_INFO]?
```

In this example, “LOG_USER” and “LOG_INFO” were the values last picked for subsystem TKR. The command specified turns off the remote logging for subsystem TKR only for messages coded for “info”. Because *syslog_facility* and *syslog_level* was not specified, the software prompts for *syslog_facility* and *syslog_level*. If you enter another value at the prompts, that value will replace *syslog_facility* and *syslog_level* for the remaining remote-logged messages for the TKR subsystem.

Use the **list all** or **list status** commands to display what you have set with the **noremote** and **remote** commands.

For more information about *syslog_facility* and *syslog_level* see “Remote” on page 165.

Notrace

Disables packet trace for the specified event/range/subsystem/group.

Syntax:

notrace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of packet trace data for the specified event#

group *groupname*
Suppresses the sending of packet trace data that was previously added to the specified group (groupname).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Disables the sending of packet trace data for a range of messages for the specified subsystem.

Example:

```
trace range gw 19 22
```

Suppresses the sending of packet trace data for events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Suppresses the sending of packet trace data for the specified subsystem (subsystemname).

Notrap

Use the **notrap** command to select and turn off messages so that they are no longer sent to a network management workstation in SNMP traps.

Syntax:

notrap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of the specified message in an SNMP trap (*subsystem.event#*).

group *groupname*
Suppresses the sending of messages in SNMP traps that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the sending of messages for the events in the specified range for the specified subsystem in SNMP traps.

Example:

```
notrap range gw 19 22
```

Suppresses the sending of messages for events gw.19, gw.20, gw.21, and gw.22 in SNMP traps.

subsystem *subsystemname*
Suppresses the sending of messages in SNMP traps that are associated with the specified subsystem.

Remote

Use the **remote** command to select the events to be logged to a remote workstation by event number, range of events, group, or subsystem.

Syntax:

remote	event . . .
	range . . .
	group . . .
	subsystem . . .

event *subsystem.event# syslog_facility syslog_level*

Causes the specified event to be logged remotely.

Syslog facility and level values are used by the syslog daemon in the remote workstation to determine where to log the messages. This value overrides the default values that are set with the **set facility** and **set level** commands.

syslog_facility

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

These values do NOT have any particular association with any daemons on the IBM MSS Family Client. They are merely identifiers which are used by the syslog daemon on the remote workstation.

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_numbe*r is the number of the last event of the specified event range.

Causes the events in the specified range for the specified subsystem to be remotely logged based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 165.

Example:

```
remote range gw 19 22 log_user log_info
```

Causes the event gw.19, gw.20, gw.21, and gw.22 to be logged remotely on the *syslog_facility* value of log_user and the *syslog_level* value of log_info.

group *group.name syslog_facility syslog_level*
Allows events belonging to the specified group to be logged remotely based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 165.

subsystem *subsystem.name message_level syslog_facility syslog_level*
Where *subsystem.name* is the name of the subsystem and *message_level* is the level of messages selected in the subsystem.

Causes the events within the specified *subsystem.name* whose *message_level* agrees with the specified *message_level* to be logged remotely at the files based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 165.

Message_level is a value such as “ALL,” “ERROR,” “INFO,” or “TRACE” . See “Logging Level” on page 139. The value specified in the **remote** command must agree with the value as coded on the particular event within the subsystem, or that event within the subsystem will not be remotely logged.

Example:

```
remote subsystem TKR all log_user log_info
```

In the above example, all messages in subsystem TKR (“all” includes any messages coded for “error,” “info,” or “trace”) will be logged remotely based on log_user and log_info values at the remote host.

Use the **list all** or **list status** commands to display what you have set with the **noremote** and **remote** commands.

Set

Use the **set** command to set the maximum number of tags per second, the timestamp feature, or to set tracing options.

Syntax:

set	pin . . .
	remote-logging . . .
	timestamp . . .
	trace . . .

pin *max_traps*
Use the **set pin** command to set the pin parameter to the maximum

number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number (*max_traps*) is sent every tenth of a second.)

remote-logging

Use the **set remote-logging** command to configure remote logging options. When these options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set remote-logging	on
	off
	facility . . .
	level . . .
	no-msgs
	remote_ip_addr . . .
	source_ip_addr ...
	local_id

on Turns remote logging on. Remote logging is now enabled to allow any messages selected by the **remote** command to be actively logged.

off Turns remote logging off. All messages selected by the ’remote’ command will be prevented from being logged.

facility

Specifies a value that, in combination with the *level* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog facility values:

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

level Specifies a value that, in conjunction with the *facility* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog level values:

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

no-msgs
Specifies the number of messages in the buffer for the remote log before log wraps.

remote_ip_addr
This is an ip address of the form xxx.xxx.xxx.xxx where xxx can be any integer 0 to 255. It represents the ip address of the remote host where the log files reside.

source_ip_addr
This is an ip address of the form xxx.xxx.xxx.xxx where xxx can be any integer 0 to 255.

You should use an IP address that is configured in the MSS Family Client for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address is quickly resolved to a hostname by the name server, or at least that the name server responds quickly with "address not found."

To determine that the IP address resolves properly enter the **host** command on your workstation as shown:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address that resolves more quickly.

local_id
This is any character string of up to 32 characters, which is included in the logged message at the remote file and can help identify which machine logged the message.

timestamp [timeofday or uptime or off]
Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the router was last initialized) appears next to each message. Set timestamp can also be turned off.

Use the **set timestamp** command to enable one of the following timestamp options.

timeofday
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

trace Use the **set trace** command to configure tracing options. If you configure tracing options from the monitoring environment, the changes take effect immediately. They return to their previously configured settings when the device is rebooted.

Note: Tracing should be used only under the direction of trained support personnel. Tracing, especially when used with disk-shadowing enabled, uses device resources and can impact overall performance and throughput.

Syntax:

```
set trace                     decode
                              default-bytes-per-pkt
                              max-bytes-per-pkt
                              memory-trace-buffer-size
                              off
                              on
                              reset
                              stop-event
                              wrap-mode
```

decode *off/on*
Turns packet decoding on or off. Packet decoding is not supported by all components.

default-bytes-per-pkt *bytes*
Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

max-bytes-per-pkt *bytes*
Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*
Sets the size, in bytes, of the RAM trace buffer.

Valid Values: 0, ≥10,000

Default Value: 0

off Disables packet tracing.

on Enables packet tracing.

reset Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS

event id (for example: TCP.013) or “None”. “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013”.

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

wrap-mode [off or **on]**
Turns the trace buffer wrap mode on or off. If wrap mode is on and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Trace

Enables packet trace for the specified event/range/subsystem/group. When the **trace** command is used from the `ELS Config>` prompt, the changes become part of the configuration, and a reboot is required to activate the changes.

Syntax:

trace	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Causes the specified trace event (*subsystem.event#*) to be displayed on the system monitoring.

group *groupname*
Allows trace events that were previously added to the specified group to be displayed on the router monitoring.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the trace events in the specified range for the specified subsystem to be displayed on the system monitoring.

Example:

```
trace range gw 19 22
```

Causes the trace events gw.19, gw.20, gw.21, and gw.22 to be displayed on the system monitoring.

subsystem *subsystemname*
Allows trace events associated with the specified subsystem to be displayed on the router monitoring.

Trap

Use the **trap** command to select the message to be sent to the remote SNMP network management workstation. A remote SNMP network management workstation is an IP host in the network acting as an SNMP manager.

Syntax:

trap event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*

Causes the specified message (*subsystem.event#*) to be sent to a network management workstation in an SNMP trap.

group *groupname*

Allows messages that were previously added to the specified group to be sent to a network management workstation in an SNMP trap.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be sent to a network management workstation in an SNMP trap.

Example:

```
trap range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be sent to a network management workstation in an SNMP trap.

subsystem *subsystemname*

Allows messages associated with the specified subsystem to be sent to a management station in an SNMP trap.

Note: Messages for the IP, ICMP, ARP and UDP subsystems cannot be sent in SNMP traps because these areas are or may be used in the process of sending the SNMP trap. This could lead to an infinite loop of traffic putting an undue strain on the router.

ELS Message Buffering Configuration Commands

Table 17 describes the commands available at the `ELS Config Advanced>` prompt.

Table 17. ELS Message Buffering Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Displays the configuration settings for message buffering.

Table 17. ELS Message Buffering Configuration Commands (continued)

Command	Function
Log	Enables logging of selected messages to the message buffer.
Nolog	Turns off logging of selected messages to the message buffer.
Set	Sets the size of the message buffer, the wrapping mode, whether logging occurs, which event will end message buffering, and what the system does when message buffering is stopped by an event.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 23.

List

Use the **list** command to list the ELS message buffering configuration.

Syntax:

list	status

Example:

```
ELS Config Advanced> list status
---------------------------------Configuration-----------------------------------
Logging Status:    OFF    Wrap Mode:   ON  Logging Buffer Size:    8500   Kbytes
Stop-Event:    APPN.2         Stop-String:     netdn for  intf 6
Additional Stop-Action:  NONE
```

See "Set" on page 173 for a description of the commands that change the values in the display.

Log

Use the **log** command to select which messages will be logged to the message buffer.

Syntax:

log	event
	group
	range
	subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be logged to the message buffer.

Nolog

Use the **nolog** command to remove messages from the defined list of messages that are logged to the message buffer.

Syntax:

nolog event

group

range

subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) not to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group not to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem not to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 not to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem not to be logged to the message buffer.

Set

Use the **set** command to configure various ELS message buffering options.

Syntax:

set buffer-size *Kbytes*

logging [on or off]

stop action . . .

stop event *subsystem.event#*

stop string *text*

wrap on or off]

buffer-size *Kbytes*
Specifies the size, in kilobytes, of the message buffer that the system should allocate. The **mem** command displays this memory as “Never Alloc.” Setting this value too high could prevent the router from operating correctly after a reboot because of insufficient memory for protocols and features.

Valid values: 0 KB to 80% of the memory available on the router.

Default value: 0 (no message buffering)

Note: You must allocate a buffer with this command before you can set logging on.

logging [on or **off]**
Specifies whether message buffering will occur. This command will not take affect until you allocate a buffer using the **set buffer-size** command. The default is off.

stop action [appn-dump or **disk-offload**or **none** or **system-dump]**
Specifies the additional action the system takes when the “stop event” (and if specified, the “stop string”) occurs. The actions are:

appn-dump
Dumps the APPN protocol, if it is active. The APPN dump will indicate that the dump was taken as the result of a stop action.

disk-offload
Writes a formatted version of the buffer to a file on the hard drive . If the file already exists, the new file replaces it. You can then use the **tftp file** monitoring command to send the file to a remote host.

none No other action is taken after logging stops.

system-dump
Dumps the entire system. The system dump will indicate that the dump was taken as the result of a stop action.

Default value: none

stop event [*subsystem.event#* or **none]**
Specifies the event (*subsystem.event#*) that stops logging. If you have specified a stop string, the text in the stop string must also match. When the stop event occurs:

1. The next five ELS messages are logged.
2. Logging stops.
3. The system performs the specified “stop action.”

Logging remains stopped until the next time you issue the **set logging on** command or reboot the router.

If you do not specify the stop event when you enter the command, the system prompts you to enter the stop event. Specifying **none** disables the stop event function.

Default value: none

stop string *text* or **none**

Specifies the string to be used in conjunction with the “stop event” to stop logging. If you have not specified a stop event, the system ignores the “stop string.”

Text can be any ASCII string up to 32 characters in length. If you do not specify *text* when you enter the command, the system will prompt you for the string. Entering **none** clears the “stop string.”

Default value: none

wrap [on or **off]**

Specifies whether to stop the log when the buffer is full (off) or to log the new messages at the beginning of the buffer (on).

Default value: off

Entering and Exiting the ELS Operating Environment

The ELS monitoring environment (available from the GWCON process) is characterized by the `ELS>` prompt. Commands entered at this prompt modify the current ELS parameter settings. These commands are described “Chapter 13. Configuring and Monitoring the Event Logging System (ELS)” on page 157.

To enter the ELS monitoring environment from OPCON:

1. Enter the **console** command.

   ```
   * console
   ```

   The monitoring displays the GWCON prompt (+). If the prompt does not appear when you first enter GWCON, press **enter**.
2. At the GWCON prompt, enter the following command to access ELS:

   ```
   + event
   ```

   The monitoring displays the ELS monitoring prompt (`ELS>`). Now, you can enter ELS monitoring commands.

To leave the ELS monitoring environment, enter the **exit** command.

ELS Monitoring Commands

This section summarizes and then explains all the ELS monitoring commands. After accessing the ELS Monitoring environment, you can enter ELS monitoring commands at the ELS> prompt.

Table 18. ELS Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Advanced	Places you in the advanced configuration environment in which you can configure message buffering.
Clear	Resets to zero the counts of messages associated with specified events, groups, or subsystems.
Display	Enables message display on the console.
Exit	Exits the ELS console process and returns the user to GWCON.

Table 18. ELS Monitoring Command Summary (continued)

Command	Function
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Noremote	Disables remote logging to file at remote workstation.
Notrace	Disables trace event display on the console.
Notrap	Keeps messages from being sent out in SNMP traps to the network management workstation.
Packet-trace	Provides an enhanced central environment for setting and listing active packet tracing parameters.
Remote	Allows messages to be logged at a file on a remote workstation.
Remove	Frees up memory by erasing stored information.
Restore	Clears current settings and reloads initial ELS configuration.
Retrieve	Reloads the saved ELS configuration.
Save	Stores the current configuration.
Set	Sets the pin parameter and the timestamp feature.
Statistics	Displays available subsystems and pertinent statistics.
Trace	Enables trace event display on the console.
Trap	Allows messages to be sent to a network management workstation in SNMP traps.
View	Allows viewing of traced packets.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Advanced

Use the **advanced** command to enter the advanced monitoring environment. In this environment you change message buffering operation.

Syntax:

advanced

Clear

Use the **clear** command to reset to zero the counts of the display, trace, trap, or remote commands as they relate to specific events, groups or subsystems.

Syntax:

clear event . . .
group . . .
subsystem . . .

event *subsystem. event#*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified event (*subsystem.event#*).

group *group.name*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified group (*group.name*).

subsystem *subsystem.name*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified subsystem (*subsystem.name*).

Display

Use the display command to enable the message display on the monitoring monitor for specific events.

Syntax:

display	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Displays messages for the specified event (subsystem.event#).

group *groupname*
Displays messages of a specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event in the specified event range.

Displays a range of messages for the specified subsystem.

Example:

```
display range gw 19 22
```

Displays events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystem.name*
Displays any messages associated with the specified subsystem (*logging level*). If you do not specify a logging level, all messages for that subsystem are turned on.

List

Use the **list** command to get updated information regarding ELS settings and to get listings of selected messages.

Syntax:

list	all
	active . . .
	event . . .
	groups . . .
	pin
	remote-log status
	subsystem . . .
	trace-status

all Lists all subsystems, defined groups, enabled subsystems, enabled events, and pins.

active *subsystem.name*

Displays the events that are active for a specific subsystem or have non-zero message counts.

Example:

```
list active ip
Event      Active  Count  Message

IP.007              2874  %I -> %I
IP.022                13  add nt %I int %I nt %n int %s/%d
IP.036              2874  rcv pkt prt %d frm %I
IP.058                23  del nt %I rt via %I nt %n int %s/%d
IP.068     D          37  routing cache cleared
D=Display on   T=Trap on   P=Packet Trace on   F=Filter on  R=Remote Logging on
A=Advanced on
```

If Remote logging is turned on, those events displayed as active for a subsystem will have an “R” next to their name.

event *subsystem.event#*

Displays the logging level, the message, and the count of the specified event.

Example:

```
list event ip.007

Level: p-TRACE
Message: source_ip_address -> destination_ip_address
Active:  Count: 84182
```

If Remote-logging had been activated for this event, and the *syslog_facility* and *syslog_level* values were log_daemon and log_crit, the last lines would look like:

```
Active:  R count:84182
Syslog Facility: log_daemon   Syslog Level: log_crit
```

groups *group.name*

Displays the user-defined group names.

pin Lists the current number of ELS event messages sent per second in SNMP traps. This is a threshold value that can be used to reduce the amount of SNMP trap traffic.

Example:

```
list pin

Pin: 100 events/second
```

remote-log status

Lists the current values of the remote logging options set in the **set remote-logging** command.

Example:

```
list r

Remote Logging is On
Source Ip Address = 192.9.200.8
Remote  Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_USER
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log = 256
Remote Logging Local ID =  SPHINX
```

subsystem *subsystem.name*

Lists event names, the total number of events that have occurred, and their descriptions.

Note: Although ELS supports all subsystems on the router, not all devices support all subsystems. See *ELS Messages* for a list of currently supported subsystems.

subsystem *subsystem.name*

Lists all events, logging levels, and messages for the specified subsystem.

Example:

```
list subsystem eth

Event      Level      Message
ETH.001    P-TRACE    brd rcv unkwn type packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.002    UE-ERROR   rcv unkwn typ packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.010    C-INFO     LLC unk SAP DSAP source_Ethernet_address ->
                      destination_Ethernet_address nt network
```

subsystem all

Lists all events, logging levels, and messages for every event that has occurred on the router.

trace-status

Displays information on the status of packet tracing, including configuration and run-time information.

Example:

```
list trace-status

------------------------- Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013

------------------------ Run-time Status ----------------------------
Packets in RAM Trace Buffer:1   Free Trace Buffer Memory:99958
Trace Errors:0  First Packet:1  Last Packet:1
Trace Records Stored on HD:8  Trace Buffer File Size:16560

Has Stop Trace Event Occurred? NO
```

- “Trace Status” in the LIST TRACE-STATUS display will indicate OFF when STOP-ON-EVENT action occurs.
- “Trace Buffer File Size” will display “<wrapped>” when a wraparound has occurred in the trace file.

`ELS Config>`**LIST TRACE** command under **talk 6** displays information similar to the following:

```
------------------------- Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
```

Nodisplay

Use the **nodisplay** command to select and turn off messages displaying on the console.

Syntax:

nodisplay	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Suppresses the displaying of messages for the specified event.

group *group.name*
Suppresses the displaying of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the displaying of a range of messages for the specified subsystem.

Example:

```
nodisplay range gw 19 22
```

Suppresses the display of events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystem.name*
Suppresses the displaying of messages associated with the specified subsystem (*logging level*).

Noremote

Use the **noremote** command to select and turn off messages logging to a remote workstation.

Syntax:

noremote	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Suppresses the remote logging of messages for the specified event.

group *group.name*
Suppresses the remote logging of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the remote logging of a range of messages for the specified subsystem.

Example:

```
noremote range gw 19 22
```

Suppresses the remote logging of events gw.19, gw.20, gw.21, and g.22

subsystem *subsystem.name*
Suppresses the remote logging of messages associated with the specified subsystem (*logging level*).

Example:

```
noremote subsystem tkr
```

Note: With Noremote, there is no need to specify a Syslog Facility and Level, such as there is with Remote.

Use the **list event** and **list active** commands to verify what you set with the **remote** and **noremote** commands.

Notrace

Use the **notrace** command to stop display of selected trace events at the monitoring.

Syntax:

notrace	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Suppresses the display of the specified tracing event.

group *groupname*
Suppresses the display of tracing events related to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Disables the sending of packet trace data for a range of messages for the specified subsystem.

Example:

```
notrace range gw 19 22
```

Suppresses the sending of packet trace data for events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname [logging-level]*
Suppresses the display of tracing events that are associated with the specified subsystem and logging level. If you do not specify a *logging-level* you suppress tracing for all logging levels for the subsystem.

Example:

```
notrace subsystem frl error

notrace subsystem frl
```

Notrap

Use the **notrap** command to select and turn off messages so that they are no longer sent to a network management workstation in SNMP traps.

Syntax:

notrap	event. . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Suppresses the sending of the specified message in an SNMP trap (*subsystem.event#*).

group *groupname*
Suppresses the sending of messages in SNMP traps that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the sending of messages for the events in the specified range for the specified subsystem in SNMP traps.

Example:

```
notrap range gw 19 22
```

Suppresses the sending of messages for events gw.19, gw.20, gw.21, and gw.22 in SNMP traps.

subsystem *subsystemname [logging-level]*
Suppresses the sending of messages in SNMP traps that are associated with the specified subsystem and logging level. If you do not specify a *logging-level* you suppress trapping for all logging levels for the subsystem.

Example:

```
notrap subsystem eth error
```

Packet Trace

Use the **packet-trace** command to display/enable/disable packet tracing information for various subsystems.

Syntax:

packet-trace

Use the **Exit** command when you are finished using Packet Trace.

For complete command descriptions, see “Packet-trace Monitoring Commands” on page 193.

Remote

Use the **remote** command to select the events to be logged to a remote file by event number, range of events, group, or subsystem.

Syntax:

remote	event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event# syslog_facility syslog_level*
Causes the specified event to be logged remotely.

Syslog facility and level values are used by the syslog daemon in the remote workstation to determine where to log the messages. This value overrides the default values that are set with the **set facility** and **set level** commands.

syslog_facility

log_auth

log_authpriv

log_cron

log_daemon

log_kern

log_lpr

log_mail

log_news

log_syslog

log_user

log_uucp

log_local0-7

syslog_level

log_emerg

log_alert

log_crit

log_err

log_warning

log_notice

log_info

log_debug

These values do NOT have any particular association with any daemons on the IBM MSS Family Client. They are merely identifiers which are used by the syslog daemon on the remote workstation.

Example:

```
remote event gw.019 log_user log_info
```

group *group.name syslog_facility syslog_level*
Allows events belonging to the specified group to be logged remotely based on the *syslog_facility* and *syslog_level* values. See “the remote event command”.

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the events in the specified range for the specified subsystem to be remotely logged based on the *syslog_facility* and *syslog_level*. See “the remote event command” on page 183.

Example:

```
remote range gw 19 22 log_user log_info
```

Causes the event gw.19, gw.20, gw.21, and gw.22 to be logged remotely to the files specified by the *syslog_facility* value of log_user and the *syslog_level* value of log_info.

subsystem *subsystem.name message_level syslog_facility syslog_level*

Where *subsystem.name* is the name of the subsystem and *message_level* is the level of messages selected in the subsystem.

Causes the events within the specified *subsystem.name* whose *message_level* agrees with the specified *message_level* to be logged remotely based on the *syslog_facility* and *syslog_level*. See “the remote event command” on page 183.

Message_level is a value such as “ALL,” “ERROR,” “INFO,” or “TRACE” . See “Logging Level” on page 139. The value specified in the **remote** command must agree with the value as coded on the particular event within the subsystem, or that event within the subsystem will not be remotely logged.

Example:

```
remote subsystem eth all log_user log_info
```

In the above example, all messages in subsystem TKR (“all” includes any messages coded for “error,” “info,” or “trace”) will be logged remotely to files specified by log_user and log_info at the remote host.

Use the **list event** and **list active** commands to verify what you set with the **remote** and **noremote** commands.

Remove

Use the **remove** command to free up memory by erasing stored information. If you have previously saved the current configuration with the **save** command, remove allows you to erase the saved configuration.

Syntax:

remove

Restore

Use the **restore** command to clear all current settings (except counters) and reload the initial ELS configuration. To retain the current settings, use the **save** command before restoring the initial configuration.

Syntax:

restore

Retrieve

Use the **retrieve** command to reload the saved ELS configuration. If you have previously saved the current configuration with the **save** command, use **retrieve** to reload it. **Retrieve** does not erase the saved configuration after it executes. To erase the saved configuration, use the **remove** command.

Syntax:

retrieve

Save

Use the **save** command to store the current configuration (except counters). **Save** does not affect the default configuration (the one you set with the configuration commands). Use **save** after modifying the configuration with the monitoring commands with the intention of saving this configuration over a restart. There can be only one saved configuration at a time. To reload the saved configuration, use the **retrieve** command.

Syntax:

save

Set

Use the **set** command to set the maximum number of traps per second, to set the timestamp feature, or to set the tracing options.

Syntax:

set pin . . .
remote-logging . . .
timestamp . . .
trace . . .

pin Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number *max_traps* is sent every tenth of a second.)

remote-logging
Use the **set remote-logging** command to configure remote logging options. When these options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set remote-logging on
off
facility . . .
level . . .
local_id

remote_ip_addr . . .

source_ip_addr ...

on Turns remote logging on. Remote logging is now enabled to allow any messages selected by the **remote** command to be actively logged.

off Turns remote logging off. All messages selected by the **remote** command will be prevented from being logged.

facility

Specifies a value that, in combination with the *level* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog facility values:

log_auth

log_authpriv

log_cron

log_daemon

log_kern

log_lpr

log_mail

log_news

log_syslog

log_user

log_uucp

log_local0-7

level Specifies a value that, in conjunction with the *facility* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog level values:

log_emerg

log_alert

log_crit

log_err

log_warning

log_notice

log_info

log_debug

local_id

Specifies a 1-32 character identifier that appears in the remote logging message that you can use to identify which machine logged a particular message.

remote_ip_addr

This is an IP address of the remote host where the log files reside.

source_ip_addr

Specifies the IP address of the machine that originated the message that is being remotely-logged.

You should use an IP address that is configured in the MSS Family Client for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address is quickly resolved to a hostname by the name server, or at least that the name server responds quickly with "address not found."

To determine that the IP address resolves properly enter the **host** command on your workstation as shown:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address that resolves more quickly.

timestamp

Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the router was last initialized) appears next to each message, or to turn off message timestamping.

Note: If you turn on timestamping, you must remember to go back into the CONFIG process and set the router's date and time using the time command. Otherwise, all messages will come out with 00:00:00, or negative numbers in the hours, minutes, and/or seconds, for example 00:-4:-5.

Use the **set timestamp** command to enable one of the following timestamp options:

timeofday

Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime

Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle of uptime for the router. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

Syntax:

set timestamp [timeofday or uptime or off]

trace Use the **set trace** command to configure tracing options. When tracing options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set trace decode . . .

default-bytes-per-pkt . . .

max-bytes-per-pkt . . .

memory-trace-buffer-size . . .

off

on

reset

stop-event . . .

wrap-mode . . .

decode . . .
Sets packet decode options. Packet decoding is not supported by all components.

exclude
Excludes the specified frame type for decode. The possible frame types for exclusion are:

lecontrol
LE Control

ip IP

arp ARP

ipx IPX

netbios
NetBIOS

bpdu BPDU

appletalk
AppleTalk

aarp AppleTalk ARP

hex Turns off printing of hexadecimal frame data.

summary
Turns off printing of a one-line summary decode. A complete decode is printed.

all Excludes all packet types from the trace. No frame types are decoded.

none Excludes no packet types from the trace. *exlcude all*.

include
Includes the specified frame type for decode. The possible frame types for inclusion are:

lecontrol
LE Control

ip IP

arp ARP

ipx IPX

netbios
NetBIOS

bpdu BPDU

appletalk
AppleTalk

aarp AppleTalk ARP

hex Turns on printing of hexadecimal frame data.

summary
Turns on printing of a one-line summary decode. A complete decode is not printed.

all Includes all packet types in the trace.

none Includes no packet types in the trace. This is the opposite of *include all*.

off Sets decoding off.

on Sets decoding on.

Note: The default setting is to print complete decode output for all frame types. Use the **list trace-status** command to see the current decode settings. See page 179.

default-bytes-per-pkt *bytes*
Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

max-bytes-per-pkt *bytes*
Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*
Sets the size, in bytes, of the RAM trace buffer.

Valid Values: 0, ≥10,000

Default Value: 0

off Disables packet tracing.

on Enables packet tracing.

reset Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None”. “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013”.

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

Example:

```
set trace stop-event TCP.013
```

wrap-mode *off/on*
Turns the trace buffer wrap mode on or off. When wrap mode is enabled and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Statistics

Use the **statistics** command to display a list of all of the available subsystems and their statistics.

Note: The following example may not match your display exactly. The output of the command depends on the version and release of the installed software.

Syntax:

statistics

Example:

```
statistics

Subsys  Vector  Exist   String  Active    Heap

  GW     105     101      3411     0         0
 FLT      20       7       184     0         0
 BRS      50       5       201     0         0
 ARP     150     142      7030     0         0
  IP     100     100      2463     2        20
ICMP      30      21       529     0         0
 TCP      60      57      2420     0         0
 UDP      10       6       179     0         0
 BTP      40      13       695     0         0
 RIP      30      22       474     0         0
OSPF      80      73      2859     0         0
MSPF      40      17       593     0         0
TFTP      35      29       819     0         0
SNMP      30      28       821     0         0
 DVM      30      21       589     0         0
  DN     140     115      5842     0         0
  XN      35      21       780     0         0
 IPX     110     110      4705     0         0
CLNP      80      58      1763     0         0
ESIS      40      24       716     0         0
ISIS      80      58      2422     0         0
DNAV      50      26      1314     0         0
 AP2      80      70      1755     0         0
ZIP2      60      51      1859     0         0
R2MP      50      38      1185     0         0
 VIN      90      79      3159     0         0
 SRT     120      94      5040     0         0
 STP      60      32      1590     0         0
  BR      50      30      1616     0         0
SRLY      30      28      1409     0         0
 ETH      60      47      1098     0         0
  SL      50      35       584     0         0
 TKR      60      45      2031     0         0
 X25      70      53      1909     0         0
FDDI      30      27      1155     0         0
SDLC     100      95      4263     0         0
 FRL     130      97      6068     0         0
 PPP     190     186      6394     0         0
X251      50      16       546     0         0
X252      50      34       996     0         0
X253      50      42      1649     0         0
ISDN      50      43      1994     0         0
IPPN      20       4       132     0         0
 WRS      40      33      1938     0         0
 LNM      70      60      3137     0         0
 LLC     170     168      9840     0         0
 BGP      80      74      2477     0         0
 MCF      15       9       244     0         0

 V25B     30      28      1058     0         0

 COMP     80      26      1050     0         0
 NBS     100      50      3029     0         0
 ATM     300     216     10808     0         0
 LEC     200     174      7258     0         0
APPN     100      28       467     0         0
ILMI     150      23       487     0         0
```

```
SAAL     30     26       621     0        0
 SVC     30     26       465     0        0
 LES    400    361     22333     0        0
LECS    150    145      5666     0        0

EVLOG      1       1       105     0         0
 NOT      25      15       508     0         0
NHRP     250     211      8193     0         0
 XTP      64      58      2271     0         0
 ESC     150      67      3122     0         0
 LCS      40      22       858     0         0
 LSA      70      61      3506     0         0
 MPC     130      30      1677     3        44
SCSP      40      34      1234     0         0
ALLC      50      36      1842     0         0
 NDR      50      38      1150     0         0
 MLP     100      93      4006     0         0
 SEC      50      30       688     0         0
ENCR     100       4       194     0         0
  PM      25       6       120     0         0
 DGW      20       9       238     0         0
QLLC      55      54      2411     0         0

Total   6490    4942    215805     5        64

Maximum:7976 vector, 155 subsystem
Memory:71784/620 vector+ 81256/217714 data+ 64 heap=371438Subsys
```

Subsys
Name of subsystem

Vector
Maximum size of subsystem

Exist Number of events defined in this subsystem

String Number of bytes used for message storage in this subsystem

Active Number of active (displayed, trapped, or counted) events in the subsystem

Heap Dynamic memory in use by subsystem

Trace

Use the **trace** command to select the trace events to be displayed on the system monitoring. This command provides function that is similar to the **packet trace** command described in “Packet-trace Monitoring Commands” on page 193.

Syntax:

trace event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*
Causes the specified trace event (*subsystem.event#*) to be displayed on the system monitoring.

group *groupname*
Allows trace events that were previously added to the specified group to be displayed on the router monitoring.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_numbe*r is the number of the last event of the specified event range.

Causes the trace events in the specified range for the specified subsystem to be displayed on the system monitoring.

Example:

```
trace range gw 19 22
```

Causes the trace events gw.19, gw.20, gw.21, and gw.22 to be displayed on the system monitoring.

subsystem *subsystemname*
Allows trace events associated with the specified subsystem to be displayed on the router monitoring.

Trap

Use the **trap** command to select the message to be sent to the remote SNMP network management workstation. A remote SNMP network management workstation is an IP host in the network acting as an SNMP manager.

Syntax:

trap	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be sent to a network management workstation in an SNMP trap.

group *groupname*
Allows messages that were previously added to the specified group to be sent to a network management workstation in an SNMP trap.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be sent to a network management workstation in an SNMP trap.

Example:

```
trap range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be sent to a network management workstation in an SNMP trap.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be sent to a management station in an SNMP trap.

Note: Messages for the IP, ICMP, ARP and UDP subsystems cannot be sent in SNMP traps because these areas are or may be used in the process of sending the SNMP trap. This could lead to an infinite loop of traffic putting an undue strain on the router.

View

Use the **view** command to view traced packets.

Syntax:

view current
first
jump
last
next
prev
search ...

current
Displays the current trace packet. If the current packet is not valid, the first packet in the trace buffer is displayed.

first Displays the first traced packet in the trace buffer.

jump *n*
Displays the traced packet *n* packets ahead of or behind the current packet.

last Displays the last traced packet in the trace buffer.

next Displays the next traced packet.

prev Displays the previous traced packet.

search
Displays the next traced packet that contains the specified information. You can specify the search information by:

- Hexadecimal string
- IP address
- ASCII text

Packet-trace Monitoring Commands

This section describes the Packet-trace Monitoring commands. After accessing the Packet-trace Monitoring environment, you can enter Packet-trace Monitoring commands at the `ELS Packet Trace>` prompt.

Table 19. Packet Trace Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Off	Disables packet tracing.
On	Enables packet tracing. Prompts for memory trace buffer size if not previously set.
Reset	Clears the trace buffer and resets all associated counters.
Set	Configures tracing options.

Table 19. Packet Trace Monitoring Command Summary (continued)

Command	Function
Subsystems	Activates tracing for the subsystems that support packet tracing, or displays a summary.
Trace-status	Displays information on the status of packet tracing, including configuration and run-time.
View	Provides View Captured Packet Trace Buffers Console
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Off

Use the **off** command to disable packet tracing.

Syntax:

off

On

Use the **on** command to enable packet tracing.

Syntax:

on

Reset

Use the **reset** command to clear the trace buffer and reset all associated counters.

Syntax:

reset

Set

Use the **set** command to configure tracing options.

Syntax:

set	decode
	default-bytes-per-pkt
	max-bytes-per-pkt
	memory-trace-buffer-size
	stop-event
	wrap-mode
	exit

For an explanation of the `set` command, see page 187.

Subsystems

Use the **subsystems** command to activate tracing for the subsystems that support packet tracing, or to display a summary.

Syntax:

Example:

```
subsystems atm
Network number? 0
ATM Interface is selected
on | off | list [list]? on
Note that SVC  uses VPI = 0, VCI = 5
and ILMI uses VPI = 0, VCI = 16
Beginning of VPI range [0]?
End of VPI range [0]?
Beginning of VCI range [0]? 16
End of VCI range [0]? 16
Tracing event ATM.88: ATM frames
```

Example:

```
subsystems lec
Network number? 1
ATM Emulated LAN is selected
on | off | list [list]? on
Trace which types of frames (data, control, both) [both]?
Tracing event LEC.11: data frames over ATM Forum LEC: interface 1
Tracing event LEC.12: control frames over ATM Forum LEC: interface 1
Note that if the user DISABLEs and TESTs this LEC interface,
the LEC trace settings from Talk 6 Config will take effect.

MAC Address packet filtering can be enabled under the LEC net
using the 'trace mac-address' command.
```

Trace-Status

Use the **trace-status** command to get updated information regarding packet trace.

Syntax:

trace-status

Example:

```
trace-status
------------------------- Configuration -----------------------------
Trace Status:OFF  Wrap Mode:OFF  Decode Packets:OFF
RAM Trace Buffer Size:0  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: None

------------------------ Run-time Status ----------------------------
Packets in RAM Trace Buffer:0   Free Trace Buffer Memory:0
Trace Errors:0  First Packet:0  Last Packet:0
Trace Records Stored on HD:0  Trace Buffer File Size:0

Has Stop Trace Event Occurred? NO
```

View

Use the **view** command to enter the View Captured Packet Trace Buffers Monitoring.

For an explanation of the **view** commands, see “View” on page 193.

Syntax:

view	current
	first
	jump
	last

next

prev

search

exit

ELS Message Buffering Monitoring Commands

Table 20 describes the commands available at the `ELS Config Advanced>` prompt.

Table 20. ELS Message Buffering Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Flush	Clears the message buffer and turns off logging to the message buffer.
List	Displays the operational settings for message buffering.
Log	Enables logging of selected messages to the message buffer.
Nolog	Turns off logging of selected messages to the message buffer.
Set	Sets the size of the message buffer, the wrapping mode, whether logging occurs, which event will end message buffering, and what the system does when message buffering is stopped by an event.
Tftp	Sends the ELS message buffer to a file at a remote host.
View	Displays all or a specific number of messages in the message buffer. You can also control how the messages scroll off the screen.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Flush

Use the **flush** command to set logging off, clear the messages from the buffer, and release the buffer memory for other use by the system.

Syntax:

flush buffer

List

Use the **list** command to list the ELS message buffering configuration.

Syntax:

list status

Example:

```
ELS Advanced> list status
------------------------------------Configuration--------------------------------
Logging Status:    OFF       Wrap Mode:   ON    Logging Buffer Size:    8500 Kytes
Stop-Event:    APPN.2          Stop-String:     netdn for  intf 6
Additional Stop-Action:  APPN DUMP
-----------------------------------Run-Time Status------------------------------
Has Stop Condition Occurred ?     YES       Messages currently in buffer:         1222
```

See “Set” on page 198 for a description of the commands that change the values in the display.

Log

Use the **log** command to select which messages will be logged to the message buffer.

Syntax:

log	event
	group
	range
	subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be logged to the message buffer.

Nolog

Use the **nolog** command to remove messages from the defined list of messages that are logged to the message buffer.

Syntax:

nolog	event
	group
	range
	subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) not to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group not to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem not to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 not to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem not to be logged to the message buffer.

Set

Use the **set** command to change configured ELS message buffering options.

Syntax:

set	logging [on or off]
	stop action . . .
	stop event *subsystem.event#*
	stop string *text*
	wrap [on or off]

logging [on or **off]**
Specifies whether message buffering will occur. This command will not take affect until you allocate a buffer using the **set buffer-size** command. The default is off.

stop action [appn-dump or **disk-offload**or **none** or **system-dump]**
Specifies the additional action the system takes when the “stop event” (and if specified, the “stop string”) occurs. The actions are:

appn-dump
Dumps the APPN protocol, if it is active. The APPN dump will indicate that the dump was taken as the result of a stop action.

disk-offload
Writes a formatted version of the buffer to a file on the hard drive . If the file already exists, the new file replaces it. You can then use the **tftp file** monitoring command to send the file to a remote host.

none No other action is taken after logging stops.

system-dump
Dumps the entire system. The system dump will indicate that the dump was taken as the result of a stop action.

Default value: none

stop event [*subsystem.event#* or **none]**

Specifies the event (*subsystem.event#*) that stops logging. If you have specified a stop string, the text in the stop string must also match. When the stop event occurs:

1. The next five ELS messages are logged.
2. Logging stops.
3. The system performs the specified "stop action."

Logging remains stopped until the next time you issue the **set logging on** command or the router reboots.

If you do not specify the stop event when you enter the command, the system prompts you to enter the stop event. Specifying **none** disables the stop event function.

Default value: none

stop string *text* or **none**

Specifies the string to be used in conjunction with the "stop event" to stop logging. If you have not specified a stop event, the system ignores the "stop string."

Text can be any ASCII string up to 32 characters in length. If you do not specify *text* when you enter the command, the system will prompt you for the string. Entering **none** clears the "stop string."

Default value: none

wrap [on or **off]**

Specifies whether to stop the log when the buffer is full (off) or to log the new messages at the beginning of the buffer (on).

Default value: off

Tftp

Use the **tftp** command to send the ELS message buffer to a remote host as a formatted file.

Syntax:

tftp	buffer [formatted] *dest_ip_address dest_filename*

buffer [formatted] *dest_ip_address dest_filename*

Specifies that the ELS message buffer is to be sent to the remote host indicated by *dest_ip_address* as file *dest_filename.* The buffer can be either formatted.

View

Use the **view** command to view all of the messages or a specific number of messages in the message buffer.

Syntax:

view	all [scroll/noscroll]
	last [scroll/noscroll *number*]

all *scroll/noscroll*

Displays all of the messages in the message buffer.

[scroll]
Specifies that the screen pauses until you hit the spacebar.

Note: If you are displaying a large number of messages, specify scroll so you do not miss any critical messages.

noscroll
Specifies that the messages will scroll off the screen if the number of messages exceeds the screen length.

last *scroll/noscroll number*
Display the last *number* messages in the message buffer.

[scroll]
Specifies that the screen pauses after displaying a full screen of messages and waits for the user to hit the space bar to get the next screen.

Note: If you are displaying a large number of messages, specify scroll so you do not miss any critical messages.

noscroll
Specifies that the messages will continuously scroll off the screen with no scroll control until either all messages in the buffer (or the last number of messages requested) have been displayed.

number
Specify a number from 1 to the total number of messages in the message buffer. To display the total number of messages in the buffer, use the **list status** monitoring command.

Chapter 14. Configuring and Monitoring Performance

This chapter describes how to use the Performance configuration and monitor operating commands and includes the following sections:

- “Performance Overview”
- “Performance Reporting Accuracy”
- “Accessing the Performance Configuration Environment”
- “Performance Configuration Commands” on page 202
- “Accessing the Performance Monitoring Environment” on page 203
- “Performance Monitoring Commands” on page 203

Performance Overview

Configuring performance allows you to monitor your CPU load. In the idle (non-work load) state, performance reflects operations that the router continuously performs as a part of managing external interfaces. The CPU load registered in the idle state is dependent upon:

- Number of protocols running.
- Number of interfaces/cards installed.
- Type of interfaces installed.

The performance function can be used as a tool for trend analysis, bottleneck evaluation, and capacity planning. By collecting the CPU utilization information on the router, a network manager can monitor:

- CPU load versus time of day.
- CPU load versus location of the router in the network.
- CPU load versus traffic throughput.
- CPU load versus user load

Performance Reporting Accuracy

If you request a performance analysis when the MSS Family Client first comes online, you will see values that reflect an initialization state that has little or no network traffic, so it is of little use in helping to balance your network load.

It is best to use performance reports that are generated under normal loads after approximately 2 minutes of operation.

Accessing the Performance Configuration Environment

Use the following procedure to access the Performance monitor configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, see “What is CONFIG?” on page 81.) For example:

```
* talk 6
Config>
```

After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **enter** again.

2. At the CONFIG prompt, enter the **perf** command to get to the `PERF Config>` prompt.

Performance Configuration Commands

To configure Performance, enter the commands at the `PERF Config>` prompt.

Table 21. PERF Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Disable	Disables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
Enable	Enables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
List	Lists the configuration.
Set	Sets the reporting period.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Disable

Use the **disable** command to disable collection of CPU utilization statistics and disable the `talk 2` ELS monitor output.

Syntax:

disable cpu statistics

t2 output

Enable

Use the **enable** command to enable collection of CPU utilization statistics and enable the `talk 2` ELS monitor output.

Syntax:

enable cpu statistics

t2 output

List

Use the **list** command to display the performance monitor configuration.

Syntax:

list

Set

Use the **set** command to set the reporting period.

Syntax:

set *time*

time Specifies the short window time.

Valid Values: 2 - 30 seconds

Default Value: 2

Accessing the Performance Monitoring Environment

Use the following procedure to access the Performance monitoring commands. This process gives you access to the Performance *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, see “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 117.) For example:

```
* talk 5
+
```

After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **enter** again.

2. At the + prompt, enter the **perf** command to get you to the `PERF Console>` prompt.

Example:

```
+ perf
PERF Console>
```

Performance Monitoring Commands

This section describes the Performance monitoring commands.

Table 22. PERF Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Clear	Clear the CPU utilization high water statistics and resets the reporting period to a new cycle.
Disable	Disables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
Enable	Enables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
List	Lists the configuration.
Report	Displays a report of performance statistics.
Set	Sets the reporting period.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Disable

Use the **disable** command to disable collection of CPU utilization statistics and disable the `talk 2` ELS monitor output.

Syntax:

disable cpu statistics
t2 output

Enable

Use the **enable** command to enable collection of CPU utilization statistics and enable the `talk 2` ELS monitor output.

Syntax:

enable cpu statistics
t2 output

List

Use the **list** command to display the performance monitor configuration.

Syntax:

list

Report

Use the **report** command to display performance monitor statistics.

Syntax:

report

Example:

```
PERF Console>report
--------------------------------------------------------------
KEY:  SW = Short Window = 9 seconds
KEY:  LW = Long Window =  9.0 minutes  (60 x SW)

  CPU UTIL :   Most recent SW                     = 38%
               Most recent LW                     = 33%
               Highest for all SW's               = 92%
               Highest for all LW's               = 52%
               % of time cpu util (SW) was > 60%  = 16%
               % of time cpu util (SW) was > 70%  = 15%
               % of time cpu util (SW) was > 80%  = 1%
               % of time cpu util (SW) was > 90%  = 0%
               % of time cpu util (SW) was > 95%  = 0%
--------------------------------------------------------------
```

Set

Use the **set** command to set the reporting period.

Syntax:

set *time*

time Specifies the short window time.

Valid Values: 2 - 30 seconds

Default Value: 2

Chapter 15. Using LAN Network Manager (LNM)

This chapter describes IBM’s ASRT LAN Network Manager (LNM). It includes the following sections:

- “About LNM”
- “LNM Agents and Functions”
- “LNM Configuration Restrictions” on page 210
- “LNM and MSS Family Client Considerations” on page 210

About LNM

Use LNM to manage token-ring networks interconnected by source route bridges. It lets you monitor the operation of rings, bridges, and individual ring stations.

Information collected by software agents on the bridge is available to LNM management stations. More specifically, LNM agents forward collected information via another agent called the LAN Reporting Mechanism (LRM), a proprietary IBM protocol. Information forwarding is done via an LLC2 connection to a LAN Network Manager station.

LNM Agents and Functions

The LNM agents and their functions include:

- Configuration Report Server (CRS) - reports ring topology changes and ring station status to LNM.
- Ring Parameter Server (RPS) - services requests from ring stations for ring parameter information including ring number, the soft error report timer value, and the physical location.
- Ring Error Monitor (REM) - collects error reports from ring stations and analyzes them. When thresholds are exceeded, REM may forward error information to LNM.
- LAN Reporting Mechanism (LRM) - controls the establishment of reporting links from LNM stations to the bridge agents. Also manages the transfer of information to and from the other agents over these links.

Figure 34 on page 208 illustrates the connection between the IBM bridge, LNM agents, and the IBM LNM station.

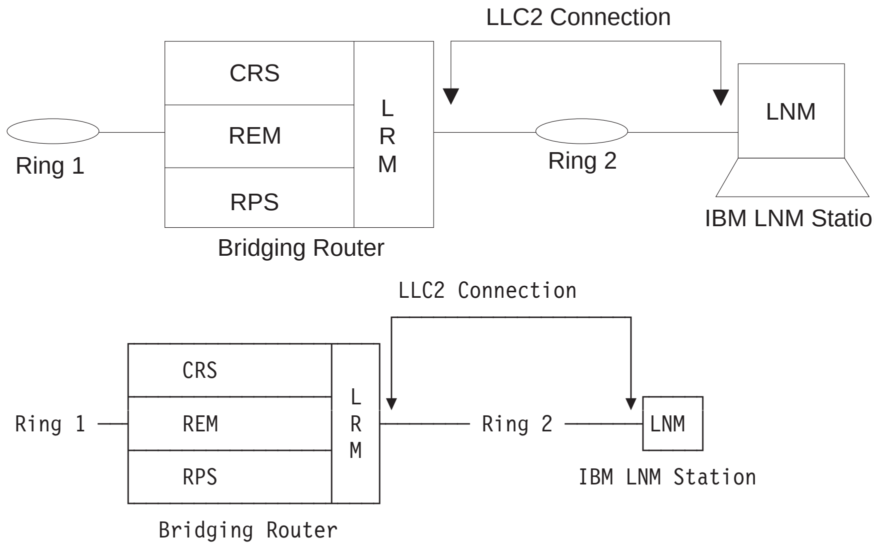


Figure 34. LNM Station and Agents

The following sections describe each LNM agent in more detail.

Configuration Report Server

At the request of LNM, CRS obtains and forwards ring station status to LNM. Use CRS to set ring station parameters and remove a station from the ring.

Configuration information generated by ring stations is forwarded to LNM. When LNM requests the status of a ring station, CRS builds and sends MAC frames to the station to obtain the information. CRS then sends the following frames to the ring station:

- Request Ring Station Address MAC frame
- Request Ring Station State MAC frame
- Request Ring Station Attachments MAC frame

When the ring station replies, CRS puts the information into a properly formatted LLC2 frame and forwards it to LNM.

CRS can also remove a ring station from the ring at the request of LNM. To remove a ring station, CRS sends a Remove Station MAC frame to the ring. CRS also returns a response to LNM indicating the success or failure of the removal.

When CRS receives a Report New Active Monitor MAC frame, it forwards the information to LNM. When a Report NAUN (Next Active Upstream Neighbor) Change MAC frame is received, this information is also reported. The CRS agent has its own functional address that ring station MAC layers can use to forward MAC frames to CRS.

Ring Parameter Server

RPS inserts ring stations onto the ring. When a ring station is newly inserted into the ring the following occurs:

- The new station sends a Request Initialization MAC frame to RPS for that ring. This MAC frame includes some information about the station.

- RPS responds with an Initialize Ring Station MAC frame containing the ring number and the interval of time to wait between sending Report Soft Error MAC frames. The information gleaned from the Request Initialization frame is passed to LNM so that it can maintain a database of all ring stations on the ring.
- RPS also responds to a request for status from LNM. The ring number, RPS version information and the soft error report timer value are returned to LNM.

The RPS function has an associated functional address for receiving the MAC frames that other ring stations send to it.

Attention: When a station attempts to insert into a ring, it sends a Request Initialization MAC frame to the Ring Parameter Server (RPS) for that ring. If this frame is copied successfully by the RPS, then the station expects to receive an Initialize Ring Station MAC frame back from the RPS. If no such frame is received, the station will not insert into the ring.

A station may fail to insert into the ring if the device is configured for LNM, becomes the Ring Parameter Server, and enters a congested state that prevents the sending of the Initialize Ring Station MAC frame. The solution to this problem is to disable RPS on the affected port. If RPS is not enabled and no server copies the Request Initialization frame, the sending station does not expect a response and it will insert into the ring.

Ring Error Monitor

REM observes the operation of the attached token-ring by looking for hard errors and soft errors. It then reports these to the LRM and aids in isolating the cause of the errors. It does the following during hard error detection:

- Hard errors are detected on the ring by the receipt of Beacon MAC frames.
- Stations in the fault domain attempt to correct the problem by possibly removing themselves from the ring.
- REM determines if the hard error condition is corrected or not and then reports the results to LNM.

REM monitors soft errors as follows:

- Soft Error MAC frames are sent periodically by ring stations to REM to inform it of the number of times various intermittent faults, for example, CRC errors and frequency errors, occur.
- When the number of soft errors for a station exceeds a certain threshold, REM reports this condition to LNM.
- REM also monitors the Report Soft Error MAC frames for receiver congestion conditions. Receiver congestion indicates that a ring station discarded frames due to a shortage of receive buffers.
- If the number of times a station reports receiver congestion exceeds a certain threshold, REM reports this condition to LNM. When the receiver congestion condition returns to normal, LNM is notified that the receiver congestion condition has ended.

LAN Reporting Mechanism

LRM controls the connection of LNM to the agents. LRM establishes reporting links between itself and each connected LNM. A *reporting link* is an LLC2 connection between LNM and LRM.

All communication between LNM and the agents is done via a reporting link. LRM passes management data to and from the appropriate agents to the reporting links. Up to four reporting links are supported. One is designated the *controlling link* and the other three are designated as *observing links*.

An LNM connected via the controlling link can perform all available operations. LNMs connected by observing links can perform only a limited subset of the available operations.

LNM Configuration Restrictions

The LNM agent and the LNM station always assume that messages are being passed on a two-party model. LNM is enabled, however, on a per-bridge port basis to be consistent with the existing configuration.

To obtain the MAC addresses needed to configure the LNM Manager, enter **`list lnm ports`** at the `ASRT>` prompt.

The LAN Bridge Server (LBS) can report packets-forwarded and packets-discarded performance data statistics when requested by the manager station. Remote configuration updates from the manager station are not supported.

Logical Link Class 2 Support

In LANs, the data link layer comprises two sublayers: the medium access control (MAC) and the link layer control (LLC). LLC provides two types of service:

- LLC1 (Type 1) - an unacknowledged connectionless service
- LLC2 (Type 2) - a set of connection-oriented service

LAN Network Manager (LNM) requires LLC2 connection-oriented services. LLC2 provides capabilities for:

- Initiating new data link connections
- Managing data link connections
- Exchanging data in sequential order (in a guaranteed fashion)
- Executing a level of flow control on the established connections
- Terminating link connections upon request from the service user or unrecoverable link errors.

The LLC sublayer conforms to the IEEE 802.5 standard.

LNM and MSS Family Client Considerations

When configuring LNM with the MSS Family Client, you must remember the following:

1. Only one physical port on the LAN Switch can be in a domain that LNM manages.

2. Any configuration of domains/ports on the LAN Switch that affect ports managed by LNM requires you to reset the MSS Family Client.
3. LNM displays each MSS Family Client as a series of two port-bridges connected to a virtual ring segment. The virtual ring segment will not be used during the actual forwarding of frames, but will only be used to represent the MSS Family Clients to LNM.
4. The MAC addresses that you configure for the bridge ports in the MSS Family Clients are virtual MAC addresses. These addresses are used by the various bridging functions in the MSS Family Clients as if they have a physical presence on the ring segments. These MAC addresses will appear to LNM as real physical ports on the rings, but the MSS Family Client do not have a unique physical presence on the ring segment. When viewing the ring segments, you should assume that the physical configuration of the ring segments are as if those bridge MAC addresses do not exist.

Chapter 16. Configuring and Monitoring LAN Network Manager (LNM)

This chapter describes IBM’s ASRT implementation of the LAN Network Manager (LNM). It includes the following sections:

- “Configuring LNM”
- “LNM Commands” on page 214

Configuring LNM

This section summarizes the procedure for basic configuration of the LNM feature on your bridging router.

1. Obtain the MAC address required for network manager software.

   Enter the **list lnm ports** command at the `ASRT>` prompt to obtain the MAC addresses required by the Network Manager software running on the Network Manager Station. For example:

   ```
   MSS Client ASRT>list lnm ports
   Port 2
   LNM Agents Enabled: RPS CRS REM
   Reporting Link          State          LNM Station Address
         0                 ACTIVE         10:00:5A:25:0B:CA
         1                 AVAILABLE
         2                 AVAILABLE
         3                 AVAILABLE
   MAC Addresses to use when configuring LNM Manager:
         00:04:AC:C4:07:20
         40:04:BC:C4:07:20
   LNM not enabled on port 3
   Port 4
   LNM Agents Enabled: RPS CRS REM
   Reporting Link          State          LNM Station Address
         0                 ACTIVE         10:00:5A:25:0B:CA
         1                 AVAILABLE
         2                 AVAILABLE
         3                 AVAILABLE
   MAC Addresses to use when configuring LNM Manager:
         00:04:AC:C4:07:22
         40:04:BC:C4:07:22
   LNM not enabled on port 5
   ```

   The MAC addresses displayed (shown in bold in the example) are used by the Network Manager to configure it to the LNM agents present in the router.

   Note: These addresses must be entered exactly as they appear in the output, otherwise LNM will not configure correctly.

2. Enable the LNM agents on the router. Type **`enable lnm`** at the `LNM config>` prompt to enable the LNM agents on the desired port of your bridging router. For example:

   ```
     LNM config>enable lnm
     Port Number [1]? 1
   ```

   The default setting has all LNM agents enabled.

3. Check the configuration by displaying enabled LNM agents. Type **`list port`** at the `LNM config>` prompt to display which LNM agents are enabled on your configured port. For example:

   ```
     LNM config>list port
     Port Number [1]? 1
     LNM Agents Enabled: RPS CRS REM
   ```

LNM Commands

This section describes the LNM configuration and monitoring commands. These commands allow you to configure and monitor network parameters for the LNM.

Enter configuration commands at the `LNM config>` prompt. Access this prompt as follows:

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>lnm
LNM configuration
LNM config>
```

Enter monitoring commands at the `LNM>` prompt. Display this prompt as follows:

```
+protocol asrt
ASRT>lnm
LNM>
```

Table 23 lists the LNM commands.

Table 23. LNM Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Disable	Disables all LNM agents on a specified port or specified LNM agents (RPS, CRS, or REM) on a specified port. Disables the setting of certain LNM parameters from the remote LNM application linked to the bridge. Applies globally to all instances of LNM within the bridge. This command is used for configuration only.
Enable	Enables all LNM agents on a specified port or specified LNM agents (RPS, CRS, or REM) on a specified port. Enables the setting of certain LNM parameters from the remote LNM application linked to the bridge. Applies globally to all instances of LNM within the bridge. This command is used for configuration only.
List	Displays the LNM agents that have been enabled for the specified port. Displays the passwords configured for the bridge. This command is used for both configuration and monitoring.
Set	Sets the password for the specified reporting link number. This command is used for configuration only.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Disable

Use the **disable** command to disable all LNM agents (RPS, CRS, or REM) on a specified port.

This command also disables the setting of the reporting link passwords from the remote LNM application linked to the bridge.

Syntax:

disable *agent port#*

lnm . . .

configuration-remote-change

agent *port#*

Disables the specified LNM agent (RPS, CRS, or REM) on the specified port. If the port is not configured then the message `LNM not configured for port XX` is displayed, and the command has no effect.

Example:

```
disable REM 1
```

lnm Disables LNM on the specified port. If the port is not configured for LNM, the message `LNM not configured for port XX` is displayed, and the command has no effect.

Example:

```
disable lnm

Port number [1]? 1
LNM not configured for Port 1
```

configuration-remote-change

Disables the setting of the reporting link passwords from the remote LNM application linked to the bridge. This command applies globally to all instances of LNM within the bridge.

Example:

```
disable configuration-remote-change

CONFIGURATION-REMOTE-CHANGE: disabled
```

Enable

Enables all LNM agents on a specified port or enables specified LNM agents (CRS, REM, or RPS) on a specified port.

If the interface is not a token-ring then the message `Port number XX is not token-ring` is displayed and the command has no effect.

If the port is not configured, then the message `Port number XX does not exist` is displayed and the command has no effect.

If the specified agent is already enabled for the specified port the message `Already enabled` is displayed.

This command also enables the setting of the reporting link passwords from the remote LNM application linked to the bridge.

Syntax:

enable *agent port#*

lnm . . .

configuration-remote-change

agent *port#*

Enables the specified LNM agent (RPS, CRS, or REM) on the specified port.

Example:

```
enable CRS 1
```

lnm *port#*

Enables all LNM agents on the specified port.

Example:

```
enable lnm

Port Number [1]? 1
```

configuration-remote-change

Enables the setting of the reporting link passwords from the remote LNM application linked to the bridge. The default setting disables the setting of LNM configuration parameters remotely.

This command applies globally to all instances of LNM within the bridge.

Example:

```
enable configuration-remote-change

CONFIGURATION-REMOTE-CHANGE: Enabled
```

List (configuration command)

Displays the LNM agents enabled for the specified port, and also displays passwords that have been configured for the bridge. The command is entered at the ASRT> prompt.

Syntax:

list password

port . . .

password

Displays the passwords that have been configured for the reporting links of the bridge. Displays whether or not the passwords can be changed by the remote LNM application.

Example:

```
list password

Reporting Link     Password
0            87654321
1            MADRAS
2            ABC1234
3            123ABC
CONFIGURATION-REMOTE-CHANGE: Disabled
```

port *port#*

Displays the LNM agents enabled for the specified port if the port is a token-ring port supporting Source Routing Bridging.

Example:

```
list port

Port Number [1]? 1
LNM Agents Enabled: RPS CRS REM
```

List (monitoring command)

Displays information about the status of the LNM configuration. The command is entered at the ASRT> prompt.

Syntax:

list bridge

lnm ports

bridge

Displays whether LNM is enabled on a specific port.

Example:

```
list bridge
```

```
SRB Bridge ID (prio/add):  32768/00-20-C8-E2-AE-98
Bridge state:          Enabled
Bridge type:           SRB
Number of ports:       5
STP Participation:     IBM-SRB proprietary

                                                        Maximum
Port  Interface        State  MAC Address         Modes   MSDU   Segment
   2  TKR/1              Up   00-20-35-23-20-85    SR      2096  346,LE
   3  TKR/2              Up   00-20-35-23-20-45    SR      2096  403,LE
   4  TKR/3              Up   00-20-35-23-20-C5    SR      2096  404,LE
   5  TKR/4              Up   00-20-C8-E2-AE-98    SR      4518  FAB
   6  TKR/5              Up   E0-84-2E-E0-84-2E    SR      4518  423

        LE = LNM Enabled, LD = LNM Disabled, LF = LNM Failed

SR bridge number:      4
```

lnm ports

Displays information about the configuration of the LNM enabled on the bridging router.

Example:

```
list LNM ports
```

```
Port 2
LNM Agents Enabled: RPS CRS REM
Reporting Link          State          LNM Station Address
      0                 ACTIVE         10:00:5A:25:0B:CA
      1                 AVAILABLE
      2                 AVAILABLE
      3                 AVAILABLE
MAC Addresses to use when configuring LNM Manager:
      00:04:AC:C4:07:20
      40:04:BC:C4:07:20
LNM not enabled on port 3
Port 4
LNM Agents Enabled: RPS CRS REM
Reporting Link          State          LNM Station Address
      0                 ACTIVE         10:00:5A:25:0B:CA
      1                 AVAILABLE
      2                 AVAILABLE
      3                 AVAILABLE
MAC Addresses to use when configuring LNM Manager:
      00:04:AC:C4:07:22
      40:04:BC:C4:07:22
LNM not enabled on port 5
```

source-routing configuration

Displays whether LNM is enabled on a specific port.

Example:

```
list source-routing configuration
```

```
Bridge number:               4
Bridge state:                Enabled
Maximum STE hop count        14
Maximum ARE hop count        14
Virtual segment:             444  (1:N SRB Active)

Port  Segment  Interface        State     MTU    STE Forwarding   LNM
   2  346      TKR/1            Enabled   2052   Auto             ENA
   3  403      TKR/2            Enabled   2052   Auto             ENA
   4  404      TKR/3            Enabled   2052   Auto             ENA
   5  FAB      TKR/4            Enabled   4399   Auto             N/A
   6  423      TKR/5            Enabled   4399   Auto             N/A
```

Set

Sets the password for the specified reporting link number. The link number can be 0, 1, 2, or 3. Link 0 is used for the controlling link. Links 1, 2, and 3 are used for observing links.

The password must consist of six to eight characters, and must match the password used by LNM when it establishes a reporting link with the bridge. If the password is not set for a link, it defaults to the string 00000000.

Syntax:

set password *link# password*

Example: `set password`

Example:

```
set password

Link Number [0]? 1
Enter new password :  [ABCDEFGH]? guesswho
```

Part 2. ATM and LAN Emulation

Chapter 17. Overview of LAN Emulation

Note: See the glossary for definitions of the acronyms and terms used in this chapter.

The MSS Client implements the *LAN Emulation Over ATM: Version 1.0 Specification* which is widely accepted as the industry standard for multivendor multiprotocol interoperability. This chapter introduces basic LAN emulation (LE) concepts in the context of the MSS implementation. It begins by examining the motivation for installing emulated LANs (ELANs).

LAN Emulation Benefits

LAN emulation protocols allow ATM networks to provide the appearance of Ethernet and Token-Ring LANs. Although LAN emulation does not exploit all of the benefits of ATM, it is useful in migrating to ATM technology and lowering network management costs. It enables you to utilize high-speed ATM links and still protect your software and hardware investments.

Software investments are protected because application interfaces are unchanged (LAN emulation is implemented within the data link control layer, which is below the device driver interface of end stations). Hardware investments are protected with forwarding engines that bridge LAN and ATM networks so that existing adapters and wiring can continue to be used.

LAN emulation allows incremental installation of ATM adapters in stations with high-bandwidth requirements, for example, servers and engineering or multimedia workstations. Physical and logical views of a simple LAN emulation example are illustrated in 35.

Simple LAN Emulation Network

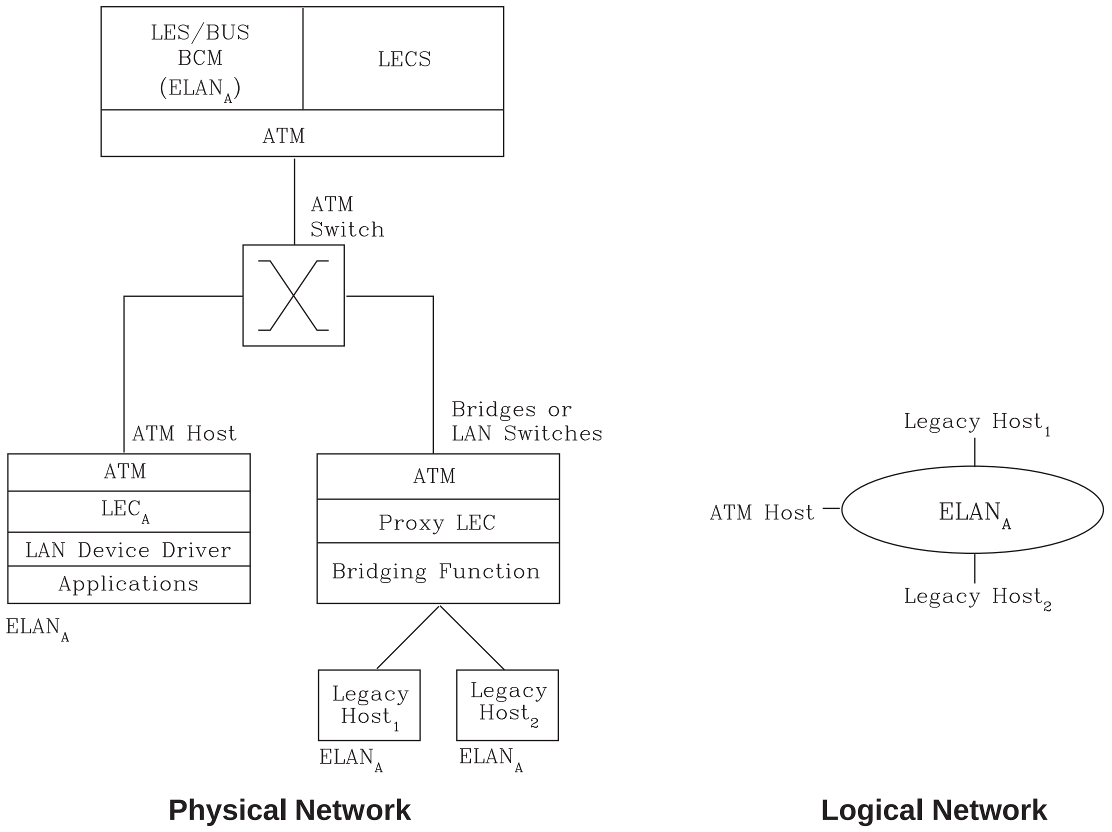


Figure 35. Physical and Logical Views of a Simple LAN Emulation Network

The network management benefits of emulated LANs (ELANs) come from increased flexibility in handling moves, adds, and changes. Membership in an ELAN is not based on physical location; instead, logically-related stations are grouped to form an ELAN (stations can also be members of multiple ELANs).

As long as ELAN memberships are retained, no reconfiguration is needed when stations move to new physical locations. Similarly, no wiring modifications are needed to move stations from one ELAN to another.

LAN Emulation Components

The following components implement an ELAN:

LAN emulation (LE) clients (LECs)
LAN emulation components that represent users of the Emulated LAN.

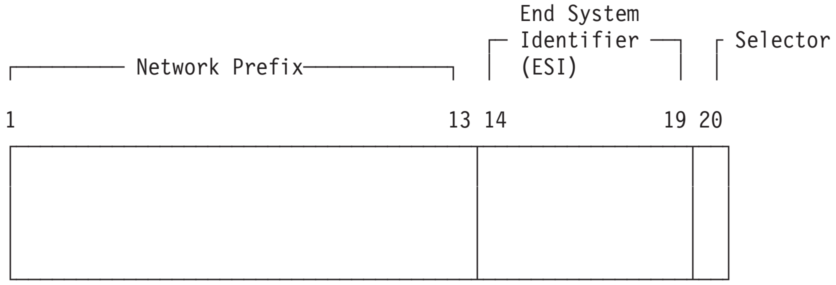
LE configuration server (LECS)
A LAN emulation service component that centralizes and disseminates configuration data.

Broadcast and Unknown Server (BUS)
A LAN emulation service component responsible for the delivery of multicast and unknown unicast frames.

The function that bridges between Token-Ring or Ethernet LAN segments and ELANs is called a Proxy LEC. To emulate a LAN, LE clients request services from the LECS. The following sections briefly review ATM addressing and pertinent Interim Local Management Interface (ILMI) functions. You need to understand these concepts before you can understand how the LE components function in the network.

Addressing in ATM

ATM uses 20-byte hierarchical addressing:



The first 13 octets of an ATM address are the Network Prefix. Each switch in your ATM network must have a unique Network Prefix. ATM switches use the Network Prefix to route VCC setup requests the destination ATM switch. End systems, like this router, retrieve their Network Prefix from their ATM switch when they activate.

Octets 14–19 of an ATM address are the End System Identifier (ESI). Each end system attached to the same switch must use a disjoint set of ESIs. When an end system activates, it attempts to register its ESIs with its ATM switch using the Interim Local Management Interface (ILMI).

The ILMI defines a set of SNMP-based procedures used to manage the interface between an end system and an ATM switch. End systems use ILMI to:

- Obtain the network prefix from the switch
- Register their ESIs with the switch
- Dynamically determine the UNI version of the ATM switch
- LECs may get a list of LECS addresses from the switch

The switch forces all of its registered ESIs to be unique.

Octet 20 of an ATM address is the selector.

End stations obtain their Network Prefix from the switch and form their own addresses by appending an ESI and selector. These addresses must then be registered with the switch, which rejects the registration if the ATM address is not unique.

ESI

Each ATM interface on the router has a universally administered, or burned-in, MAC address. You can use the MAC address as an ESI for some or all of the router’s ATM addresses. Alternatively, you can define up to 64 locally administered ESIs on each interface. If every end system uses its universally administered MAC address as its ESI, then ATM addresses are guaranteed to be unique. This eases the configuration burden. However, using locally administered ESIs can ease problem determination. You can use any combination of universal or locally administered ESIs.

One way to obtain a unique ATM address is to use a burned-in IEEE MAC address as the ESI and to locally choose a unique selector. By default, the router uses the MAC address of the ATM interface as the ESI in its ATM addresses. Additional ESIs can be configured on each ATM interface.

Each ESI can have up to 255 associated selectors (0x00 through 0xff). The range of selectors is partitioned into two subranges, a configured selector range and an automatically assigned selector range. The ATM interface parameter max-configured-selector gives the upper bound on the configured selector range.

The ATM components on the router have various ways of choosing a selector. Some components require you to explicitly configure a selector from the configured selector range. Other components, such as Classical IP clients, allow the selector to be automatically assigned at run-time. You do not have to choose the selector because the router does this when it activates. This selector is not guaranteed to be consistent across router restarts. Automatic selector assignment is useful only for those ATM components whose ATM address does not have to be already known by other network devices.

You must configure ATM before you configure emulated LANs, bridging or routing.

Key Configuration Parameters for LAN Emulation

This section briefly describes the required configuration parameters of the MSS Family Client LEC. The ATM interface for the LEC must be defined before the components can be created.

To create an LE client, you only need to specify the ELAN type. If you define two LE clients on a single ATM interface and bridge them together, then one of the LE clients must use a non-default MAC address. By default, LE clients use the burned-in MAC address of the ATM interface. The default maximum frame size is 1516 bytes for Ethernet LE clients and 4544 bytes for token-ring LE clients.

Chapter 18. Using ATM

This chapter describes how to use the ATM interface. It includes the following sections:

- “ATM and LAN Emulation”
- “How to Enter Addresses”
- “ATM-LLC Multiplexing” on page 226
- “ATM Virtual Interface Concepts” on page 226

ATM and LAN Emulation

LAN emulation provides support for virtual Token-Ring and Ethernet LANs over an ATM network. Refer to “How to Enter Addresses” for a discussion of ATM addressing.

How to Enter Addresses

Enter addresses in two ways, depending upon whether the address represents (1) an IP address, or (2) an ATM address, MAC address, or route descriptor, as follows:

1. IP address

   Enter IP addresses in dotted decimal format, a 4-byte field represented by four decimal numbers (0 to 255) separated by periods (.).

   Example of IP Address:

   ```
   01.255.01.00
   ```

2. ATM or MAC address or route descriptor

   Enter ATM addresses, MAC addresses, and route descriptors as strings of hexadecimal characters with or without optional separator characters between bytes. Valid separator characters are dashes (-), periods (.), or colons (:).

   Examples of ATM address, MAC address or route descriptor

   ```
   A1FF01020304
       or
   A1-FF-01-02-03-04
       or
   A1.FF.01.02.03.04
       or
   39.84.0F.00.00.00.00.00.00.00.00.00.03.10.00.5A.00.DE.AD.08
       or
   A1:FF:01:02:03:04
       or even
   A1-FF.01:0203:04
   ```

   Each type of address requires a different number of hexadecimal characters:

ATM	40
MAC	12
ESI	12
Route descriptor	4

This information applies to addresses entered for ATM, LAN emulation, Classical IP and ARP over ATM, IPX over ATM, and ARP over ATM.

ATM-LLC Multiplexing

Protocols that run natively over an ATM interface can use ATM-LLC multiplexing to share ATM addresses and both SVC and PVC channels between users. ATM-LLC is implicitly configured when the protocols are configured and can be monitored using the `ATM Config+` command prompt from **t 5**. There are no explicit configuration options for the ATM-LLC multiplexing function. For example, if two protocols which use ATM-LLC multiplexing are configured to use the same local ATM address (local endpoint), this implicitly configures ATM-LLC to use the same shared ATM address for both protocols.

See “ATM-LLC Monitoring Commands” on page 242 for additional information.

Sharing of ATM addresses or SVC/PVC channels is not possible between protocols that use the ATM-LLC multiplexing function and those that do not use the ATM-LLC multiplexing function (such as Classical IP). Currently, Server Cache Synchronization Protocol (SCSP) and APPN are the only two protocols that use the ATM-LLC multiplexing function.

ATM Virtual Interface Concepts

An ATM Virtual Interface (AVI) creates the appearance of multiple ATM interfaces when, in fact, there is only one physical ATM interface. One or more AVIs can be configured for each physical ATM interface on the router. AVIs have the following characteristics:

- Each AVI must be defined on one (and only one) physical ATM interface. ATM real interface (ARI) will be used to mean a physical ATM interface.
- One or more AVIs can be configured on each ARI on a router.
- Higher layer protocols treat ARIs and AVIs equally. The protocols see the total number of ATM interfaces as the sum of the number of ARIs and AVIs configured on the router.
- Protocols can be configured on each ATM interface (real or virtual) independently of other interfaces.

  For example, one can configure IP on interface 0 (which is a real ATM interface) with IP address 9.1.1.1 and another instance of IP with address 9.2.1.1 on interface 1 (which is an AVI). Whether an interface is a real ATM interface or a virtual interface configured on a real interface makes no difference to the protocol (IP in the example). In addition, whether virtual interface 1 is configured on top of real ATM interface 0 or some other physical ATM interface is also transparent to the protocols.

Advantages of Using ATM Virtual Interfaces

Major advantages of using the ATM Virtual Interfaces are:

- Using the ATM Virtual Interface feature increases the number of protocol instances that can be supported on a physical ATM interface.

  The actual number of AVIs that can be configured on an ARI is limited by physical resources, such as memory, available on the router. The total number of interfaces that can be created depends on the data packet size for the interfaces and is limited to a maximum number of 253 per router.

The use of AVIs significantly improves the configuration options for protocols such as IPX that are limited to one instance or address per ATM interface. By configuring an appropriate number of AVIs, several IPX addresses can be supported on each physical ATM interface.

- The ATM Virtual Interface feature is crucial for supporting multicast routing protocols (such as MOSPF) over ATM networks.

  In order for multicast to operate correctly, each logical subnet ***must*** be configured on a different interface because multicast routing protocols typically function in such a way that a packet coming in from a router interface will never be sent out over the same interface. Thus, if more than one subnet is configured on an interface and a source in one subnet sends a multicast packet to a member in another subnet defined on the same interface, this member will never receive the packet.

  By creating an individual virtual interface for each subnet, packet multicasting can be performed successfully. Typically, the number of ATM interfaces on a router will be limited, in turn limiting the number of subnets that can be correctly configured for multicast operation. However, by creating as many AVIs as needed (according to the number of subnets that are required to be configured on the router), the number of physical ATM interfaces will no longer limit the number of subnets that can be configured on a router for correct multicast operation.

  For example, the “one-armed” router cannot support multicast traffic over interfaces other than ELANs without the AVI feature, because incoming packets will never be sent out the same interface and will be discarded instead.

- Creating multiple AVIs on an ARI and configuring each different protocol instance (for example, each IP subnet) on a different AVI on the same ARI, can improve performance.

  For example, when multiple subnets are configured on a single physical ATM interface, the interface will have to reduce the maximum transmission unit or MTU (the maximum packet size that can be sent or received over that interface) to the smallest MTU of all subnets sharing the same interface. However, if multiple AVIs are created on that ARI and each IP subnet is configured on a different AVI, every subnet can continue to use its existing MTU size without consideration of other subnets configured on the same physical ATM interface. This avoids possible reduction in throughput and delays due to packet fragmentation and reassembly caused by MTU size reduction.

  Another performance improvement can be achieved by distributing the number of protocol addresses configured on a physical interface over different virtual interfaces configured on the same physical interface. The per-interface protocol lists get shortened, resulting in faster searches and reduced processing time.

Disadvantages of using ATM Virtual Interfaces

The disadvantages of using ATM Virtual Interfaces are:

- Because AVIs do not have any physical resources of their own, each virtual interface may have fewer Virtual Connections (VCs) than a single physical interface. The available resources (in this example VCs) are partitioned among the different virtual interfaces configured on a single ARI and the ARI itself.

  In the current implementation, resource allocation is *on demand*. Each physical ATM interface has a pool of resources that are available for use by all AVIs and the single ARI itself.

ATM Virtual Interface Configuration Concepts

Note: Because all resources are shared among the ARI and all its AVIs, an ESI added on an ARI is automatically available to all AVIs configured on the ARI. You should not assign the same ESI and selector combination to two different protocol clients using the same ARI even though they are configured on different AVIs.

Limited PVC sharing is allowed across the ARI and the AVIs configured on the ARI. PVC sharing is limited to different protocol instances. Multiple instances of the same protocol are not allowed to share the same PVC.

Chapter 19. Configuring and Monitoring ATM

This chapter describe the ATM interface configuration and operational commands. It includes the following sections:

- “Accessing the ATM Interface Configuration Process”
- “ATM Configuration Commands” on page 230
- “ATM Interface Configuration Commands” on page 230
- “ATM Virtual Interface Configuration Commands” on page 237
- “ATM Virtual Interface Monitoring Commands” on page 243
- “Accessing the ATM Monitoring Process” on page 238
- “ATM Monitoring Commands” on page 238
- “ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)” on page 239
- “ATM-LLC Monitoring Commands” on page 242

Accessing the ATM Interface Configuration Process

Use the following procedure to access the configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to “What is the OPCON Process?” on page 69.) For example:

   ```
   * talk 6
     Config>
   ```

   The CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the router is currently configured.

3. Record the interface numbers. If ATM is not specified as an interface, then create an ATM interface by using the **add device** command at the Config> prompt.

   If ATM is not specified as an interface, enter the **add device atm** command.

   ```
   Config> add dev atm
   Device Slot #(1-1) [1]?
   Adding CHARM ATM Adapter device in slot 1 port 1 as interface 1
   Use "net 1" to configure ATM parameters
   ```

4. Enter the **network** command and the number of the ATM interface you want to configure. For example:

   ```
   Config> network 1
   ATM Config>
   ```

   The ATM configuration prompt (`ATM Config>`), is displayed.

ATM Configuration Commands

This section summarizes the ATM configuration commands. Enter the commands at the `ATM config>` prompt.

Table 24. ATM Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
INTERFACE	Displays the `ATM Interface Config>` prompt from which you can list, change, or configure the ATM Interface. • Add an ESI. • List the current configuration or list ESIs. • Remove an ESI. • Set parameters of the ATM network. • Enable or disable an ESI. • Exit
LE-CLIENT	Displays the `LE Client Config>` prompt from which you can list, change, or configure the LAN Emulation Client Interface as described in “Chapter 20. Using LAN Emulation Clients” on page 245. • Add a LAN Emulation Client (LEC) for a token-ring or Ethernet emulated LAN. • Configure a LEC by network #. This command displays the `LE Config>` prompt, from which you can configure a specific LAN Emulation Client (LEC). • List LAN Emulation Clients (LECs). • Remove a LAN Emulation Client (LEC).
VIRTUAL ATM	Displays the `ATM Virtual Interface Config>` prompt from which you can list, add, or remove the ATM Virtual Interface as described in “ATM Virtual Interface Configuration Commands” on page 237
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

ATM Interface Configuration Commands

This section summarizes and then explains the commands for configuring a specific ATM interface.

Enter the commands at the `ATM INTERFACE>` prompt.

Table 25. ATM INTERFACE Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Add	Adds an ESI.
List	Lists the current configuration or list ESIs.
Qos	Displays the `ATM I/F 0 QOS Config>` prompt from which you can configure Quality of Service as described in “QoS Configuration” on page 232.

Table 25. ATM INTERFACE Configuration Command Summary (continued)

Command	Function
Remove	Removes an ESI.
Set	Sets parameters of the ATM network.
Disable	Disables an ESI.
Enable	Enables an ESI.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 23.

Add

Use the **add** command to add an ESI to your ATM configuration.

Octets 14–19 of an ATM address are the End System Identifier (ESI). Each end system attached to the same switch must use a disjoint set of ESIs. When an end system activates, it attempts to register its ESIs with its ATM switch using ILMI. The switch forces all of its registered ESIs to be unique.

Syntax:

add esi *esi-address*

esi *esi-address*
Address of End System Identifier.

Valid Values: Any 12 hexadecimal digits

Default Value:
none

List

Use the **list** command to list the configuration of this ATM device or to list the set of configured ESIs.

Syntax:

list configuration
esi

configuration
Lists the ATM device configuration. For an explanation of the listed fields, see "Set" on page 232.

Example: `list con`

```
                       ATM Configuration

 Interface (net) number =     0
 Maximum VCC data rate Mbps   =      155
 Maximum frame size    = 9234
 Maximum number of callers =  209
 Maximum number of calls =  1024
 Maximum number of parties to a multipoint call =  512
 Maximum number of Selectors that can be configured  =  200
 UNI Version = UNI 3.0
 Packet trace = OFF
```

esi Lists the ESIs in the ATM configuration.

Example: `list esi`

```
 ATM INTERFACE> list esi


          ESI                 Enabled
```

```
                        -----------------------    -------
                        000000000009                  YES
                        000000000100                  YES
```

QoS Configuration

Use the **qos-configuration** command to display the `ATM I/F 0 QOS Config>` prompt from which you can configure Quality of Service as described in “QoS Configuration”.

Syntax:

qos-configuration

Remove

Use the **remove** command to remove an ESI from your ATM configuration. All ATM components using this ESI should be reconfigured to use a different ESI. An ATM component that attempts to use a removed ESI may not activate on the next router restart.

Syntax:

remove esi *esi-address*

esi *esi-address*
Address of End System Identifier.

Valid Values: Any 12 hexadecimal digits

Default Value:
none

Set

Use the **set** command to specify ATM network parameters.

Syntax:

set
max-data-rate
max-frame
max-config-selectors
max-calls
max-callers
max-mp-parties
trace
uni-version
network-id

max-data-rate *speed*
Sets the default and upper bound for VCC traffic parameters of most LANE and CIP connections. For example, this is the default PCR for best-effort VCCs initiated by LE Clients. Signaled SCRs and PCRs cannot exceed this

limit. The default value should be satisfactory in most situations. An example of a situation where it is beneficial to change this value would be if the majority of the stations use 25–Mbps adapters. In this case, it may be desirable to limit the data rate on VCCs to 25 Mbps so that the lower speed stations are not overwhelmed with frames from the router. The units for this parameter are Mbps.

Valid Values:

25

100

155

Default Value:
155

Example:

```
ATM INTERFACE> set speed 155
```

max-calls

Sets the maximum number of switched virtual circuits (SVCs) that can exist on this ATM device. Every point-to-point and point-to-multipoint SVC uses system resources. This parameter helps limit the system resources reserved for signaling and switched connections. Increasing this parameter will allow more simultaneous SVCs. However, more system memory will be required to manage these connections.

Valid Values:
An integer in the range 64 - 10500

Default Value:
1024

Example:

```
ATM INTERFACE> set max-calls 500
```

max-callers

Sets the maximum number of entities on the router that use the ATM interface. Each LEC, Classical IP Client, and 1483 bridge interface qualifies as a user of the ATM interface. Increasing this parameter allows more users of the interface and uses more system memory.

Valid Values:
An integer in the range 64 – 1024

Default Value:
209

Example:

```
ATM INTERFACE> set max-callers 25
```

max-config-selectors

Sets the maximum number of selectors under your specific control.

The selector is used to distinguish different users on the same end system. VCC setup requests are routed in the following hierarchical fashion: ATM switches route to the destination ATM switch using the Network Prefix, the destination ATM switch routes to the destination end system using the ESI, and the end system notifies the destination user based on the selector.

Each ESI can have up to 255 associated selectors (0x00 through 0xff). The range of selectors is partitioned into two subranges, a configured selector range and an automatically assigned selector range. The ATM interface parameter max-configured-selector gives the upper bound on the configured selector range.

The ATM components on the router have various ways of choosing a selector. Some components require you to explicitly configure a selector from the configured selector range. Other components, such as Classical IP clients, allow the selector to be automatically assigned at run-time. You do not have to choose the selector because the router does this when it activates. This selector is not guaranteed to be consistent across router restarts. Automatic selector assignment is useful only for those ATM components whose ATM address does not have to be already known by other network devices.

The relative sizes of the selector range can be modified to conform to the types and numbers of ATM users on the router.

Valid Values:
0 – 255 (0x00 – 0xFF)

Default Value:
200

Note: The selector is byte 20 of a 20-byte ATM address.

Example:

```
ATM INTERFACE> set max-config-selectors 225
```

max-frame

Sets the maximum number of octets permitted in any data frame sent or received on the ATM interface. System memory is allocated based upon this parameter. Increasing the max-frame requires more system memory, but allows processing of larger frames.

All router entities using the ATM interface must use a maximum frame size less than or equal to the max-frame-size of the ATM interface. This includes all LECs, CIP clients, and 1483 bridge interfaces.

Valid Values:
An integer in the range 512 - 31000

Default Value:
9234

Example:

```
ATM INTERFACE> set max-frame 1000
```

max-mp-parties

Sets the maximum number of leaves on a point-to-multipoint connection initiated by the router. This parameter affects system memory allocation. Increasing this value is necessary if the router must set up point-to-multipoint connection(s) to a large number of destinations.

Valid Values:
An integer in the range 1 – 5000

Default Value:
512

Example:

```
ATM INTERFACE> set max-mp-parties 300
```

trace Sets the packet tracing parameters on the interface. Packet tracing can be enabled or disabled on a range of VPI/VCI values. Common VPI/VCI values to trace are:

- 0/5 for signalling packets
- 0/16 for ILMI packets.

Valid Values:
ON or OFF

Default Value:
ON

You are prompted for the VPI/VCI range you want to trace.

Beginning VPI Valid Values:
0 – 255

Default Value:
0

Ending VPI Valid Values:
0 - 255

Default Value:
255

Beginning VCI Valid Values:
0 - 65535

Default Value:
0

Ending VCI Valid Values:
0 - 65535

Default Value:
65535

Example:

```
ATM INTERFACE> set trace on
beginning of VPI range [0]? 0
end of VPI range [255]? 0
beginning of VCI range [0]? 5
end of VCI range [65535]? 5
```

uni-version

Sets the User Network Interface (UNI) version used by the ATM interface with communicating with the attached ATM switch. If the UNI versions are configured on the ATM switch and ATM device interface to a specific version (not AUTO-DETECT), the UNI versions must match.

If the UNI version is configured as AUTO, the ATM device attempts to learn the UNI version to use from the switch.

In UNI AUTO-DETECT mode, if the switch does not respond to the query for UNI version, the default is UNI 3.0. If the switch responds with a value other than UNI 3.0 or UNI 3.1, the default is UNI 3.1.

Valid Values:
[UNI 3.0|UNI 3.1|AUTO-DETECT|None]

Default Value:
UNI 3.0

Note: Must be compatible with the ATM switch.

Example:

```
ATM INTERFACE> set uni-version 3.0
```

network-id
Sets the network id of the ATM interface. Multiple ATM interfaces should have the same network id if there is ATM connectivity between the interfaces.

Valid Values:
0 - 255

Default Value:
0

Enable

Use the **enable** command to enable an ESI in the configuration of your ATM device. The ATM interface attempts to register only enabled ESIs when it activates.

Syntax:

enable esi *esi-address*

esi *esi-address*
Address of End System Identifiers.

Valid Values:
Any 12 hexadecimal digits

Default Value:
none

Example: **enable esi**

```
ATM INTERFACE> enable esi 00:00:00:00:00:09
```

Disable

Use the **disable** command to disable an ESI in the configuration. ATM components using disabled ESIs will not become active on the next router restart.

Syntax: **disable** esi *esi-address*

esi *esi-address*
Address of End System Identifiers.

Valid Values:
Any 12 hexadecimal digits

Default Value:
none

Example: **disable esi**

```
ATM INTERFACE> disable esi 00:00:00:00:00:09
```

Accessing the Virtual ATM Interface Configuration Process

From the `ATM Config>` prompt of a selected real ATM interface, use the **Virtual ATM** command to enter the Virtual ATM configuration command mode.

ATM Virtual Interface Configuration Commands

This section summarizes the ATM virtual interface configuration commands. Enter the commands at the `ATM virtual interface config>` prompt.

Table 26. ATM Virtual Interface Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Add	Adds a virtual ATM interface.
List	Lists the current configured virtual ATM interfaces.
Remove	Removes the virtual ATM interface from the current configuration.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Add

Use the **add** command to add an ATM virtual interface. A new ATM virtual interface is added to the corresponding ATM real interface (the configuration menu from which this ATM virtual interface configuration menu is accessed). The net/interface number assigned to the newly created ATM virtual interface is displayed and it is one number greater than the current largest interface number.

Syntax:

add

Example:

```
ATM Virtual Interface config> add
Added ATM Virtual Interface Net as interface 5 on physical ATM interface 0
ATM Virtual Interface config>
```

List

Use the **list** command to list configured ATM virtual interfaces defined on the current real ATM interface.

Syntax:

list

Example:

```
ATM Virtual Interface config> list

                   ATM Virtual Interface Nets
----------------------------------------------------------------------
  ATM interface number = 0
  ATM Virtual Interface Net interface number = 5

ATM Virtual Interface config>
```

Remove

Use the **remove** command to delete an ATM virtual interface. The virtual ATM interface on the real ATM interface with the specified interface number will be removed from the SRAM configuration records. If you do not specify an interface number, the last ATM virtual interface on this real ATM interface will be deleted. If you enter a question mark (?), all ATM virtual interfaces on the current real ATM interface will be listed and you can select from that list the interface you want to remove.

Syntax:

remove *n*

Example: **remove** 5

```
Virtual ATM 5 deleted successfully.
ATM Virtual Interface config>
```

Accessing the ATM Monitoring Process

Use the following procedure to access the ATM monitoring commands. This process gives you access to an ATM's *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to "What is the OPCON Process?" on page 69.) For example:

   ```
   * talk 5
   +
   ```

   The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter the console, press **Return** again.
2. Enter **interface** at the + prompt to display a list of configured interfaces.
3. Record the interface numbers.
4. Enter **network** followed by the number of the ATM interface.

   ```
     + network 1
     ATM+
   ```

   The ATM monitoring prompt (ATM+) is displayed.

ATM Monitoring Commands

This section summarizes the ATM monitoring commands for monitoring ATM interfaces. Enter the commands at the ATM+ prompt.

Table 27. ATM monitoring command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 22.
Interface	Displays the ATM Interface+ prompt from which you can monitor the ATM Interface, as described in "ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)" on page 239.
Atm-llc	Displays the ATM LLC+ prompt from which you can monitor endpoints, a set of user clients, and a set of ATM channels.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 23.

Interface

Displays the `ATM Interface+` prompt, described in “ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)”.

Syntax:

interface

ATM-LLC

Displays the `ATM-LLC+` prompt, described in “ATM-LLC Monitoring Commands” on page 242.

Syntax:

atm-llc

ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)

This section summarizes and then explains the commands for monitoring a specific ATM interface.

Enter the commands at the `ATM INTERFACE+` prompt.

Table 28. ATM INTERFACE monitoring command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Lists ATM addresses and VCCs.
Trace	Starts/Stops packet tracing on a specified VPI/VCI range. Trace can be viewed by ELS.
Wrap	Starts/Stops a loopback test on the VCC.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to list various categories of ATM data.

Syntax:

list addresses
all
circuit
vccs
reserved-bandwidth

addresses
Lists the ATM addresses, along with a descriptive name, in use on the device.

Example:

ATM Interface Monitoring Commands (Talk 5)

```
MSS Client ATM Interface+list addresses

               ATM Address                                  Name
----------------------------------------  -------------------------------------
3999999999999900009999350144444444444403  LEC 7 'poll'
39999999999999000099993501000413477519CA
39999999999999000099993501000413477519C9
3999999999999900009999350100041347751903  MPOA Client - LANE
3999999999999900009999350100041347751903  MPOA Client
39999999999999000099993501000413477519C8
```

all Lists all of the following:

- Addresses
- Circuit statistics
- VCCs
- Reserved Bandwidth

circuit Lists the statistics for a particular VCC by specifying the particular VCI-VPI pair. You can also specify the circuit on the command line; for example: list circuit 33.

Example:

```
ATM INTERFACE+ list circuit
VPI [0]?
VCI [32]?33

     Frames transmitted   =         2  Bytes transmitted   =       216
     Frames received      =         2  Bytes received      =       216
```

vccs Lists all the VCCs established by the router. The VCCs may be permanent (PVC) or switched (SVC), point-to-point or point-to-multipoint, and each is identified by a unique VPI/VCI. The trace command uses the VPI/VCI value for a VCC to perform packet tracing over a particular VCC.

Example:

```
ATM Interface+ list vccs
                      VCCs
 VPI  VCI   Hndl   Type    FrmXmt     FrmRcv     ByteXmt    ByteRcv
 --- ----- ----- ------- ---------- ---------- ---------- ----------
   0   142    17    P-MP         0          0          0          0
   0   143    19    P-MP         0          0          0          0
 Name = LEC 1 (LECID 0001) Mcast Fwd 'eth1'

   0   138    13  B0-139         1          0         62          0
 Name = LEC 1 (LECID 0001) Mcast Send 'eth1'

   0   139    16  B0-138         0          1          0         62
   0   134     9    P-MP         0          0          0          0
 Name = LES Cntrl Dist on 'eth1'

   0   135    11    P-MP         0          0          0          0
 Name = LEC 1 (LECID 0001) Cntrl Dist 'eth1'

   0   130     5     P-P         2          2        216        216
 Name = LEC 1 (LECID 0001) Cntrl Dir 'eth1'

   0   131     7     P-P         2          2        216        216
 Name = LES Cntrl Dir LECID 0001 on 'eth1'

   0     5     1    SAAL      2592       2592      27380      27036
 Name = SAAL

   0    16     2    ILMI       545        544      23646      35030
 Name = ILMI

VCC Totals: 4 point-to-point, 4 point-to-multipoint
ATM Interface+
```

P-P point to point VCC

P-MP point to multipoint VCC

ILMI Interim Local Management Interface VCC

SAAL signalling VCC

Bx-y Internally bound VCC to VPI x, VCI y

Sx-y Internally spliced VCC to VPI x, VCI y

reserved-bandwidth
Lists the reserved bandwidth on the ATM Interface.

Example:

```
ATM INTERFACE+ list reserved-bandwidth
Line Rate                    : 155000 Kbps
Peak Reserved Bandwidth      : None
Sustained Reserved Bandwidth : None
```

Trace

Use the **trace** command activate packet tracing over a specified range of VPI/VCI values. You can view trace data by using ELS as described in “View” on page 193.

Syntax:

trace list
on
off

list Displays the current packet tracing options on the ATM interface.

Example:

```
ATM Interface+ trace
on | off | list []? list
Packet trace is ON
Range of VPIs to be traced:       0 -       0
Range of VCIs to be traced:      32 -      39
```

on Starts packet tracing on all active VCCs within the specified VPI/VCI range.

Example:

```
ATM Interface+ trace on
beginning of VPI range [0]?
end of VPI range [0]?
beginning of VCI range [32]?
end of VCI range [65535]? 39
```

off Stops packet tracing on all VCCs.

Example:

```
ATM Interface+ trace off
ATM Interface+ trace list
Packet trace is OFF
```

Wrap

Use the **wrap** command to perform a loopback data test on the ATM interface of the adapter. Wrap can be issued on a per VC basis by specifying VPI-VCI pairs. Data is looped back internally.

You can selectively start a wrap, stop a wrap, or display the current wrap settings.

If you stop or display a wrap, the following statistics will be displayed:

- Wrap transmits
- Wrap receives
- Wrap transmit errors
- Wrap receive errors

- Wrap receive timeouts

For display, the current wrap statistics are displayed.

For stop, the final wrap statistics are displayed.

Syntax:

wrap display

start

stop

display
Displays the current wrap settings.

start Starts the wrap procedure and specifies the VPI-VCI length of pattern and the pattern itself.

Example:

```
ATM Interface+ wrap start
VPI [0]?
VCI [32]?
wrap pattern length [32]?
Enter 32-byte wrap pattern: [ABCDEFGHIJKLMNOPQRSTUVWXYZ123456]?
```

stop Stops the wrap procedure and displays final wrap statistics.

ATM-LLC Monitoring Commands

This section explains the commands for monitoring ATM LLC multiplexing.

Enter the commands at the `ATM-LLC+` prompt.

Table 29. ATM LLC Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Lists various options
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to list various categories of ATM LLC monitoring data.

Syntax:

list endpoints

channels

endpoints
Lists the ATM addresses in use by protocols using the ATM-LLC multiplexing function on the device. The endpoint is displayed as the End System Identifier and the Selector.

Example: `list endpoints`

```
ATM-LLC+ list endpoints
```

channels

Lists the channels in use by protocols using the ATM-LLC multiplexing function on the device.

Example: `list channels`

```
ATM-LLC+ list channels
```

ATM Virtual Interface Monitoring Commands

Monitoring the ATM virtual interface is done using the ATM LLC monitoring commands. See “ATM-LLC Monitoring Commands” on page 242 for additional information.

Chapter 20. Using LAN Emulation Clients

This chapter describes LAN Emulation Clients (LECs). It includes the following sections:

- "LAN Emulation Client Overview"

LAN Emulation Client Overview

The MSS Family Client can provide routing and bridging services for ATM Forum LAN Emulation clients. Configuration for a LEC can be:

- Ethernet (ATM Forum-Compliant)
- Token-Ring (ATM Forum-Compliant)

LECs are equivalent to "ports" or "interfaces" on traditional routers and bridges. The router bridges and routes traffic between ports by receiving and transmitting traffic through its LECs.

There are two levels to the configuration menus for LE Clients:

1. `LE Client Config>` permits you to view the set of LE Clients on a particular ATM interface, to add or remove LECs from this set, or to enter into a more detailed configuration environment for any member of this set (see LEC commands in the following). The commands for this prompt level are described in "Configuring LAN Emulation Clients" on page 247.
2. `Token-Ring Forum Compliant LEC Config>` or `Ethernet-Forum Compliant LEC Config>` permits you to configure all parameters for a particular LE Client. The commands available at this level are described in "Configuring an ATM Forum-Compliant LE Client" on page 248.

Chapter 21. Configuring and Monitoring LAN Emulation Clients

This chapter describes how to configure LAN Emulation Clients (LECs). It includes the following sections:

- “Configuring LAN Emulation Clients”
- “Configuring an ATM Forum-Compliant LE Client” on page 248
- “Accessing the LEC Monitoring Environment” on page 264
- “LEC Monitoring Commands” on page 265

Configuring LAN Emulation Clients

This section explains the commands for viewing, changing, and using the set of LE Clients on a particular ATM interface.

Enter the commands at the `LE Client Config>` prompt under the `ATM Config>` prompt, as described in “ATM Configuration Commands” on page 230.

To get to the `LE Client Config>` prompt, enter **le-c** at the ATM Config> prompt as described in “ATM Configuration Commands” on page 230.

Table 30. LAN EMULATION Client Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Add	Adds a LEC for the following types of Emulated LANs architectures: • Ethernet (ATM Forum-Compliant) • Token-Ring (ATM Forum-Compliant)
Config	Gets you to the `LEC Config>` prompt, from which you can configure a specific LAN Emulation Client as described in: • “Configuring an ATM Forum-Compliant LE Client” on page 248
List	Lists the LECs
Remove	Removes a LEC.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Add

Use the **add** command to add an ATM Forum-compliant for a Token-Ring or Ethernet emulated LAN.

Syntax:

add	ethernet
	token-ring

token-ring

Token ring ATM Forum compliant LEC.

Example:

```
LE Client Config> add token-ring
Added device as interface 3
```

ethernet

Ethernet Forum-Compliant LEC.

Example:

```
LE Client Config> add ethernet
Added device as interface 2
```

Config

Use the **config** command to get you to the `LEC Config>` prompt, from which you can configure the details of a specific LAN Emulation Client. Refer to “Configuring an ATM Forum-Compliant LE Client”.

Syntax:

config interface#

interface#

An integer number assigned by the router when the LEC was added to the configuration. Use the **list** command to determine the interface number assigned to the LEC.

Example:

```
LE Client Config> config 3
```

List

Use the **list** command to list the LAN emulation clients.

Syntax:

list

Example:

```
LE Client Config> list
                  ATM Emulated LANs
------------------------------------------------------
  ATM interface number = 0
  LEC interface number = 1
  Emulated LAN type    = Ethernet Forum Compliant
  Emulated LAN name    =
```

Remove

Use the **remove** command to remove a LEC.

Syntax:

remove interface#

interface#

You must specify the interface number that was assigned when the LEC was added to the configuration. Use the **list** command to determine the interface number assigned to the LEC.

Configuring an ATM Forum-Compliant LE Client

Use this process to access the appropriate `LEC Config>` prompt.:

1. Use the **config** command at the `LE Client Config>` prompt to access the appropriate LEC interface number, or use the **network** configuration command with the appropriate LEC interface number.
2. Commands in the following table apply to both Token-Ring and Ethernet LECs except where indicated.

This section explains the commands for configuring an ATM Forum-compliant LAN Emulation Client.

Table 31. LAN Emulation Client Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
ARP-Configuration	Allows you to configure the LE-ARP configuration for the ATM Forum-compliant client
Frame	Sets the NetWare IPX encapsulation type.
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type X’0800’) or IEEE (802.3 with SNAP). Applies only to Ethernet LECs.
List	Lists the LAN Emulation Client configuration.
LLC	Accesses the `LLC Config>` configuration prompt for Token Ring LECs.
QoS-Configuration	Gets you to the `LEC QoS Config` prompt from which you can configure Quality of Service as described in “LE Client QoS Configuration Commands” on page 283.
RIF-Timer	Sets the maximum amount of time that information in the RIF is maintained before it is refreshed. Applies only to Token-Ring LECs.
Set	Sets the LAN Emulation Client parameters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

ARP Configuration

Use the **arp-configuration** command to configure the static LE-ARP entries for the ATM forum-compliant LAN Emulation Client.

Syntax:

arp-configuration

Example:

```
Token Ring Forum Compliant LEC Config> arp-configuration
ATM LAN Emulation Clients ARP configuration
```

Table 32. ATM LAN Emulation Client ARP Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Add	Adds an LE-ARP cache entry using a MAC or route descriptor ARP.
Config	Sets cache entry QoS parameter values.
List	Lists configured ARP cache entries.
Remove	Removes an ARP cache entry.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Add

Use the **add** command to add an ARP cache entry using the MAC address or a route descriptor.

MAC addresses, and route descriptors are entered as strings of hexadecimal characters with or without optional separator characters between bytes. Valid separator characters are dashes (–), periods (.), or colons (:).

Syntax:

add mac

route-descriptor

Example 1:

```
ARP config for LEC>add mac
MAC address of LE ARP Entry []? 123456789098
ATM address in 00.00.00.00.00.00:... form []? 390f000000000000000000000000123456789098
Destination Type -  REMOTE or LOCAL [Remote]?
```

Example 2:

```
ARP config for LEC>add route 12.34
ATM address in 00.00.00.00.00.00:... form []? 390f0000000000000000000001234567890988888
ARP config for LEC>
```

Config

Use the **Config** command to configure the permanent ARP cache entry QoS parameters for the ATM forum-specific LAN Emulation Client.

Syntax:

config *arp-entry-number*

Example:

```
ARP config for LEC> config
ARP entry number [1]
Configure LEC ARP entry
```

Table 33. ATM LAN Emulation Client ARP Config Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Set	Sets QoS parameter values.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Set:

Use the **Set** command to configure the permanent ARP cache entry QoS parameters for the ATM forum-specific LAN Emulation Client.

Syntax:

set max-reserved-bandwidth

traffic-type

peak-cell-rate

sustained-cell-rate

qos-class

max-burst-size

Example:

```
ARP entry 'identifier' config> set ?
 MAX-RESERVED-BANDWIDTH
 TRAFFIC-TYPE
 PEAK-CELL-RATE
 SUSTAINED-CELL-RATE
 QOS-CLASS
 MAX-BURST-SIZE
```

See “Chapter 22. Configuring and Monitoring Quality of Service (QoS)” on page 277 for detailed information about the QoS parameters.

List

Use the **list** command to display information about ARP configuration.

Remove

Use the **remove** command to remove an configured MAC address or Route Descriptor LE-ARP entry.

Select the ARP entry number to be removed from the list provided.

Syntax:

remove *arp-entry-number*

Frame

Use the **frame** command to set the NetWare IPX encapsulation type. The command options differ depending on the type of LEC (Token-Ring or Ethernet). For Token-Ring LECs, enter one of the following:

Option	Description	Syntax
Token-Ring using MSB	Uses the standard 802.2 IPX header with the noncanonical Token-Ring address bit ordering (MSB).	frame token-ring msb
Token-Ring using LSB	Uses the 802.2 IPX header with the canonical address bit ordering (LSB).	frame token-ring lsb
Token-Ring with 802.2 SNAP using MSB	Uses the 802.2 format with a SNAP header and noncanonical address bit ordering. This encapsulation is used primarily in bridging environments.	frame token-ring_snap msb
Token-Ring with 802.2 SNAP using LSB	Uses the 802.2 format with a SNAP header and canonical address bit ordering.	frame token-ring_snap lsb
Ethernet 2.0	Uses Ethernet version 2.0 protocol 81-37.	frame ethernet_II
Ethernet 802.2	Uses Ethernet 802.3 with 802.2 SA E0.	frame ethernet_8022

Option	Description	Syntax
Ethernet 802.3	Uses Ethernet 802.3 without any 802.2 header.	frame ethernet_802.3
Ethernet SNAP	Uses 802.3, 802.2 with SNAP PID 00-00-00-81-37.	frame ethernet_SNAP

Syntax:

frame *ipx-encapsulation type*

Note: The frame command cannot be used in the network configuration process to set the IPX encapsulation unless the interface has been configured with IPX.

The IPX encapsulation can also be set in the IPX configuration environment. Refer to the Multiprotocol Switched Services (MSS) Configuring Protocols and Features chapter on Configuring IPX for details.

Example:

```
frame token_ring msb
```

IP-Encapsulation (for Ethernet ATM Forum-Compliant LEC only)

Use the **IP-encapsulation** command to select Ethernet (Ethernet type X'0800') or IEEE 802.3 (Ethernet 802.3 with SNAP). Specify either type **E**thernet or **I**EEE-802.3.

Syntax:

IP-encapsulation Ethernet
IEEE-802.3

List

Use the **list** command to list the LE client configuration.

Syntax:

list

LLC

Logical Link Control can be thought of as a “sub-protocol”. It is not accessed directly from either the Talk 6 (configuration) or the Talk 5 (console) environment. Instead, it is accessed from the Token Ring LEC configuration menu by entering an **LLC** command.

Use the **llc** command to access the `LLC Config>` prompt. See“LLC Configuration Commands” on page 263 for more information.

Syntax:

llc

| ## QoS

Use the **qos-configuration** command to get you to the `LEC QoS Config>` prompt from which you can configure Quality of Service as described in “LE Client QoS Configuration Commands” on page 283.

Syntax:

qos-configuration

RIF-Timer (for Token-Ring Forum-compliant LEC only)

Use the **RIF-Timer** command to set the maximum amount of time that information in the RIF is maintained before it is refreshed. Range is 0 to 4096. The default is 120 seconds.

Syntax:

rif-timer *value*

Example:

```
rif-timer 100
```

Set

Use the **set** command to set LE Client parameters.

Syntax:

set
arp-aging-time
arp-cache-size
arp-queue-depth
arp-response-time
auto-config
best-effort-peakrate
bus-connect-retries
conn-completion-time
control-timeout
elan-name
esi-address
flush-timeout
forward-delay
forward-disconnect-timeout
frame-size
initial-control-timeout
lecs-atm-address
les-atm-address

mac-address

multicast-send-avg

multicast-send-peak

multicast-send-type

multiplier-control-timeout

path-switch-delay

reconfig-delay-min

reconfig-delay-max

retry-count

selector

trace

unknown-count

unknown-time

vcc-timeout

arp-aging-time

Sets ARP aging time. This is the maximum time that a LEC will maintain an entry in its LE_ARP cache in the absence of a verification of that relationship. A larger aging time may result in a faster session setup time, but may also use more memory and reacts slower to changes in network configuration.

Valid Values:
An integer number of seconds in the range of 10 to 300.

Default Value:
300

Example:

```
LEC Config> set arp-aging-time 200
```

arp-cache-size

Sets the number of entries in the ARP cache. The size of the ARP cache limits the number of simultaneous data direct VCCs. Larger ARP caches require more memory, but permit the client to simultaneously converse with a larger number of destinations.

Valid Values:
An integer number in the range of 10 to 65535.

Default Value:
5000

Example:

```
LEC Config> set arp-cache-size 10
```

arp-queue-depth

Sets the maximum number of queued frames per ARP cache entry. The LEC enqueues frames when switching the data path from the Multicast Send VCC to a Data Direct VCC. Frames passed to the LEC for transmission will be discarded if the queue is full. A larger queue requires more memory, but results in fewer discarded frames during the data path switch.

Valid Values:
An integer number in the range of 0 to 10.

Default Value:
5

Example:

```
LEC Config> set arp-queue-depth 10
```

arp-response-time
Sets expected ARP response time. This value controls how frequently an unanswered LE ARP request is retried. Larger values result in fewer LE ARPs, which causes less traffic and possibly increase the amount of time before a Data Direct VCC is established.

Valid Values:
An integer number of seconds in the range of 1 to 30.

Default Value:
1 second

Example:

```
LEC Config> set arp-response-time 20
```

auto-config
Specifies whether this LEC uses LECS auto-config mode. Specify YES or NO. The LEC may contact the LECS to obtain the address of its LES and various other configuration parameters. This value must be Yes for the client to use a redundant IBM MSS Server LES.

Valid Values:
If YES, then you do not have to configure the ATM address of the LES.

If NO, then you *must* configure the ATM address of the LES using the **set les-atm-address** command as described on page 258.

Default Value:
NO

Example:

```
LEC Config> set auto-config yes
```

best-effort-peakrate
Sets the Best Effort Peak Rate. Used when establishing best effort multicast send connections.

The maximum peak rate depends on the maximum data rate of the ATM device.

Specify an integer from 1 to the maximum peak rate in Kbps (the definition is the maximum data rate) as follows:

- If ATM maximum data rate is 25 Mbps, the maximum peak rate is 25,000 Kbps.
- If ATM maximum data rate is 155 Mbps, the maximum peak rate is 155,000 Kbps.

Valid Values:
An integer number in the range of 1 - device maximum data rate.

Default Value:
155000

Example:

```
LEC Config> set best-effort-peakrate 24000
```

bus-connect-retries

This parameter sets the maximum number of times that the LEC will attempt to reconnect to the BUS before returning to the initial state.

Valid Values:
0 - 2

Default Value:
1

connection-completion-time

Sets the connection completion time. This is the time interval in which data or a READY_IND message is expected from a calling party.

When a Data Direct VCC is established to the client, the LEC expects data or a READY_IND message within this time period. The LEC will not transmit frames over a Data Direct VCC established to it until receiving data or a READY_IND. This parameter value controls the amount of time which passes before the LEC issues a READY QUERY (in hopes of receiving a READY_IND). Smaller values lead to faster response times, but also to unnecessary transmissions.

Valid Values:
An integer number of seconds in the range of 1 to 10.

Default Value:
4

Example:

```
LEC Config> set connection-completion-time 5
```

control-timeout

This parameter sets the maximum cumulative control timeout of a request.

A current timeout value is initialized to the value of ***initial-control-timeout***. If a response to a request is not received within the current timeout value, the current timeout is multiplied by the value of the ***multiplier-control-timeout*** and the request is reissued. Each time the current timeout value expires, this process is repeated until the current timeout value exceeds the value of ***control-timeout***.

Valid Values:
An integer number of seconds in the range of 10 to 300.

Default Value:
30

Example:

```
LEC Config> set control-timeout 100
```

elan-name

Specifies name of the ELAN that the LEC wishes to join. This is the ELAN name sent to the LECS in the configure request (if the LEC autoconfigures) or to the LES in the join request. The LECS or LES may return a different ELAN name in the response.

Valid Values:
Any character string length of 0 - 32 bytes.

Default Value:
Blank

Note: A blank name (0 length string) is valid.

Example:

```
LEC Config> set elan-name FUZZY
```

esi-address

Sets the ESI portion of the LEC’s ATM address.

Specify the ESI portion (octets 13 through 19) of the LEC’s ATM address. The ESI and selector combination of the LEC must be unique among all LAN emulation components on the device.

Valid Values:
Any 12 hexadecimal digits.

Default Value:
Burned-in ESI

Example:

```
set esi
Select ESI
   (1) Use burned in ESI
   (2) 11.22.33.44.55.66

Enter selection [1]?
```

flush-timeout

Sets the flush timeout. This is the time limit to wait to receive the LE_FLUSH_RESPONSE after the LE_FLUSH_REQUEST has been sent before taking recovery action. During recovery, any queued frames are dropped and a new flush request is sent.

When switching from the multicast send to a data direct data path, the client sends a flush request over the multicast send VCC. Until a flush response is received, or until the path switch delay expires, frames are queued for the destination.

Valid Values:
An integer number of seconds in the range of 1 to 4.

Default Value:
4

Example:

```
LEC Config> set flush-timeout 3
```

forward-delay

Sets the forward delay. Entries in the LE ARP cache must be periodically re-verified. The forward delay time is the maximum amount of time a remote entry may remain in the cache during a network topology change. Larger aging times may result in stale (invalid) entries, but also cause less re-verification traffic.

Valid Values:
An integer number of seconds in the range of 4 to 30.

Default Value:
15

Example:

```
LEC Config> set forward-delay 10
```

forward-disconnect-timeout

This parameter sets the amount of time that a LEC will wait after losing its last Multicast Forward VCC from the BUS before returning to the initial state. This delay permits the BUS to attempt to reconnect to the client without returning to the initial state.

Valid Values:
10 - 300 seconds

Default Value:
60

frame-size

Sets the frame size.

The value specified for frame-size must be equal to or less than the value specified for ATM max-frame using the ATM INTERFACE> **set max-frame** command as described on page 234.

Valid Values:
1516

4544

9234

18190

Default Value:
If the ELAN type is token ring, the default is 4544. If the ELAN type is Ethernet, the default is 1516.

Example:

```
LEC Config> set frame-size 4544
```

initial-control-timeout

This parameter sets the value of the initial control timeout used in the control timeout algorithm described in 256.

Valid Values:
1 - 10

Default Value:
5

Example:

```
LEC Config> set initial-control-timeout 10
```

lecs-atm-address

Specifies the ATM address of the LECS.

If the client is set to auto configure, it attempts to connect to a LECS. If it is unable to connect to a LECS, then it may try another LECS ATM address. The LECS ATM addresses that are tried, in order, are:

1. This configured LECS address
2. Any LECS address obtained through ILMI
3. The well-known LECS address defined by the ATM Forum.

No default is provided.

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
  LEC Config> set lecs-atm-address
39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.01
```

les-atm-address

Sets the LES ATM address. This command may be optional or required depending upon the setting of lecs-auto-config as described in the **set auto-config** command on page 255.

- If auto-config is YES, the les-atm-address is not configurable.
- If auto-config is NO, then the les-atm-address is required.

Specify the ATM address of the LES. No default is provided.

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
  LEC Config> set les-atm-address
        39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
```

mac-address

Sets the MAC address for this LE client. You *may* specify that the client use the burned-in MAC address of the ATM interface, or you may specify a different MAC address. If you have two clients that are bridged together, they should use different MAC addresses.

This MAC address is registered with the LES when the client joins the ELAN.

Valid Values:
Any valid MAC address.

Default Value:
none

Example:

```
  LEC Config> set mac-address
    Use adapter address for MAC? [No]
    MAC address []: 10.00.5a.00.00.01
```

multicast-send-avg

Sets the multicast send VCC average rate in Kbps. Used by the LEC for reserving bandwidth on the VCC to the BUS. It specifies the forward and backward sustained cell rate used when setting up a reserved bandwidth multicast send VCC.

This parameter is only applicable when the multicast-send-type is reserved bandwidth. If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must be less than or equal to multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-avg and multicast-send-peak must be specified.

Example:

```
LEC Config> set multicast-send-avg 4000
```

multicast-send-peak

Sets the multicast send peak rate in Kbps. Used by LEC for reserving bandwidth on the VCC to the BUS. It specifies the forward and backward peak cell rate used when establishing a reserved bandwidth multicast send VCC.

This parameter is only applicable when the multicast-send-type is reserved bandwidth. If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must be less than or equal to multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-avg and multicast-send-peak must be specified.

Example:

```
LEC Config> set multicast-send-peak 155
```

multicast-send-type

Sets the multicast send type. Specifies the method used by the LEC when establishing the multicast send VCC.

If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must at least equal multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-no and multicast-send-peak must be specified.

Valid Values:
Best Effort or Reserved

Default Value:
Best Effort

Example:

```
LEC Config> set multicast-send-type best-effort
```

multiplier-control-timeout

This parameter sets the value of the control timeout multiplier used in the control timeout algorithm described on page 256.

Valid Values:
2 - 5

Default Value:
2

Example:

```
LEC Config> set multiplier-control-timeout 5
```

path-switch-delay

Sets the path switch delay.

The LEC must ensure that all frames sent through the BUS to a destination have arrived at the destination before it can start using a Data Direct VCC. This is accomplished using the flush protocol, or by waiting path-switch-delay seconds after sending the last packet to the BUS. Smaller values improve performance, but may result in out-of-order packets in a heavily congested network.

Valid Values:

An integer number of seconds in the range of 1 to 8.

Default Value:

6

Example:

```
LEC Config> set path-switch-delay 5
```

reconfig-delay-min

This parameter sets the minimum delay time when LEC returns to the initial state. This value must be ≤ ***reconfig-delay-max***.

Valid Values:

1 - the value of ***reconfig-delay-max***

Default Value:

1

Example:

```
LEC Config> set reconfig-delay-min  5
```

reconfig-delay-max

This parameter sets the maximum delay time when LEC returns to the initial state. This value must be ≥ ***reconfig-delay-min***.

Valid Values:

1 - 10

Default Value:

5

Example:

```
LEC Config> set reconfig-delay-max 9
```

retry-count

Sets the retry count. This is maximum number of times that the LEC retries an LE_ARP_REQUEST for a specific frame's LAN destination. If no ARP response is received after the specified number of retries, then the entry is purged from the LE ARP cache.

Valid Values:

0, 1, or 2

Default Value:

1

Example:

```
LEC Config> set retry-count 2
```

selector

Specifies the selector portion of the client's ATM address. The combination of ESI and selector must be unique among all LANE components on the device. By default, a unique selector is selected for the configured ESI.

Valid Values:
Any octet, in hexadecimal, that is not in use by another LANE component with the same ESI.

Example:

```
LEC Config> set selector 01
```

trace Enables tracing for the LEC. To perform packet tracing, three steps are required:

1. Enable packet tracing system (under ELS)
2. Enable tracing on the LEC subsystem (under ELS)
3. Enable packet tracing on the desired LECs (using this command).

Valid Values:
Yes or No

Default Value:
No

Example:

```
Token Ring LEC config>set trace
Trace packets on the LEC? [No]?yes
```

unknown-count
Sets the unknown frame count. This is the maximum number of frames for a specific unicast MAC address or route descriptor that may be sent to the BUS within the time specified by the unknown-time parameter. Larger values decrease the number of discarded frames while increasing the load on the BUS.

Valid Values:
An integer number of frames in the range of 1 to 255.

Default Value:
10

unknown-time
Sets the unknown frame time. This is the time interval during which the maximum number of frames for a specific unicast MAC address or route descriptor (specified by the unknown-count parameter) may be sent to the BUS. Larger values increase the number of discarded frames while decreasing the load on the BUS.

Valid Values:
An integer number of seconds in the range of 1 to 60.

Default Value:
1

Example:

```
LEC Config> set unknown-time 5
```

vcc-timeout
Sets the VCC timeout. Data direct VCCs over which no traffic has been sent for this period of time should be released.

Valid Values: 0 to 31536000 seconds (1 year).

Default Value: 1200

Note: This parameter is meaningful only for SVC connections.

Example:

```
LEC Config> set vcc-timeout 1000
```

LLC Configuration Commands

This section summarizes and then explains all of the LLC commands. These commands, shown in Table 34, let you monitor the LLC while passing packets over an SNA network.

Table 34. LLC Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Displays configuration information.
Set	Allows the user to dynamically configure LLC parameters that are valid for the life of the session.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to display configuration information.

Syntax:

list

Set

Use the **set** command to dynamically configure the LLC parameters on a current LLC session. Any changes that you make to the parameters are effective for the life of session.

Attention: Changing LLC parameters from the default can affect how the LLC protocol works.

Syntax:

set n2-max_retry *count*
n3-frames-rcvd-before-ack *count*
nw-acks-to-inc-ww *count*
rw-receive-window *seconds*
t1-reply-timer *seconds*
t2-receive-ack-timer *seconds*
ti-inactivity-timer *seconds*
tw-transmit-window *seconds*

n2-max_retry
The maximum number of retries by LLC protocol. For example, N2 is the

maximum number of times the LLC transmits an RR without receiving an acknowledgment when the inactivity timer expires. Default is 8. Minimum is 1. Maximum is 127.

n3-frames-rcvd-before-ack
This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. Set this counter to a specified value. Each time an I-frame is received, this value is decremented. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1. Minimum is 1. Maximum is 255.

nw-acks-to-inc-ww
This field is set to a default value of 1.

rw-receive-window
Sets the number of I-frames that can be recived before an RR is transmitted. Default is 2. Minimum is 1. Maximum is 127.

t1-reply-timer
This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station. When this timer expires, an RR is sent with the poll bit set and T1 is started again. If the LLC receives no response after the configured maximum number of retries (N2), the link underneath is declared inoperative. Default is 1. Minimum is 1. Maximum is 256.

t2-receive-ack-timer
This timer is used to delay sending of an acknowledgment for a received I-format frame. This timer is started when an I-frame is received and reset when an acknowledgment is sent. If this timer expires, LLC2 sends an acknowledgment as soon as possible. Set this value so that it is less than that of T1. This insures that the remote LLC2 peer receives the delayed acknowledgment before the T1 timer expires. Default is 1 (100 ms). Minimum is 1. Maximum is 2560.

Note: If this timer is set to 1 (the default) it will not run (for example, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer
This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 timer expires. Default is 30 seconds. Minimum is 1 second. Maximum is 256 seconds.

tw-transmit-window
Sets the maximum number of I-frames that can be sent before receiving an RR. Assuming that the other end of the LLC session can actually receive this many consecutive I-frames, and the router has enough heap memory to keep copies of these frames until an acknowledgment is received, increasing this value may increase the throughput. Default is 2. Minimum is 1. Maximum is 127.

Accessing the LEC Monitoring Environment

Use the following procedure to access the LEC monitoring commands. This process gives you access to the LEC *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to “What is the OPCON Process?” on page 69.) For example:

```
* talk 5
+
```

After you enter the **talk 5** command, the GWCON prompt (+) displays on the console. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the + prompt, enter the **network ?** command to display the network interface numbers for which the router is currently configured, and enter the *interface number* for the LEC you wish to monitor. For example:

```
+ network ?

0  : ATM
1  : ATM Ethernet LAN Emulation: ETH
2  : IP Protocol Network
3  : Bridge Application
Network number [0]? 1
LEC+
```

The LEC monitoring prompt (`LEC+`), is displayed.

If you know the interface number of the LEC you wish to monitor, enter the **network** command followed by the *interface number* of the LEC.

```
+ network 1
LEC+
```

LEC Monitoring Commands

This section summarizes and then explains the LEC monitoring commands. You can access LEC monitoring commands at the `LEC+` prompt. Table 35 shows the commands.

Table 35. LE Client Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Lists: • LEC Address Resolution Table (ARP) • LEC configuration • Data Direct VCC information • Group addresses • RIF information • LEC statistics • VCC table.
LLC	Gets you to the `LLC>` monitoring prompt for Token Ring LECs.
MIB	Displays LEC MIB objects including: • LEC MIB Configuration Table • LEC MAC ARP Table • LEC Route Descriptor Table • LEC MIB Server VCC Tables • LEC MIB Statistics Table • LEC MIB Status Table
QoS	Gets you to the `LEC x QoS+` prompt from which you can monitor Quality of Service as described in “Quality of Service Monitoring Commands” on page 291.
Trace	Sets packet tracing on or off or sets a trace address or trace mask.

Table 35. LE Client Monitoring Command Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to list the LEC Address Resolution Table (ART), list the LEC configuration, list Data Direct VCC information, or list LEC statistics.

Syntax:

list arp-table
configuration
data-direct-vccs
group
rif
statistics
vcc-table

arp Lists the LEC Address Resolution Table (entries in the ARP cache).

Example:

```
LEC+ list arp

         LEC Address Resolution (LE ARP Cache) Table

  Max Table Size          = 10
  Free Table Entries      = 10
  Current Mac Entries     = 0
  Current RD Entries      = 0
  Arp Aging Time          = 300
  Verify Sweep Interval   = 60

                                Xmit  BUS   Arp
                       Conn   Queue Frame Retry Aging
 MAC Address     Remote Handle Depth Count Count Timer  Destination ATM Ad
                                                                    dress
 ------------------------------------------------------------------------
 40.00.00.00.00.09 False 652   0     0     0     60     39.99.99.99.99.99.
                               99.00.00.99.99.30.02.40.00.00.00.00.09.81
```

Note: The Sweep Interval is always one-fifth of the ARP Aging Timer value.

Max Table Size
The total number of entries available

Free Table Entries
The number of free entries

Current MAC Entries

Current RD Entries
Route Descriptor ATM entries

ARP Aging Time
Time for an entry to be aged out

Verify Sweep Interval

MAC Address

Remote

Connection Handle

Queue Depth

Xmit Frame Count

BUS Retry Count

ARP Aging Timer

Destination ATM Address

configuration

Lists the LEC configuration.

For Ethernet:

Example:

```
IBM LEC+ list config
                 ATM IBM LEC Configuration
   Physical ATM interface number             = 0
   LEC interface number             = 7
   Primary ATM address
          ESI address               = Use burned in addr
          Selector byte             = 0x3
   Emulated LAN type                = Ethernet
   Maximum frame size               = 1523
   LE Client MAC address            = Use burned in addr
   LE Server ATM address            = 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
   Forward Peak Rate                = 155000
   Backward Peak Rate               = 155000
    MAC cache size                   = 32
   MAC cache aging period           = 60
   Route Descriptor cache size      = 32
   Route Descriptor aging period    = 60
   LES Registration interval        = 60
   LES Registration retry count     = 3
   LES keep alive count             = 10
   Packet trace                     = No
   IP Encapsulation                 = ETHER
```

For Token Ring IBM:

Example:

```
IBM LEC+list config

                      ATM IBM LEC Configuration
   Physical ATM interface number             = 0
   LEC interface number             = 10
   Primary ATM address
          ESI address               = Use burned in addr
          Selector byte             = 0x6
   Emulated LAN type                = Token Ring
   Maximum frame size               = 4551
   LE Client MAC address            = Use burned in addr
   LE Server ATM address            = 39.84.07.00.00.00.00.00.00.00.00.00.00.01.10.00.5A.DD.DA.02
   Forward Peak Rate                = 155000
   Backward Peak Rate               = 155000
    MAC cache size                   = 32
   MAC cache aging period           = 60
   Route Descriptor cache size      = 32
   Route Descriptor aging period    = 60
   LES Registration interval        = 60
   LES Registration retry count     = 3
   LES keep alive count             = 10
   Packet trace                     = No
   RIF Aging Timer                  = 120
   Source Routing                   = Enabled
```

For Token Ring Forum Compliant:

Example:

```
LEC+ list config

   Physical ATM interface number = 0
   LEC interface number          = 9
   LEC ATM address               = 39.99.99.99.99.99.99.00.00.99.99.31.01.09.FC.DD.D0.32.70.0A
   LEC MAC address               = 40.00.82.10.17.09
   lecConfigMode                 = Manual
   lecConfigLanType              = 802.5 - Token Ring
   lecConfigMaxDataFrameSize     = 4544
   lecConfigLanName              =
   lecConfigLesAtmAddress        = 39.99.99.99.99.99.99.00.00.99.99.31.01.40.00.82.10.17.00.09
   lecControlTimeout             = 30
   lecMaxUnknownFrameCount       = 10
   lecMaxUnknownFrameTime        = 1
   lecVccTimeoutPeriod           = 1200
   lecMaxRetryCount              = 1
   lecAgingTime                  = 300
   lecForwardDelayTime           = 15
   lecExpectedArpResponseTime    = 1
   lecFlushTimeout               = 4
   lecPathSwitchingDelay         = 6
   lecLocalSegmentId             = 0x0
   lecMulticastSendType          = 1
   lecMulticastSendAvgRate       = 365566
   lecMulticastSendPeakRate      = 365566
   lecConnectionCompleteTimer    = 4
   lecInitialControlTimeout      = 5
   lecControlTimeoutMultiplier   = 2
   V2 Capable                    = TRUE
   lecForwardDisconnectTimeout   = 60
   lecMinReconfigDelay           = 1
   lecMaxReconfigDelay           = 5
   lecMaxBusConnectRetries       = 0
   lecElanId                     = 0
   ExplorerExclude               = TRUE
   LE ARP queue depth            = 5
   LE ARP cache size             = 5000
   Forward peakrate              = 365566
   Backward peakrate             = 365566
   Packet trace                  = Off
   RIF aging timer               = 120
   Source Routing                = enabled
```

See “Set” on page 253 for a definition of the parameters shown in the above examples.

data Lists the LEC Data Direct VCC information.

Example:

```
LEC+ list data

          LEC Data Direct VCC Table

   Max Table Size     = 1019    Max no of SVC connections
   Current Size       = 0       Currently used
   Inactivity Timeout = 1200    No Data Xfer Timeout before connection is
                                closed (seconds)
   Sweep Interval     = 60
      Conn              Inactive  User
      Handle  VPI  VCI   Timer    Count  Destination ATM Address
    ----------------------------------------------------------------------------

       652     0  7241    300       1    39.99.99.99.99.99.99.00.00.99.99.30.02.
                                         40.00.00.00.00.09.81


    ----------------------------------------------------------------------------
```

group Lists the group addresses in use by the LEC.

rif Lists the MAC address to Routing Information Field (RIF) mappings in use by the LEC.

statistics

Lists LEC statistics.

Example:

```
LEC+ list stat

          LEC Statistics

   In Octets.high     = 0       No of Bytes received
   In Octets.low      = 346
   In Discards        = 2       Packets discarded
   In Errors          = 0       Rx.Errors
   In Unknown Protos  = 0       Unknown protocols received
   Out Octets.high    = 0       No of Bytes xmitted.
   Out Octets.low     = 0
   Out Discards       = 0
   Out Errors         = 0       Tx.Errors
   In Frames          = 0
   Out Frames         = 0
   In Bytes           = 0
   Out Bytes          = 0
```

VCC table

Lists VCC table.

Example:

```
LEC+ list vcc
```

LLC

Logical Link Control can be thought of as a “sub-protocol”. It is not accessed directly from either the Talk 6 (configuration) or the Talk 5 (console) environment. Instead, it is accessed from the Token Ring LEC monitoring menu by entering an **LLC** command.

Use the **llc** command to access the LLC> prompt. See“LLC Monitoring Commands” on page 273 for more information.

Syntax:

llc

MIB

Use the **mib** command to display MIB objects.

Note: Some of this information may be displayed in a different format using the **list** command.

Syntax:

mib config-table

mac-arp-table

rd-arp-table

server-vcc-table

statistics-table

status-table

super-elan-table

Monitoring LE Clients

config Displays the LEC MIB Configuration Table.

Example:

```
LEC+ mib config

 lecConfigTable:
 lecConfigMode                 = Manual
 lecConfigLanType              = 802.3 - Ethernet
 lecConfigMaxDataFrameSize     = 1516
 lecConfigLanName              =
 lecConfigLesAtmAddress        = 39.84.0F.00.00.00.00.00.11.23.24.24.24.24.55.66.77.88.99.00
 lecControlTimeout             = 120
 lecMaxUnknownFrameCount       = 1
 lecMaxUnknownFrameTime        = 0
 lecVccTimeoutPeriod           = 1200
 lecMaxRetryCount              = 1
 lecAgingTime                  = 300
 lecForwardDelayTime           = 15
 lecExpectedArpResponseTime    = 1
 lecFlushTimeout               = 4
 lecPathSwitchingDelay         = 6
 lecLocalSegmentId             = 0
 lecMulticastSendType          = 1


 lecMulticastSendAvgRate       = 155000000
 lecMulticastSendPeakRate      = 155000000
 lecConnectionCompleteTimer    = 4
```

lecConfigMode
LEC config mode: AUTO or MANUAL. If AUTO, LEC Uses LECS to get the LES ATM address.

lecConfigLanType
LAN type, either Ethernet or token-ring

lecConfigMaxDataFrameSize
Maximum frame size

lecConfigLanName
ELAN Name

lecConfigLesAtmAddress
LE Server ATM address

lecControlTimeout
Timeout for request/response control frame

lecMaxUnknownFrameCount
Maximum number of unknown frames

lecMaxUnknownFrameTime
Period in which LEC will send a maximum of MaxUnknownFrameCount frames to the BUS for a given unicast LAN Destination, and it must also initiate the address resolution protocol to resolve that LAN Destination.

lecVccTimeoutPeriod
Inactivity timeout of SVC Data Direct VCCs

lecMaxRetryCount
LE ARP retry count

lecAgingTime
Life of unverified entry in the ARP table

lecForwardDelayTime

lecExpectedArpResponseTime
ARP Request/Response cycle time

lecFlushTimeout
LE Flush Request/Flush Reply timeout period

lecPathSwitchingDelay

lecLocalSegmentId
Segment ID of emulated LAN. Only for 802.5 clients

lecMulticastSendType
Signaling parameter used by LEC for multicast send VCC

lecMulticastSendAvgRate
Signaling parameter used by LEC for multicast send VCC

lecMulticastSendPeakRate
Signaling parameter used by LEC for multicast send VCC

lecConnectionCompleteTimer

mac Displays the LEC MAC ARP Table

rd Displays the LEC Route Descriptor Table

server Displays the LEC MIB Server VCC Tables

Example:

```
LEC+ mib server

lecServerVccTable:
   lecConfigDirectInterface      = 0
   lecConfigDirectVpi            = 0
   lecConfigDirectVci            = 0
   lecControlDirectInterface     = 1
   lecControlDirectVpi           = 0
   lecControlDirectVci           = 38
   lecControlDistributeInterface = 1
   lecControlDistributeVpi       = 0
   lecControlDistributeVci       = 37
   lecMulticastSendInterface     = 1
   lecMulticastSendVpi           = 0
   lecMulticastSendVci           = 34
   lecMulticastForwardInterface  = 1
   lecMulticastForwardVpi        = 0
   lecMulticastForwardVci        = 33
```

lecConfigDirectInterface
The interface associated with the Configuration Direct VCC

lecConfigDirectVpi
VPI which identifies the above VCC if it exists

lecConfigDirectVci
VCI which identifies the above VCC if it exists

lecControlDirectInterface
The interface associated with the Control Direct VCC

lecControlDirectVpi
VPI which identifies the above VCC if it exists

lecControlDirectVci
VCI which identifies the above VCC if it exists

lecControlDistributeInterface
The interface associated with the Control Distribute VCC

lecControlDistributeVpi
VPI which identifies the above VCC if it exists

lecControlDistributeVci
VCI which identifies the above VCC if it exists

lecMulticastSendInterface
The interface associated with the Multicast Send VCC

lecMulticastSendVpi
VPI which identifies the above VCC if it exists

lecMulticastSendVci
VCI which identifies the above VCC if it exists

lecMulticastForwardInterface
The interface associated with the Multicast Forward VCC

lecMulticastForwardVpi
VPI which identifies the above VCC if it exists

lecMulticastForwardVci
VCI which identifies the above VCC if it exists

statistics
Displays the LEC MIB Statistics Table.

Example:

```
LEC+ mib statistics

lecStatisticsTable:
   lecArpRequestsOut             = 1
   lecArpRequestsIn              = 0
   lecArpRepliesOut              = 0
   lecArpRepliesIn               = 1
   lecControlFramesOut           = 2
   lecControlFramesIn            = 2
   lecSvcFailures                = 1
```

lecArpRequestsOut
No. of LE ARP requests sent by this LEC

lecArpRequestsIn
No. of LE ARP requests received by this LEC

lecArpRepliesOut
No. of LE ARP responses sent by this LEC

lecArpRepliesIn
No. of LE ARP responses received by this LEC

lecControlFramesOut
No. of Control Packets sent by this LEC

lecControlFramesIn
No. of Control Packets received by this LEC

lecSvcFailures
The total number of:

- Outgoing LAN Emulation SVCs which this client tried but failed, to open
- Incoming LAN Emulation SVCs which this client tried, but failed to establish
- Incoming LAN Emulation SVCs which this client rejected for protocol or security reasons

status Lists MIB status.

Example:

```
LEC+ mib status

lecStatusTable:
   lecPrimaryAtmAddress          = 39.84.0F.00.00.00
   Client ATM address=           = 00.00.00.00.00.01.10.00.5A.00.DE.AD.03
   lecId                         = 1                    Assigned by LES
   lecInterfaceState             = Operational          State of the LEC
   lecLastFailureRespCode        = None                 Error code from last
                                                        failed Config/Join resp.
   lecLastFailureState           = Initial State        State of LEC when
                                                        updating above field.
   lecProtocol                   = 1                    Protocol specified by
                                                        LEC in Join requests.
   LecVersion                    = 1                    LEC Protocol Version
                                                        of above
   lecTopologyChange             = False
   lecConfigServerAtmAddress     = 00.00.00.00.00.00.
   ATM Address of LECS           = 00.00.00.00.00.00.00.00.00.00.00.00.00.00
   lecConfigSource               = Did not use LECS
   lecActualLanType              = 802.3 - Ethernet     Frame format currently
                                                        used by LEC
   lecActualMaxDataFrameSize     = 1516
   lecActualLanName              = ETH                  Name of emulated LAN
                                                        that LEC joined.
   lecActualLesAtmAddress        = 39.84.0F.00.00.00.
   ATM Address of LES            = 00.00.00.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
   lecProxyClient                = False                Is LES acting like a
                                                        proxy ?
```

super-elan

Example:

```
LEC+ mib super-elan
```

QoS Information

Use the **qos-information** command to get to the `LEC x QoS+` prompt from which you can monitor Quality of Service as described in “Quality of Service Monitoring Commands” on page 291.

Syntax:

qos-information

Trace

Use the **trace** command to turn packet tracing on or off on the LEC. See “Packet-trace Monitoring Commands” on page 193 for more information.

Use the **trace mac-address** command to limit the data traced. A packet will only be traced if its destination or source MAC address logically ANDed with the trace MAC mask equals the trace MAC address logically ANDed with the trace MAC mask.

Syntax:

trace

LLC Monitoring Commands

This section summarizes and then explains all of the LLC commands. These commands, shown in Table 36, let you monitor the LLC while passing packets over an SNA network.

Table 36. LLC Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Displays configuration information.

Table 36. LLC Monitoring Command Summary (continued)

Command	Function
Set	Allows the user to dynamically configure LLC parameters that are valid for the life of the session.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to display configuration information.

Syntax:

list

Set

Use the **set** command to dynamically configure the LLC parameters on a current LLC session. Any changes that you make to the parameters are effective for the life of session.

Attention: Changing LLC parameters from the default can affect how the LLC protocol works.

Syntax:

set	n2-max_retry *count*
	n3-frames-rcvd-before-ack *count*
	nw-acks-to-inc-ww *count*
	t1-reply-timer *seconds*
	t2-receive-ack-timer *seconds*
	ti-inactivity-timer *seconds*
	tw-transmit-window *seconds*

n2-max_retry
The maximum number of retries by LLC protocol. For example, N2 is the maximum number of times the LLC transmits an RR without receiving an acknowledgment when the inactivity timer expires. Default is 8. Minimum is 1. Maximum is 127.

n3-frames-rcvd-before-ack
This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. Set this counter to a specified value. Each time an I-frame is received, this value is decremented. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1. Minimum is 1. Maximum is 255.

nw-acks-to-inc-ww
This field is set to a default value of 1.

t1-reply-timer
This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station. When this timer expires, an RR is sent with the poll bit set and T1 is started again. If the LLC receives no

response after the configured maximum number of retries (N2), the link underneath is declared inoperative. Default is 1. Minimum is 1. Maximum is 256.

t2-receive-ack-timer

This timer is used to delay sending of an acknowledgment for a received I-format frame. This timer is started when an I-frame is received and reset when an acknowledgment is sent. If this timer expires, LLC2 sends an acknowledgment as soon as possible. Set this value so that it is less than that of T1. This insures that the remote LLC2 peer receives the delayed acknowledgment before the T1 timer expires. Default is 1 (100 ms). Minimum is 1. Maximum is 2560.

Note: If this timer is set to 1 (the default) it will not run (for example, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer

This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 timer expires. Default is 30 seconds. Minimum is 1 second. Maximum is 256 seconds.

tw-transmit-window

Sets the maximum number of I-frames that can be sent before receiving an RR. Assuming that the other end of the LLC session can actually receive this many consecutive I-frames, and the router has enough heap memory to keep copies of these frames until an acknowledgment is received, increasing this value may increase the throughput. Default is 2. Minimum is 1. Maximum is 127.

Chapter 22. Configuring and Monitoring Quality of Service (QoS)

This chapter describes Quality of Service (QoS) configuration and operational commands for LAN and ELAN interfaces in the router. It contains the following sections:

Quality of Service Overview

The QoS feature leverages the benefits of ATM QoS capabilities for LAN Emulation Data Direct VCCs. This support is referred to as “Configurable QoS for LAN Emulation”. The key attributes and the benefits of this feature are as follows:

- An LE Client makes use of configured QoS parameters for its Data Direct VCCs.
- QoS parameters can be configured for:
  - LE Client
  - ATM Interface
- The set of QoS parameters configured are for use with ATM Forum UNI 3.0/3.1 signaling. The parameters include the desired Peak Cell Rate, Sustained Cell Rate, QoS Class and Maximum Burst Size.
- Maximum Reserved Bandwidth per VCC can be configured to protect an LE Client from accepting/establishing VCCs whose traffic parameters it cannot support.
- The QoS Negotiation mechanism enables the participating LE Clients to be aware of each other’s QoS parameters. A data-direct VCC is set up using the negotiated parameters.

Benefits of QoS

- Using QoS for the LE Client, ATM Interface, or Emulated LAN provides the following benefits for LANE Data Direct VCCs.
  - An LE Client can be configured with QoS if the QoS required by the client is different from the QoS required by other clients on the ELAN. For example, if an LE Client serves a file server, then the user may want to configure appropriate QoS parameters for all traffic to and from the file server.
  - An ATM Interface can be configured with QoS if a user wants all LE Clients on that ATM interface to use the same set of parameters. For example, if an ATM Interface is connected at 25 Mbps, the user can configure appropriate parameters that are different from those at a 155-Mbps interface.

QoS Configuration Parameters

This section describes nine parameters that are used for QoS configuration. The following six parameters can be configured for an LE Client or an ATM Interface:

1. max-reserved-bandwidth
2. traffic-type
3. peak-cell-rate
4. sustained-cell-rate
5. max-burst-size
6. qos-class

The following two parameters can be configured for an Emulated LAN and an LE Client:

1. *validate-pcr-of-best-effort-vccs*
2. *negotiate-qos*

The *accept-qos-parms-from-lecs* parameter can be configured only for an LE Client.

The first six parameters control the traffic characteristics of Data Direct VCCs established by the LE Client while the first parameter also applies to the calls received by the LE Client. The following characteristics are associated with all the Data Direct VCCs established by the LE Client:

- Bandwidth is not reserved for best-effort traffic.
- Traffic parameters apply to both forward and backward directions.
- When a reserved bandwidth connection is rejected due to the traffic parameters or QoS Class, the call is retried as a best-effort connection with the configured peak cell rate (cause codes on release or release-complete messages are used to determine why a VCC was released).
- When a best-effort connection is rejected due to the Peak Cell Rate (PCR), the call may be automatically retried with a lower PCR. Retries are performed under the following conditions:
  1. If the rejected PCR is greater than 100 Mbps, the call is retried with a PCR of 100 Mbps.
  2. Otherwise, if the rejected PCR is greater than 25 Mbps, the call is retried with a PCR of 25 Mbps.

Maximum Reserved Bandwidth (max-reserved-bandwidth)

The maximum reserved bandwidth acceptable for a Data Direct VCC. This parameter applies to both Data Direct VCC calls received by the LE Client and Data Direct VCC calls placed by the LE Client. For incoming calls, this parameter defines the maximum acceptable SCR for a Data Direct VCC. If SCR is not specified on the incoming call, then this parameter defines the maximum acceptable PCR for a Data Direct VCC with reserved bandwidth.

Calls received with traffic parameters specifying higher rates will be released. If SCR is specified on the incoming call, the call will not be rejected due to the PCR or Maximum Burst Size. The constraint imposed by this parameter is not applicable to BEST_EFFORT connections. For outgoing calls, this parameter sets an upper bound on the amount of reserved bandwidth that can be requested for a Data Direct VCC. Therefore the traffic-type and sustained-cell-rate parameters are dependent upon this parameter.

Valid Values:
Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:
0

Traffic Type (traffic-type)

The desired traffic type for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the type of calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired type of traffic characteristics for Data Direct VCCs. When QoS parameters are negotiated, if either the source or target LEC desires a reserved bandwidth connection and both LECs support reserved bandwidth connections (that is, max-reserved-bandwidth > 0), then an attempt will be made to establish a reserved bandwidth Data Direct VCC between the two LECs. Otherwise, the Data Direct VCC will be a best-effort connection. Dependencies: max-reserved-bandwidth

Valid Values:
best_effort or reserved_bandwidth

Default:
best_effort

Peak Cell Rate (peak-cell-rate)

The desired peak cell rate for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the PCR traffic parameter for Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired PCR traffic parameter for Data Direct VCCs. The minimum of the desired PCRs of the two LECs is used for negotiated best-effort VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired PCR of that LEC is used for the Data Direct VCC subject to the upper bound imposed by the line rate of the local ATM device. If both LECs request a reserved bandwidth connection, then the maximum of the desired PCRs of the LE Clients is used for the Data Direct VCC subject to the upper bound imposed the line rate of the local ATM device.

Valid Values:
An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:
Line speed of LEC ATM Device in Kbps.

Sustained Cell Rate (sustained-cell-rate)

The desired sustained cell rate for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the SCR traffic parameter for Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired SCR traffic parameter for Data Direct VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired SCR of that LEC is used for the Data Direct VCC (subject to the upper bound imposed by the max-reserved-bandwidth parameter of the other LEC). If both LECs request a reserved bandwidth connection, then the maximum of the desired SCRs of the LE Clients is used for the Data Direct VCC (subject to the upper bound imposed by the max-reserved-bandwidth parameters of both LECs). In any case (negotiation or not), if the SCR that is to be signaled equals the PCR that is to be signaled, then the call is signaled with PCR only.

Dependencies: max-reserved-bandwidth, traffic-type and peak-cell-rate. This parameter is applicable only when traffic-type is RESERVED_BANDWIDTH.

Valid Values:
An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate, specified in Kbps

Default Value
None

Maximum Burst Size (max-burst-size)

The desired maximum burst size for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the Maximum Burst Size traffic parameter for Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired Maximum Burst Size traffic parameter for Data Direct VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired Maximum Burst Size of that LEC is used for the Data Direct VCC. If both LECs request a reserved bandwidth connection, then the maximum of the desired Maximum Burst Sizes of the LE Clients is used for the Data Direct VCC.

In any case (negotiation or not), the Maximum Burst Size is signaled only when SCR is signaled. Although this parameter is expressed in units of cells, it is configured as an integer multiple of the Maximum Data Frame Size (specified in LEC’s C3 parameter) with a lower bound of 1.

Dependencies: This parameter is applicable only when traffic-type is RESERVED_BANDWIDTH.

Valid Values:
An integer number of frames; must be greater than 0

Default:
1 frame

QoS Class (qos-class)

The desired QoS class for reserved bandwidth calls. If QoS parameters are not negotiated, then this parameter specifies the QoS Class to be used for reserved bandwidth Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the QoS Class that is desired for Data Direct VCCs. Unspecified QoS Class is always used on best-effort calls.

Specified QoS Classes define objective values for ATM performance. Specified QoS Classes define objective values for ATM performance parameters such as cell loss ratio and cell transfer delay.

The UNI Specification states that:

Specified QoS Class 1
should yield performance comparable to current digital private line performance.

Specified QoS Class 2
is intended for packetized video and audio in teleconferencing and multimedia applications.

Specified QoS Class 3
is intended for interoperation of connection oriented protocols, such as Frame Relay.

Specified QoS Class 4
is intended for interoperation of connectionless protocols, such as IP or SMDS.

LECs must be able to accept calls with any of the above QoS Classes. When QoS parameters are negotiated, the configured QoS Classes of the two LECs are compared, and the QoS Class with the more stringent requirements is used.

Valid Values:

0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:
0 (Unspecified QoS Class)

Validate PCR of Best-Effort VCCs (validate-pcr-of-best-effort-vccs)

To validate Peak Cell Rate of Best-Effort VCCs. When FALSE, best-effort VCCs will be accepted without regard to the signaled forward PCR. When TRUE, best- effort VCCs will be rejected if the signaled forward PCR exceeds the line rate of the LE Client ATM device. Calls will not be rejected due to the backward PCR. The signaled backward PCR will be honored if it does not exceed the line rate; otherwise, transmissions to the caller will be at line rate.

Notes:

1. Accepting best-effort VCCs with forward PCRs that exceed the line rate can result in poor performance due to excessive retransmissions; however, rejecting these VCCs can result in interoperability problems.
2. The YES setting is useful when callers will retry with a lower PCR following call rejection due to unavailable cell rate.

Valid Values:
yes, no

Default Value:
no

Negotiate QoS (negotiate-qos)

Enable QoS parameter negotiation for Data Direct VCCs. This parameter should be enabled only when connecting to an IBM MSS LES. When this parameter is YES, the LE Client will include an IBM Traffic Parameter TLV in LE_JOIN_REQUEST and LE_ARP_RESPONSE frames sent to the LES. This TLV will include the values of max-reserved-bandwidth, traffic-type, peak-cell-rate, sustained-cell-rate, max-burst-size and qos-class. An IBM Traffic Parameter TLV may also be included in a LE_ARP_RESPONSE returned to the LE Client by the LES.

If there is no TLV in a LE_ARP_RESPONSE received by the LE Client, then the local configuration parameters must be used to setup the Data Direct VCC. If a TLV is included in a LE_ARP_RESPONSE, the LE Client must compare the contents of the TLV with the corresponding local values to determine the “negotiated” or “best” set of parameters acceptable to both parties before signalling for the Data Direct VCC.

Valid Values:
yes, no

Default Value:
no

Accept QoS Parms from LECS (accept-qos-parms-from-lecs)

This parameter gives the ability to configure an LE Client to accept/reject QoS parameters from a LECS. When this parameter is YES, the LE Client should use the QoS parameters obtained from the LE Clients in the LE_CONFIGURE_RESPONSE frames, that is, the QoS parameters from the LE Clients override the locally configured QoS parameters. If this parameter is NO then the LE Client will ignore any QoS parameters received in an LE_CONFIGURE_RESPONSE frame from the LE Clients.

Valid Values:
yes, no

Default Value:
no

Accessing the QoS Configuration Prompt

Use the **feature** command from the CONFIG process to access the Quality of Service configuration commands. Enter **feature** followed by the feature number (6) or short name (QoS). For example:

```
Config> feature qos
Quality of Service - Configuration
QoS Config>
```

Once you access the `QoS Config>` prompt, you can configure the Quality of Service (QoS) of an LE Client, or an ATM Interface. To return to the `Config>` prompt at any time, enter the **exit** command at the `QoS Config>` prompt.

Alternatively, you can configure QoS parameters for an LE Client or an ATM Interface by accessing the entities as follows:

- LE Client
  1. At the `Config>` prompt, enter the **network** command and the LE Client interface number.

2. At the `LE Client configuration>` prompt enter **qos-configuration**.

   Example:

   ```
   config> network 3
   Token Ring Forum Compliant LEC Config> qos-configuration
   LEC QoS Config>
   ```

- ATM Interface
  1. at the `Config>` prompt, enter the **network** command and the ATM interface number to get you to the `ATM Config>` prompt.
  2. Enter the **interface** parameter to get to the `ATM Interface Config>` prompt.
  3. At the `ATM InterfaceConfig>` prompt enter **qos-configuration**.

     Example:

     ```
     config> network 0
     ATM Config> interface
     ATM Interface Config> qos-configuration
     ATM-I/F 0 QoS>
     ```

Quality of Service Commands

This section summarizes the QoS configuration commands. Use the following commands to configure Quality of Service. Enter the commands from the `QoS Config>` prompt.

Table 37. Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
le-client	Gets you to the `LE Client QoS configuration >` prompt for the selected LE client.
atm-interface	Gets you to the `ATM Interface QoS configuration>` prompt for the selected ATM interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

LE Client QoS Configuration Commands

This section summarizes and explains the commands for configuring QoS for a specific LE Client.

Use the following commands at the `LEC QoS config>` prompt.

Table 38. LE Client Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Lists the current QoS configuration of the LE Client.
Set	Sets the QoS parameters of the LE Client.
Remove	Removes the QoS configuration of the LE Client.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to list the QoS configuration of this LE Client. QoS parameters are listed only if at least one has been specifically configured (see Example 1). Otherwise, no parameters are listed (see Example 2).

Syntax:

list

Example 1:

```
LEC QoS Config> list

           LE Client QoS Configuration for Data Direct VCCs
           ==========================================
     (ATM interface number = 0,  LEC interface number = 3)

  Maximum Reserved Bandwidth for a Data-Direct VCC = 10000 Kbps
  Data-Direct VCC Type ........................... = Best-Effort
  Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
  Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
  Desired QoS Class of Reserved Connections ...... = 0
  Max Burst Size of Reserved Connections    ...... = 0 frames

  Validate Peak Rate of Best-Effort connections .. = No
  Enable QoS Parameter Negotiation ............... = Yes
  Accept QoS Parameters from LECS ................ = Yes

LEC QoS Config>
```

Example 2:

```
LEC QoS Config> list

   QoS has not been configured for this LEC.
   Please use the SET option to configure QoS.

LEC QoS Config>
```

Set

Use the **set** command to specify LE Client QoS parameters.

Syntax:

set accept-qos-parms-from-lecs
all-default-values
max-burst-size
max-reserved-bandwidth
negotiate-qos
peak-cell-rate
qos-class
sustained-cell-rate
traffic-type
validate-pcr-of-best-effort-vccs

accept-qos-parms-from-lecs
Use this option to enable/disable the LE Client to accept/reject the QoS

parameters received from an LECS as TLVs. See “Accept QoS Parms from LECS (accept-qos-parms-from-lecs)” on page 282 for a more detailed description of this parameter.

Valid Values:
YES, NO

Default Value:
YES

Example:

```
LEC QoS Config> se acc y
LEC QoS Config>
```

all-default-values
Use this option to set the QoS parameters to default values. In the following example the default values are also listed.

Example:

```
LEC QoS Config> set all-default-values
   Failed to locate existing QoS configuration record!
   Using a new set of default values ...
   Initializing all parameters to default values
   LEC QoS Config> list

              LE Client QoS Configuration for Data Direct VCCs
              ==========================================
        (ATM interface number = 0,  LEC interface number = 3)

     Maximum Reserved Bandwidth for a Data-Direct VCC = 0 Kbps
     Data-Direct VCC Type ........................... = Best-Effort
     Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
     Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
     Desired QoS Class of Reserved Connections ...... = 0
     Max Burst Size of Reserved Connections    ...... = 0 frames

     Validate Peak Rate of Best-Effort connections .. = No
     Enable QoS Parameter Negotiation .............. = No
     Accept QoS Parameters from LECS ............... = Yes

  LEC QoS Config>
```

max-burst-size
Sets the desired maximum burst size in frames. See “Maximum Burst Size (max-burst-size)” on page 280 for a more detailed description of this parameter.

Valid Values:
An integer number of frames; must be greater than 0

Default:
1 frame

Example:

```
LEC QoS Config>  se ma
   Maximum Burst Size in Kbps [1]? 10000
   LEC QoS Config>
```

max-reserved-bandwidth
Use this option to set the maximum reserved bandwidth allowable per Data Direct VCC. See “Maximum Reserved Bandwidth (max-reserved-bandwidth)” on page 278 for a more detailed description of this parameter.

Valid Values:
Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:
0

Example:

```
LEC QoS Config> set max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]? 20000
LEC QoS Config>
```

negotiate-qos

Use this option to enable/disable the LE Client's participation in QoS negotiation. See "Negotiate QoS (negotiate-qos)" on page 282 for a more detailed description of this parameter.

Valid Values:

YES, NO

Default Value:

NO

Example:

```
LEC QoS Config>  se neg y
LEC QoS Config>
```

peak-cell-rate

Sets the desired peak cell rate for Data Direct. See "Peak Cell Rate (peak-cell-rate)" on page 279 for a more detailed description of this parameter.

Valid Values:

An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:

Line speed of LEC ATM Device in Kbps.

Example:

```
LEC QoS Config>  set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
LEC QoS Config>
```

qos-class

Sets the desired QoS Class for Data Direct VCCs. See "QoS Class (qos-class)" on page 280 for a more detailed description of this parameter.

Valid Values:

0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:

0 (Unspecified QoS Class)

Example:

```
LEC QoS Config>  se qos
Desired QoS Class for Data Direct VCCs [0]? 1
LEC QoS Config>
```

sustained-cell-rate

Sets the desired sustained cell rate for Data Direct VCCs. See "Sustained Cell Rate (sustained-cell-rate)" on page 279 for a more detailed description of this parameter.

Valid Values:
An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate, specified in Kbps

Default Value
None

Example:

```
LEC QoS Config>  se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
LEC QoS Config>
```

traffic-type
Sets the desired traffic for Data Direct VCCs. See “Traffic Type (traffic-type)” on page 279 for a more detailed description of this parameter.

Valid Values:
BEST_EFFORT or RESERVED_BANDWIDTH

Default:
BEST EFFORT.

Example:

```
LEC QoS Config> set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved-Bandwidth
Data Direct VCC Type [0]? 1
NOTE: Peak Cell Rate has been reset to 1
      Sustained Cell Rate has been reset to 1
      Max Reserved Bandwidth has been reset to 1
      Please configure appropriate values.
LEC QoS Config>
```

validate-pcr-of-best-effort-vccs
Use this option to enable/disable validation of the Peak Cell Rate traffic parameter of the Data Direct VCC calls received by this LE Client. See “Validate PCR of Best-Effort VCCs (validate-pcr-of-best-effort-vccs)” on page 281 for a more detailed description of this parameter.

Valid Values:
YES, NO

Default Value:
NO

Example:

```
LEC QoS Config>  se val y
LEC QoS Config>
```

Remove

Use the **remove** command to remove the QoS configuration of this LE Client.

Syntax:

remove

Example:

```
LEC QoS Config>  remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the LEC QoS configuration be deleted? [No]: yes
Deleted QoS configuration successfully
LEC QoS Config>
```

ATM Interface QoS Configuration Commands

Table 39. LE Client Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Lists the current ATM Interface QoS configuration.
Set	Sets the ATM Interface QoS parameters.
Remove	Removes the QoS configuration of the ATM Interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to list the QoS configuration of this ATM Interface. QoS parameters are listed only if at least one parameter has been configured (see following example). Otherwise, no parameters are listed.

Syntax:

list

Example:

```
ATM-I/F 0 QoS> list

          ATM Interface 'Quality of Service' Configuration
          ================================================
                    (ATM interface number = 0  )

     Maximum Reserved Bandwidth for a VCC = 15000 Kbps
     VCC Type .......................... = RESERVED-BANDWIDTH
     Peak Cell Rate .................... = 20000 Kbps
     Sustained Cell Rate ............... = 5000 Kbps
     QoS Class ......................... = 4
     Maximum Burst Size ................ = 5 frames
ATM-I/F 0 QoS>
```

Set

Use the **set** command to specify ATM Interface QoS parameters.

Syntax:

set max-burst-size

max-reserved-bandwidth

peak-cell-rate

qos-class

sustained-cell-rate

traffic-type

max-burst-size

Sets the desired maximum burst size in frames. See “Maximum Burst Size (max-burst-size)” on page 280 for a more detailed description of this parameter.

Valid Values:

An integer number of frames; must be greater than 0

Default:
1 frame

Example:

```
ATM-I/F 0 QoS Config> se ma
Maximum Burst Size in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

max-reserved-bandwidth
Use this option to set the maximum reserved bandwidth allowable for each Data Direct VCC. See “Maximum Reserved Bandwidth (max-reserved-bandwidth)” on page 278 for a more detailed description of this parameter.

Valid Values:
Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:
0

Example:

```
  ATM-I/F 0 QoS> se max-reserved-bandwidth
  Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]?
15000
  ATM-I/F 0 QoS>
```

peak-cell-rate
Sets the desired peak cell rate for Data Direct VCCs. See “Peak Cell Rate (peak-cell-rate)” on page 279 for a more detailed description of this parameter.

Valid Values:
An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:
Line speed of LEC ATM Device in Kbps.

Example:

```
ATM-I/F 0 QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
ATM-I/F 0 QoS Config>
```

qos-class
Sets the desired QoS Class for Data Direct VCCs. See “QoS Class (qos-class)” on page 280 for a more detailed description of this parameter.

Valid Values:
0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:
0 (Unspecified QoS Class)

Example:

```
ATM-I/F 0 QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
ATM-I/F 0 QoS Config>
```

sustained-cell-rate

Sets the desired sustained cell rate for Data Direct VCCs. See “Sustained Cell Rate (sustained-cell-rate)” on page 279 for a more detailed description of this parameter.

Valid Values:

An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate; specified in Kbps

Default Value

None

Example:

```
ATM-I/F 0 QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

traffic-type

Sets the desired traffic for Data Direct VCCs. See “Traffic Type (traffic-type)” on page 279 for a more detailed description of this parameter.

Valid Values:

BEST_EFFORT or RESERVED_BANDWIDTH

Default:

BEST EFFORT.

Example:

```
ATM-I/F 0 QoS> set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved Bandwidth
Traffic Type of VCCs [1]? 0
ATM-I/F 0 QoS>
```

Remove

Use the **remove** command to remove the QoS configuration of this ATM Interface.

Syntax:

remove

Example:

```
ATM-I/F 0 QoS> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the ATM Interface QoS configuration be deleted? [No]: yes
Deleted QoS SRAM record successfully
ATM-I/F 0 QoS>
```

Accessing the QoS Monitoring Commands

Use the **feature** command from the GWCON process to access the Quality of Service monitoring commands. Enter the **feature** followed by the feature number (6) or short name (QoS). For example:

```
+feature qos
Quality of Service (QoS) - User Monitoring
QoS+
```

Once you access the QoS monitoring prompt, you can select the monitoring of a particular LE Client. To return to the GWCON prompt at any time, enter the exit command at the QoS monitoring prompt.

Alternatively, you can access the QoS Monitoring of an LE Client as follows:

1. At the GWCON prompt (+), enter the network command and the LE Client interface number.
2. At the LE Client monitoring prompt enter **qos-information**.

   Example:

   ```
   +network 3
   ATM Emulated LAN Monitoring
   LEC+qos information
   LE Client QoS Monitoring
   LEC 3 QoS+
   ```

Quality of Service Monitoring Commands

This section summarizes the QoS monitoring commands. Enter these commands at the QoS+ prompt.

Table 40. Quality of Service (QoS) Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
le-client	Gets you to the `LE Client QoS console +` prompt for the selected LE client.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

LE Client QoS Monitoring Commands

This section summarizes the LE Client QoS monitoring commands. Enter the commands from the `LEC num QoS+` prompt.

Table 41. LE Client QoS Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Lists the current LE Client QoS information. Options include: configuration parameters, TLVs, VCCs, and statistics.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to list the QoS related information of this LE Client.

Syntax:

list configuration-parameters
data-direct-VCCs (Detailed Information)
statistics
tlv-information
vcc-information

configuration-parameters

Lists the QoS configuration parameters. Because parameters can be configured for an LE Client, ATM Interface or the ELAN, these parameters are displayed along with a resolved set of parameters that are used by the LE Client.

le-client

The parameters configured for this LE Client which are obtained from the SRAM records. If the SRAM records contain an invalid set of parameters then this column will not display any parameters values.

ATM Interface

The parameters configured for the ATM Interface used by this LE Client. These parameters are obtained from the local SRAM records. If the SRAM records contain an invalid set of parameters then this column will not display any parameter values.

From LECS

The parameters received by this LE Client from the LE Configuration Server. The parameters are received as individual TLVs in the LE_CONFIGURE_RESPONSE control message.

used The resolved set of traffic parameters which are used by for its Data Direct VCCs. If none of the entities is configured with QoS parameters, then the USED parameters represent the default parameters. If parameters are configured for at least one entity, then they are resolved as follows:

- If only the LE Client or the ATM Interface is configured with parameters and either the accept-parms-from-lecs is FALSE or no parameters were received from the LECS, then the configured LE Client or the ATM Interface parameters are used.
- If both the LE Client and the ATM Interface have configured parameters, then the LE Client parameters are used.
- If the accept-parms-from-lecs is TRUE and parameters were received from the LECS, then the LE Client parameters (or the default if the LE Client is not configured) are combined with those received from the LECS to form a complete set of the first six QoS parameters described in “QoS Configuration Parameters” on page 278.
- If the set of the first six QoS parameters described in “QoS Configuration Parameters” on page 278 contains an invalid combination then the parameters from the LECS are rejected. Note that the two flags negotiate-qos and validate-pcr-of-best-effort-vccs are validated independently.

Example:

```
LEC 1 QoS+ list configuration parameters


                ATM LEC Configured QoS  Parameters
                ==================================

      QoS                                  |   LEC      ATM-IF    FROM

   PARAMETER                        USED   |   SRAM     SRAM      LECS

 ----------------------------------------------------------------------------
 Max Reserved Bandwidth (cells/sec) :    23584  |    23584        0     none
                        (Kbits/sec) :    10000  |    10000        0     none
 VCC Type ......................... :   ResvBW  |   ResvBW   BstEft        0
 Peak Cell Rate ........(cells/sec) :    18867  |    18867   365566   365566
```

```
                     (Kbits/sec) :     8000  |      8000   155000   155000
 Sustained Cell Rate ...(cells/sec) :    18867  |     18867   365566     none
                     (Kbits/sec) :     8000  |      8000   155000     none
 QoS Class ........................ :        4  |         4        0     none
 Max Burst Size ............(cells) :       95  |        95        0     none
                        (frames) :        1  |         1        0     none
 Validate PCR of Best-Effort VCCs . :       NO  |        NO      n/a     none
 Enable QoS Negotiation ........... :      YES  |       YES      n/a     none
 Accept QoS Parameters from LECS .. :      YES  |       YES      n/a      n/a
 ---------------------------------------------------------------------------
(BstEft = Best Effort, ResvBW = Reserved Bandwidth)
(n/a = not applicable, none = no value is specified)

LEC 1 QoS+
```

data-direct-vccs (Detailed Information)

This option lists the Data Direct VCC information of this LE Client. Similar information is also listed using **list vcc-information**.

Example:

```
LEC 1 QoS+ list data direct vccs

          LEC Data Direct VCCs - QoS Information
          ======================================

Conn Handle = 80, VPI = 0, VCI = 546
        Connection Type = RETRIED CONNECTION PARAMETERS
          TrafficType    = BEST EFFORT VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 58962 (25 Mbps)
          QoS Class      = 0
          Max Burst Size = 0

Conn Handle = 78, VPI = 0, VCI = 544
        Connection Type = PARAMETERS SET BY DESTINATION
          TrafficType    = RESERVED BANDWIDTH VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 16509 (7 Mbps)
          QoS Class      = 1
          Max Burst Size = 95

LEC 1 QoS+
```

statistics

Counters are maintained for the following statistics:

Successful QoS Connections
Number of RESERVED-BANDWIDTH connections established by the LE Client.

Successful Best-Effort Connections
Number of BEST-EFFORT connections established by the LE Client.

Failed QoS Connections
Number of RESERVED-BANDWIDTH connection requests made by the LE Client that failed.

Failed Best-Effort Connections
Number of BEST-EFFORT connection requests made by the LE Client that failed.

QoS Negotiation Applied
Number of times the QoS negotiation extension was applied. Parameters are negotiated if the LE Client receives the destination LE Client’s parameters in an LE_ARP_RESPONSE control message.

PCR Proposal (IBM) Applied
Number of times the IBM Peak Cell Rate Proposal was applied. This proposal recommends using specific rate parameters if signaling at 100 Mbps or 155 Mbps for BEST-EFFORT connections.

This allows other participating IBM products (for example, 25-Mbps ATM adapters) to reject a connection based on the signaled peak cell rates.

QoS Connections Accepted
Number of RESERVED-BANDWIDTH connections accepted by this LE Client.

Best-Effort Connections Accepted
Number of BEST-EFFORT connections accepted by this LE Client.

QoS Connections Rejected
Number of RESERVED-BANDWIDTH connection requests received by this LE Client that were rejected.

Best-Effort Connections Rejected
Number of BEST-EFFORT connection requests received by this LE Client that were rejected.

Rejected due to PCR Validation
Number of BEST-EFFORT connections rejected by the LE Client due to validation of Peak Cell Rate when the validate-pcr-of-best-effort-vccs parameter is TRUE.

Example:

```
LEC 1 QoS+ li stat

QoS Statistics: of Data Direct Calls Placed by the LEC
------------------------------------------------------
    Successful QoS Connections          = 0
    Successful Best-Effort Connections  = 1
    Failed QoS Connections              = 1
    Failed Best-Effort Connections      = 1
    Qos Negotiation Applied             = 0
    PCR Proposal (IBM) Applied          = 0

QoS Statistics: of Data Direct Calls Received by the LEC
--------------------------------------------------------
    QoS Connections Accepted            = 1
    Best-Effort Connections Accepted    = 0
    QoS Connections Rejected            = 0
    Best-Effort Connections Rejected    = 0
    Rejected due to PCR Validation      = 0

LEC 1 QoS+
```

tlv-information
Lists the IBM Traffic Information TLV that this LE Client registered with the LE Server. The TLV is registered only if the LE Client is participating in QoS Negotiation.

Example:

```
LEC 1 QoS+ list tlv

  Traffic Info TLV of the LEC (registered with the LES)
  =====================================================
    TLV Type .........................= 268458498
    TLV Length .......................= 24
    TLV Value:
           Maximum Reserved Bandwidth = 23584 cells/sec (10 Mbps)
           Data Direct VCC Type...... = RESERVED BANDWIDTH VCC
           Data Direct VCC PCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC SCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC QoS Class  = 4
           Maximum Burst Size         = 95 cells (1 frames)

LEC 1 QoS+
```

vcc-information
Lists all active VCCs of the LE Client. The information includes the traffic parameters of the connections. For BEST-EFFORT connections, the

Sustained Cell Rate is displayed to be the same as the Peak Cell Rate, QoS Class and the Maximum Burst Size are displayed as 0.

The Parameter Descriptor entries are:

SrcParms
Parameters of a connection established by this LE Client.

DestParms
Parameters of a connection received by this LE Client.

NegoParms
Parameters of a connection established by the LE Client for which the QoS Negotiation was used.

RetryParms
Parameters of a connection established by this LE Client after failing at least once.

Example:

```
LEC 1 QoS+ li vcc

                             LEC VCC Table
                             =============

                                                                  Burst
Conn   Conn                 Conn          VCC    PCR    SCR   QoS   Size    Parameters
Index  Handle VPI   VCI   Type  Status  Type  (kbps) (kbps) Class (cells) Descriptor
------------------------------------------------------------------------------------
   2)     69    0   535  Cntrl  Ready  BstEft 155000 155000    0      0   SrcParms
   3)     71    0   537  Cntrl  Ready  BstEft      0      0    0      0   DestParms
   4)     72    0   538  Mcast  Ready  BstEft 155000 155000    0      0   SrcParms
   5)     74    0   540  Mcast  Ready  BstEft      0      0    0      0   DestParms
   6)     78    0   544  Data   Ready  ResvBW  25000   7000    1     95   DestParms

LEC 1 QoS+
```

Part 3. Token-Ring and Ethernet Interfaces

Chapter 23. Configuring and Monitoring LLC Interfaces

This chapter describes how to configure specific LLC interfaces in the router by using either the interface commands or the GWCON interface command.

Logical Link Level can be thought of as a “sub-protocol”. It is not accessed directly from either the Talk 6 (configuration) or the Talk 5 (monitoring) environment. Instead, it is accessed from the Token Ring protocol by entering an **LLC** command.

This chapter includes the following sections:

- “Accessing the Interface Configuration Process”
- “Accessing the Interface Monitoring Process” on page 302
- “LLC Monitoring Commands” on page 302
- “LLC Configuration Commands”

Accessing the Interface Configuration Process

Access the configuration commands for the protocol you wish to configure over LLC:

- Token Ring, as described in “Chapter 24. Configuring IEEE 802.5 Token-Ring Network Interfaces” on page 311

Each of these prompt levels has an LLC command. Enter **LLC** to access the LLC configuration commands and perform LCC configuration. When you are finished, enter **Exit** to return to the prompt level for the protocol you are configuring.

LLC Configuration Commands

LLC configuration is required when you need to pass packets over an SNA network. To enter these commands, you must first enter the LLC configuration environment (see “Accessing the Token-Ring Interface Configuration Process” on page 311).

This section summarizes and then explains all of the LLC configuration commands. These commands, shown in Table 42, enable you to configure LLC when you need to pass packets over a SNA network.

Table 42. LLC Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
List	Displays the selected LLC configuration.
Set	Sets the timers associated with LLC, and the size of the transmit and receive windows.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

List

Use the **list** command to display the current configuration for the LLC.

Syntax:

list

Example:

```
list
Reply Timer (T1):                 1 seconds
Receive ACK Timer (T2):           100 milliseconds
Inactivity Timer (Ti):            30 seconds
Max Retry value (N2):             8
Rcvd I-frames before ACK (N3):    1
Transmit Window (Tw):             2
Receive Window (Rw):              2
Acks needed to increment Ww (Nw): 1
```

Reply Timer (T1)

This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station.

Receive ACK Timer (T2)

This timer is used to delay sending of an acknowledgment for a received I-format frame.

Inactivity Timer (Ti)

This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 retry count is exceeded. Default is 30 seconds.

Max Retry value (N2)

The maximum number of retries by the LLC protocol. Default is 8.

Rcvd I-frames before ACK (N3)

This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. This counter sets a specified value and decrements each time an I-frame is received. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1.

Receive Window (Rw)

Indicates the maximum number of unacknowledged sequentially numbered I-frames that an LLC can receive from a remote host.

Transmit Window (Tw)

Indicates the maximum number of I-frames that can be sent before receiving an RR.

Acks needed to increment Ww (Nw)

This field is set to a default value of 1.

Set

Use the **set** command to configure the LLC.

Attention: Changing LLC parameters from the defaults can affect how the LLC protocol works.

Syntax:

set n2-max-retry *count*

n3-frames-rcvd-before-ack *count*

nw-acks-to-inc-window *count*

rw-receive-window *count*

t1-reply-timer *seconds*

t2-receive-ack-timer *seconds*

ti-inactivity-timer *seconds*

tw-transmit-window *count*

n2-max-retry

The maximum number of retries by LLC protocol. For example, N2 is the maximum number of times the LLC transmits an RR without receiving an acknowledgment when the inactivity timer expires. Default is 8. Minimum is 1. Maximum is 127.

Example:

```
set n2-max-retry
Max Retry value (N2) [8]?
```

n3-frames_rcvd-before-ack

This value is used with the T2 timer to reduce acknowledgment traffic for received I-frames. Set this counter to a specified value. Each time an I-frame is received, this value decrements. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1. Minimum is 1. Maximum is 255.

Example:

```
set n3-frames_rcvd-before-ack
Number I-frames received before sending ACK(N3) [1]?
```

rw-receive-window

Indicates the maximum number of unacknowledged sequentially numbered I-frames that an LLC can receive from a remote LLC peer. This value must be equal to or less than 127.

Example:

```
set rw-receive-window
Receive Window (Rw), 127 Max. [2]?
```

nw-acks-to-inc-ww

This field is set to a default value of 1.

t1-reply-timer

This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station. When this timer expires, an RR is sent with the poll bit set and T1 is started again. If the LLC receives no response after the configured maximum number of retries (N2), the link underneath is declared inoperative. Default is 1. Minimum is 1. Maximum is 256.

Example:

```
set t1-reply-timer
Reply Timer (T1) in sec. [1]?
```

t2-receive-ack-timer

This timer is used to delay sending of an acknowledgment for a received I-format frame. This timer is started when an I-frame is received. The timer is reset when an acknowledgment is sent. If this timer expires, LLC2 sends an acknowledgment as soon as possible. Set this value so that it is less than that of T1. This insures that the remote LLC2 peer receives the delayed acknowledgment before the T1 timer expires. Default is 1 (100 ms). Minimum is 1. Maximum is 2560.

Example:

```
set t2-receive-ack-timer
Receive Ack timer (T2) in 100 millisec. [1]?
```

Note: If this timer is set to 1 (the default) it will not run (for example, **n3-frames_rcvd-before-ack** =1).

ti-inactivity-timer

This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 retry count is exceeded. Default is 30 seconds. Minimum is 1 second. Maximum is 256 seconds.

Example:

```
set ti-inactivity-timer
Inactivity Timer (Ti) in sec. [30]?
```

tw-transmit-window

Sets the maximum number of I-frames that can be sent before receiving an RR. Assuming that the other end of the LLC session can actually receive this many consecutive I-frames, and the router has enough heap memory to keep copies of these frames until an acknowledgment is received, increasing this value may increase the throughput. Default is 2. Minimum is 1. Maximum is 127.

Example:

```
set tw-transmit-window
Transmit Window (Tw), 127 Max. [2]?
```

Accessing the Interface Monitoring Process

Access the monitoring commands for the protocol you wish to monitor over LLC:

- Token Ring, as described in “Chapter 24. Configuring IEEE 802.5 Token-Ring Network Interfaces” on page 311

Each of these prompt levels has an LLC command. Enter **LLC** to access the LLC monitoring commands to monitor LCC. When you are finished, enter **Exit** to return to the prompt level for the protocol you are monitoring.

LLC Monitoring Commands

This section summarizes and then explains all of the LLC monitoring commands. These commands, shown in Table 43, let you monitor the LLC while passing packets over an SNA network.

Table 43. LLC Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Clear-counters	Clears all statistical counters.
List	Displays interface, SAP, and session information.

Table 43. LLC Monitoring Command Summary (continued)

Command	Function
Set	Allows the user to dynamically configure LLC parameters that are valid for the life of the session.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Clear-Counters

Use the **clear-counters** command to clear all the LLC statistical counters.

Syntax:

clear-counters

List

Use the **list** command to display interface, service access point (SAP), and session information.

Syntax:

list interface

sap . . .

session

interface

Displays all SAPs opened on this interface.

Example:

```
list interface
SAP      Number of Sessions
F4       1
```

sap sap_number

Displays information for the specified SAP on the interface.

Example:

```
list sap
SAP value in hex (0FE) [1]? F4

Interface                      0, TKR/0
Reply Timer(T1)                1 sec
Receive ACK Timer (T2)         100 millisec
Inactivity Timer (Ti)          30 sec
MAX Retry Value (N2)           8
MAX I-field Size (N1)          2052
Rcvd I-frames before ACK (N3)  1
Transmit Window Size (Tw)      2
Acks Needed to Inc Ww (Nw)     1

Frame                          Xmt   Rcvd
UI-frames                      4     5
TEST-frames                    0     1
XID-frames                     0     0
I-frames                       291   26
RR-frames                      81    291
RNR-frames                     0     0
REJ-frames                     0     0
SABME-frames                   1     0
UA-frames                      0     1
DISC-frames                    0     0
DM-frames                      0     0
FRMR-frames                    0     0
I-frames discarded by LLC            0
I-frames Refused by LLC user         0
```

```
Cumulative number of sessions        1
Number of active sessions            1

Session ID                                          Remote
(int-sap-id)   Local MAC           Remote MAC         SAP   State
00F40000     00:00:C9:08:41:DB   10:00:5A:F1:02:37   F4    OPENED
```

SAP value in hex (0FE)
The SAP value of the session.

Interface
The interface number and type over which the session is running.

Reply Timer (T1)
Indicates the time it takes for this timer to expire when the LLC fails to receive an acknowledgment or response from the other LLC station.

Receive ACK Timer (T2)
Indicates the time delay the LLC uses before sending an acknowledgment for a received I-frame.

Inactivity Timer (Ti)
Indicates the time the LLC waits during inactivity before issuing an RR.

MAX Retry Value (N2)
The maximum number of retries by the LLC protocol.

MAX I-field Size (N1)
Maximum amount of data (in bytes) allowed in the I-field of an LLC2 frame.

Rcvd I-frame before ACK (N3)
Indicates the value that is used with T2 timer to reduce acknowledgment traffic for received I-frames.

Transmit Window Size (Tw)
Indicates the maximum number I-frames that can be sent before receiving an RR.

Acks Needed to Inc Ww (Nw)
This field is set to a default value of 1.

Frames Xmt and Rcvd
Counter that displays the total number of frame types transmitted (Xmt) and (Rcvd).

I-frames discarded by LLC
Counter that displays the total number of I-frames discarded by the LLC, usually because the sequence number is out of sequence.

I-frames refused by LLC user
Counter that displays the number of I-frames discarded by the software above the LLC. For example, DLSw (Data Link Switching).

Cumulative number of sessions
The total number of sessions that were opened over this SAP.

Number of active sessions
The total number of currently active sessions that are running over the interface.

Session ID (int-sap-id)
The session ID for the monitoring interface.

Local MAC
The router’s LLC MAC address.

Remote MAC
The remote LLC’s MAC address.

Remote SAP
The remote SAP of the LLC connection.

Remote State
The finite state(s) that results from interaction between the LLC peers. There are 21 states that are described below.

Link_Closed
The remote LLC peer is not known to the local LLC peer and is considered as not existing.

Disconnected
The local LLC peer is known to the other peer. This LLC peer can send and receive XID, TEST, SABME, and DISC commands; and XID TEST, UA, and DM responses.

Link_Opening
The state of the local LLC peer after sending a SABME or UA in response to a received SABME.

Disconnecting
The state of the local LLC after sending a DISC command to the remote LLC peer.

FRMR_Sent
The local LLC peer has entered the frame reject exception state and has sent a FRMR response across the link.

Link_Opened
The local LLC peer is in the data transfer phase.

Local_Busy
The local LLC peer is unable to receive additional I-frames.

Rejection
A local LLC peer that has received one or more out-of-sequence I-frames.

Checkpointing
The local LLC peer has sent a poll to the remote LLC peer and is waiting for an appropriate response.

CKPT_LB
A combination of checkpointing and local busy states.

CKPT_REJ
A combination of the checkpointing and rejection states.

Resetting
The local LLC peer has received a SABME and is reestablishing the link.

Remote_Busy
The state that occurs when an RNR is received from the remote LLC peer.

LB_RB
A combination of local_busy and remote_busy states.

REJ_LB
A combination of rejection and local_busy states.

REJ_RB

A combination of rejection and remote_busy states.

CKPT_REJ_LB

A combination of checkpointing, rejection, and local_busy states.

CKPT_CLR

A combination state resulting from the termination of a local_busy condition while the LLC peer is CKPT_LB.

CKPT_REJ_CLR

A combination state resulting from the transfer of an unconfirmed local busy clear while the link station is in the CKPT_REJ_LB state.

REJ_LB_RB

A combination of the rejection, local_busy, and remote_busy states.

FRMR_Received

The local LLC peer has received an FRMR response from the remote LLC peer.

Session

Displays information on the specified LLC session that is open on the interface.

Example:

```
list session
Session Id: [0]? 00-F4-0000

Interface0,                    TKR/0
Remote MAC addr                10:00:5A:F1:02:37
Source MAC addr                00:00:C9:08:35:47
Remote SAP                     F4
Local SAP                      F4
RIF                            (089E 0101 0022 0010)
Access Priority                0
State                          LINK_OPENED
Replay Timer                   1 sec
Receive ACK Timer (T2)         100 millisec
Inactivity Timer (Ti)          30 sec
MAX I-field Size (N1)          2052
MAX Retry Value (N2)           8
Rcvd I-frames before ACK (N3)  1
Transmit Window Size (Tw)      2
Working Transmit Size (Ww)     2
Acks Needed to Inc Ww (Nw)     1
Current Send Seq (Vs)          9
Current Rcv Seq (Vr)           7
Last ACK'd sent frame (Va)     9
No. of frames in ACK pend q    0
No. of frames in Tx pend q     0
Local Busy                     NO
Remote Busy                    NO
Poll Retry count               8
Appl output flow stopped       NO
Send process running           YES

Frame                           Xmt   Rcvd
I-frames                        1456  2678
RR-frames                       502   403
RNR-frames                      0     0
REJ-frames                      0     0
I-frames discarded by LLC             0
I-frames Refused by LLC user          0
```

Session Id

Indicates the session ID number.

Interface

Indicates the number of the interface over which this session is running.

Remote MAC addr

Indicates the MAC address of the remote LLC peer.

Source MAC addr
Indicates the MAC address of the local LLC.

Remote SAP
The remote side SAP of the LLC connection.

Local SAP
The local side SAP of the LLC connection.

RIF The actual RIF of the frame.

Access Priority
Priority of the packet. 07 for upper layer control.

State The finite state(s) that results from interaction between the LLC peers. Refer to the **list sap** command on page 303 for more information.

Receive ACK timer (T2)
Indicates the time delay the LLC uses before sending an acknowledgment for a received I-frame.

Inactivity timer (Ti)
Indicates the time the LLC waits during inactivity before issuing an RR.

MAX I-field size (N1)
Maximum size of the data field (in bytes) of a frame. Default is the size of the interface.

MAX Retry Value (N2)
The maximum number of times the LLC transmits an RR without receiving an acknowledgment

Rcvd I-frames before ACK (N3)
Indicates the value that is used with T2 timer to reduce acknowledgment traffic for received I-frames.

Transmit window size (Tw)
Indicates the maximum number of I-frames that can be sent before receiving an RR.

Working transmit size (Ww)
The maximum number of I-frames that are sent before receiving an RR.

Acks Needed to Inc Ww (Nw)
This field is set to a default value of 1.

Current send seq (Vs)
Send state variable (Ns value for the next I-frame to be transferred).

Current Rcv seq (Vr)
Receive state variable (next in-sequence Ns to be accepted).

Last ACK'd sent frame (Va)
Acknowledged state variable (last valid Nr received).

No. of frames in ACK pend q
Number of transmitted I-frames waiting for acknowledgment.

No. of frames in transmit pend q
Number of frames waiting to be transmitted.

Local Busy
The local side of the LLC connection is sending RNRs.

Remote Busy
The remote side of the LLC is receiving RNRs.

Poll Retry count
Indicates the current value of the retry of the counter (counts down) in the LLC protocol.

Appl output flow stopped
The LLC has told the application to stop giving it outgoing data frames.

Send process running
This process runs concurrently with all other frame actions and takes I-frames in the transmit queue and sends them.

Frames Xmt and Rcvd
Displays the total number of frame types transmitted (Xmt) and (Rcvd).

I-frames discarded by LLC
Counter that displays the total number of I-frames discarded by the LLC, usually because the sequence number is out of sequence.

I-frames refused by LLC user
Counter that displays the number of I-frames discarded by the software above the LLC. For example, DLSw (Data Link Switching).

Set

Use the **set** command to dynamically configure the LLC parameters on a current LLC session. Any changes that you make to the parameters are effective for the life of session. These parameters are the same as those listed in “Set” on page 300.

Attention: Changing LLC parameters from the default can affect how the LLC protocol works.

Syntax:

set	n2-max_retry *count*
	n3-frames-rcvd-before-ack *count*
	nw-acks-to-inc-ww *count*
	t1-reply-timer *seconds*
	t2-receive-ack-timer *seconds*
	ti-inactivity-timer *seconds*
	tw-transmit-window *seconds*

n2-max_retry
The maximum number of retries by LLC protocol. For example, N2 is the maximum number of times the LLC transmits an RR without receiving an acknowledgment when the inactivity timer expires. Default is 8. Minimum is 1. Maximum is 127.

n3-frames-rcvd-before-ack
This value is used with the T2 timer to reduce acknowledgment traffic for

received I-frames. Set this counter to a specified value. Each time an I-frame is received, this value is decremented. When this counter reaches 0 or the T2 timer expires, an acknowledgment is sent. Default is 1. Minimum is 1. Maximum is 255.

nw-acks-to-inc-ww

This field is set to a default value of 1.

t1-reply-timer

This timer expires when the LLC fails to receive a required acknowledgment or response from the other LLC station. When this timer expires, an RR is sent with the poll bit set and T1 is started again. If the LLC receives no response after the configured maximum number of retries (N2), the link underneath is declared inoperative. Default is 1. Minimum is 1. Maximum is 256.

t2-receive-ack-timer

This timer is used to delay sending of an acknowledgment for a received I-format frame. This timer is started when an I-frame is received and reset when an acknowledgment is sent. If this timer expires, LLC2 sends an acknowledgment as soon as possible. Set this value so that it is less than that of T1. This insures that the remote LLC2 peer receives the delayed acknowledgment before the T1 timer expires. Default is 1 (100 ms). Minimum is 1. Maximum is 2560.

Note: If this timer is set to 1 (the default) it will not run (for example, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer

This timer expires when the LLC does not receive a frame for a specified time period. When this timer expires the LLC transmits an RR until the other LLC responds or the N2 timer expires. Default is 30 seconds. Minimum is 1 second. Maximum is 256 seconds.

tw-transmit-window

Sets the maximum number of I-frames that can be sent before receiving an RR. Assuming that the other end of the LLC session can actually receive this many consecutive I-frames, and the router has enough heap memory to keep copies of these frames until an acknowledgment is received, increasing this value may increase the throughput. Default is 2. Minimum is 1. Maximum is 127.

Chapter 24. Configuring IEEE 802.5 Token-Ring Network Interfaces

Important

This chapter only applies for MSS Family Client installed in Token-Ring based LAN switches.

This chapter describes Token-Ring interfaces configuration and operational commands. It includes the following sections:

- "Accessing the Token-Ring Interface Configuration Process"
- "Token-Ring Configuration Commands"
- "Accessing the Interface Monitoring Process" on page 314
- "Token-Ring Interface Monitoring Commands" on page 314
- "Token-Ring Interfaces and the GWCON Interface Command" on page 315

Accessing the Token-Ring Interface Configuration Process

To display the `TKR config>` prompt, enter the network command followed by the interface number of the Token-Ring interface. For example:

```
Config>network 0
Token-Ring interface configuration
TKR Config>
```

Use the **list devices** command at the `Config>` prompt to display a list of interface numbers configured on the router.

Note: Whenever you change a parameter, you must restart the router for the changes to take effect.

Token-Ring Configuration Commands

This section describes the Token-Ring configuration commands. Enter the commands at the `TKR config>` prompt. Table 44 lists Token-Ring configuration commands.

Table 44. Token-Ring Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 22.
List	Displays the selected Token-Ring interface configuration.
LLC	Accesses the LLC configuration environment and subcommands.
Packet-size	Changes packet-size defaults for all Token-Ring networks.
Set	Sets the aging timer for the RIF cache and the physical (MAC) address.
Source-routing	Enables or disables source-routing on the interface.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 23.

List

Use the **list** command to display the current configuration for the Token-Ring interface.

Note: If the MAC address is 0, the default station address is used.

Syntax:

list

Example:

```
list
Token-Ring configuration:

    Packet size (INFO field): 2052

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
```

Packet size
Size of the Token-Ring packet.

RIF Aging Timer
Amount of time that the router holds the information contained in the Routing Information Field (RIF).

Source Routing
Status of the source-routing feature, enabled or disabled.

MAC Address
Configured MAC address that was set with the **set physical-address** command. If all zeros are displayed, the MAC address is the default address.

LLC

Use the **LLC** command to access the LLC configuration environment. See “LLC Configuration Commands” on page 299 for an explanation of each of these commands.

Syntax:

llc

Note: If APPN is not included in your router software load, you will receive the following message if you try to use this command:

```
LLC configuration is not available for this network.
```

The LLC configuration environment is only available if APPN is included in the software load.

Packet-Size

Use the **packet-size** command to change maximum packet-size for all Token-Ring networks. Enter the **packet-size** command followed by the desired number of bytes.

Syntax:

packet-size *bytes*

Table 45. Token-Ring 4/16 Valid Packet Sizes

Network Data Speed	Values (# of bytes)
4 Mbps	516 to 4498 **Note:** If a value greater than 4498 is defined for a 4 Mb TR then the software will set it to 4498. If the user does not specify a value, then the default is 2052.
16 Mbps	516 to 18144 **Note:** If you do not specify a value, then the default is 2052.

Note: If packet sizes are increased, buffer memory requirements will also increase.

Set

Use the **set** command to set the Routing Information Field (RIF) timer and the physical (MAC) address.

Syntax:

set physical-address

rif-timer

physical-address

Indicates whether you want to define a locally administered address for the Token-Ring interface’s MAC sublayer address, or use the default factory station address (indicated by all zeroes). The MAC sublayer address is the address that the Token-Ring interface uses to receive and transmit frames.

Note: Pressing **Return** leaves the value the same. Entering **0** and pressing **Return** causes the router to use the factory station address. The default is to use the factory station address.

Valid values: Any 12-digit hexadecimal address.

Default value: burned-in address (indicated by all zeroes).

Example:

```
set physical-address
MAC address in 00:00:00:00:00:00 form []?
```

rif-timer

Sets the maximum amount of time (in seconds) that the information in the RIF is maintained before it is refreshed. The default is 120.

Example:

```
set rif-timer
RIF aging timer value [120]?  120
```

Source-routing

Use the **source-routing** command to enable or disable end station source routing. Source routing is the process by which end stations determine the source route to use to cross source routing bridges. Source routing allows the IP, IPX, and AppleTalk Phase 2 protocols to reach nodes on the other side of the source routing bridge.

This switch is completely independent of whether this interface is providing source routing via the SRT forwarder. The default setting is enabled.

Some stations cannot properly receive frames with a Source Routing RIF on them. This is especially common among NetWare drivers. Disabling source routing in this situation will allow you to communicate with these stations.

Source routing should be enabled only if there are source-routing bridges on this ring that you want to bridge IP, IPX, and AppleTalk Phase 2 packets through. Source routing must also be enabled so LLC test response messages can be returned.

Syntax:

source-routing enable
disable

Accessing the Interface Monitoring Process

To display the Token-Ring monitoring prompt (TKR>), enter the network command followed by the interface number of the Token-Ring interface. For example:

```
+network 0
TKR>
```

Use the **list devices** command at the Config> prompt to display a list of interface numbers configured on the router.

Follow the procedure described in “Accessing the Network Interface Configuration Process” on page 28 to access the interface monitoring process for the interface described in this chapter. Once you have accessed the desired interface monitoring process, you can begin entering monitoring commands.

Token-Ring Interface Monitoring Commands

This section summarizes the Token-Ring monitoring commands. Enter commands at the TKR> monitoring prompt. Table 46 lists the monitoring commands.

Table 46. Token-Ring Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Dump	Displays a dump of the RIF cache.
LLC	Displays the LLC monitoring prompt.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Dump

When source routing is enabled in the tkr config> process, you can use the **dump** command to request a dump of the RIF cache contents.

Syntax:

dump

Example:

```
dump
MAC address    State     Usage   RIF
0000C90B1A57   ON_RING   Yes     0220
```

MAC address
Displays the MAC address of the Token-Ring interface.

State Displays one of the interface states:

On_ring - indicates that a RIF was found for a node on the ring.

Have_route - indicates that a RIF was found for a node on a remote ring.

No_route - is displayed for a brief period of time as an explorer frame is sent out and the router is waiting for a return.

Discovering - indicates that the router sent an explorer frame to rediscover the RIF.

St_route - indicates that a route obtained from a Spanning tree explorer.

Usage Indicates that a RIF was used in a packet. The number is arbitrary and has no functional significance.

RIF Displays a code that indicates the RIF in hexadecimal.

Note: The RIF is displayed only if Source Route Bridging is enabled on the Token-Ring interface.

LLC

Use the **LLC** command to access the LLC monitoring prompt. LLC commands are entered at this new prompt. See “LLC Monitoring Commands” on page 302 for an explanation of each of these commands.

Syntax:

llc

Token-Ring Interfaces and the GWCON Interface Command

While Token-Ring interfaces have their own monitoring processes for monitoring purposes, the router also displays complete statistics for installed network interfaces when you use the **interface** command from the GWCON environment.

Statistics Displayed for 802.5 Token-Ring Interfaces

The following statistics display when you enter the **interface *<net#>*** command for a Token-Ring interface from the GWCON environment.

```
Nt Nt' Interface      CSR  Vec     Passed     Failed      Failed

0  0   TKR/0      6000000   1C          1          0           0
Token-Ring/802.5  MAC/data-link on IBM Token-Ring interface
Microcode version: 000VL00A0 (050394)

Physical address        000C90820C7
Network speed           16 Mbps
```

```
Max packet size (INFO)  2052
Handler state           Ring open
Ring status             SERR | CO
Interface Restarts      0

# times Signal lost     0          # times Beaconing  0
Hard errors             0          Lobe wire faults   0
Auto-removal errors     0          Removes received   0
Ring recovery actions   0

Line errors             0          Burst errors       0
ARI/FCI errors          0          Inputs dropped     0
Frame copy errors       0          Token errors       0
Lost frames             0
```

The following section describes general interface statistics:

Nt Global interface number

Nt' Applies only to dial circuits

Interface
Interface name and Number of this interface within interfaces of type "intrfc"

CSR COMM and Status Registers address

Vec Interrupt vector

Self-Test: Pass
Number of times self-test succeeded

Self-Test: Fail
Number of times self-test failed

Maint: Fail
Number of maintenance failures

The following section describes the statistics displayed that are specific to the Token-Ring interfaces:

Physical address
Specifies the physical address of the Token-Ring interface.

Network speed
Specifies the speed of the Token-Ring network that connects to the interface. The Network Speed counter displays the number of packets that the interface can pass per second.

Max packet size (info)
Displays the maximum packet size configured for that interface. The Max Packet Size counter displays the maximum length, in bytes, of a packet that the interface transmits or receives. This counter is user-defined.

Handler state
Displays the current state of the Token-Ring handler. The Handler state counter displays the state of the handler after the self-test runs.

Ring status
Last Ring Status of the Token Ring interface.

SIGL SIGNAL_LOSS The interface has detected a loss of signal on the ring.

HERR HARD_ERROR The interface is presently transmitting or receiving beacon frames on the ring.

SERR SOFT_ERROR The interface has transmitted a report error MAC frame.

BEAC TRANSMIT_BEACON The interface is transmitting beacon frames to or from the ring.

LWF LOBE_WIRE_FAULT The interface has detected an open or short circuit in the cable between the interface and the wiring concentrator. The interface is closed and is at the state following initialization.

ARMV AUTO_REMOVAL_ERROR The interface has failed the lobe wrap test, which resulted from the beacon auto-removal process, and has removed itself from the ring. The interface has closed and is at the state following initialization.

RMVD REMOVED_RECEIVED The interface has received a remove ring station MAC frame request and has removed itself from the ring. The interface is closed and is at the state following initialization.

CO COUNTER_OVERFLOW One of the following error counters has incremented from 254 to 255: Line, ARI/FCI, Frame Copy, Lost Frames, Burst, Lobe wire faults, Removes received. This display shows these error counters.

SSTA SINGLE_STATION The interface has sensed that it is the only station on the ring.

RR RING_RECOVERY The interface observes claim Token MAC frames on the ring. The interface may be transmitting the claim Token frames. This status remains until the interface transmits a ring purge frame.

Interface Restarts
Specifies the number of times the Token Ring chip timed out, or the Token Ring driver received a bad command from the handler. For information about why a restart occurred, see messages TKR.37, TKR.38, TKR.39, TKR.40, and TKR.41. in *Event Logging System Messages Guide*

# of times signal lost
Specifies the total number of times that the router was unable to transmit a packet due to loss of signal.

Hard errors
Displays the number of times the interface transmits or receives beacon frames from the network.

Auto-removal errors
Displays the number of times the interface, due to the beacon auto-removal process, fails the lobe wrap test and removes itself from the network.

Ring recovery actions
Displays the number of times the interface detects claim token medium access control (MAC) frames on the network.

Line errors
The Line Errors counter increments when a frame is repeated or copied and the Error Detected Indicator (EDI) is zero for the incoming frame:

One of the following conditions must also exist:

- A token with a code violation exists.

- A frame has a code violation between the starting and ending delimiter.
- A Frame Check Sequence (FCS) error occurs.

ARI/FCI errors
The ARI/FCI (Address Recognized Indicator/Frame Copied Indicator) Errors counter increments if the interface receives either of the following:

An Active Monitor Present (AMP) MAC frame with the ARI/FCI bits equal to zero and a Standby Monitor Present (SMP) MAC frame with the ARI/FCI bits equal to zero.

More than one SMP MAC frame with the ARI/FCI bits equal to zero, without an intervening AMP MAC frame.

This error indicates that the upstream neighbor copied the frame but is unable to set the ARI/FCI bits.

Frame copy errors
Displays the number of times the interface in receive/repeat mode recognizes a frame addressed to its specific address but finds the address recognize indicator (ARI) bits not equal to zero. This error indicates a possible line hit or duplicate address.

Lost frames
Displays the number of times the interface is in transmit mode (stripping) and fails to receive the end of a transmitted frame.

# times beaconing
Displays the number of times the interface transmits a beacon frame to the network.

Lobe wire faults
Displays the number of times the network detects an open or short circuit in the cable between the interface and the wiring concentrator.

Removes received
Displays the number of times the interface receives a remove ring station MAC frame request and removes itself from the network.

Burst errors
Displays the number of times the interface detects the absence of transitions for five half-bit times between the start delimiter (SDEL) and the end delimiter (EDEL) or between the EDEL and the SDEL.

Inputs dropped
Displays the number of times an interface in repeat mode recognizes a frame addressed to it but has no buffer space available to copy the frame.

Token errors
The token errors counter increments when the active monitor detects a token protocol with any of the following errors:

The MONITOR_COUNT bit of token with nonzero priority equals one.

The MONITOR_COUNT bit of a frame equals one. No token or frame is received within a 10-ms window.

The starting delimiter/token sequence has a code violation in an area where code violations must not exist.

Chapter 25. Using the Ethernet Network Interface

Important

This chapter only applies for MSS Family Client installed in Ethernet-based LAN switches.

This chapter describes how to use the Ethernet interface. It includes “Displaying Ethernet Statistics through the Interface Command”.

Displaying Ethernet Statistics through the Interface Command

You can also use the **interface** command from the GWCON environment to display the following statistics.

```
+ interface 0
                                Self-Test  Self-Test  Maintenance
Nt Nt′ Interface      CSR  Vec     Passed     Failed       Failed
0  0   Eth/0       81600   5E          1          1           0
Ethernet/IEEE 802.3 MAC/data-link on SCC Ethernet interface

Physical address         000093808000
PROM address             000093808000

Input statistics:
  failed, frame too long          0   failed, FCS error           0
  failed, alignment error         0   failed, FIFO overrun        0
  internal MAC rcv error          0   packets missed              0

Output statistics:
  deferred transmission           6   single collision            2
  multiple collisions             0   total collisions            2
  failed, excess collisions       0   failed, FIFO underrun       0
  failed, carrier sense err       0   SQE test error              0
  late collision                  0   internal MAC trans errors   0
RISC Microcode Revision:            1
```

These statistics have the following meaning:

Nt Global network number.

Nt′ This field is for the serial interface card. Disregard the output.

Interface
Interface name and its instance number.

CSR Command and status register address.

Vec Interrupt vector

Self-Test: Passed
Number of self-tests that succeeded.

Self-Test: Failed
Number of self-tests that failed.

Maintenance: Failed
Number of maintenance failures.

Physical address
The Ethernet address of the device currently in use. This may be the PROM address or an address overwritten by some other protocol.

PROM address
The permanent unique Ethernet address in the PROM for this Ethernet interface.

Interface restarts
The number of times the Ethernet chip timed out, or the Ethernet driver received a bad command from the handler. For information about why a restart occurred, refer to messages Eth.043 and Eth.044 in the *IBM Multiprotocol Switched Services Client Event Logging System Messages Guide*

Interface type
This specifies the connector type as AUI or RJ45.

Input statistics:

failed, packet too long or failed, frame too long
The Failed, Packet Too Long counter increments when the interface receives a packet that is larger than the maximum size of 1518 bytes for an Ethernet frame. This data is exported via SNMP as the dot3StatsFrameTooLongs counter.

failed, CRC error or failed, FCS (Frame Check Sequence) error
The Failed, CRC (Cyclic Redundancy Check) Error counter increments when the interface receives a packet with a CRC error. This data is exported via SNMP as the dd3StatsFCSErrors counter.

failed, framing error or failed, alignment error
The Failed, Framing Error counter increments when the interface receives a packet whose length in bits is not a multiple of eight.

failed, FIFO over-run or failed, FIFO overrun
The Failed, FIFO (First In, First Out) Overrun counter increments when the Ethernet chipset is unable to store bytes in the local packet buffer as fast as they come off the wire.

collision in packet
The counter increments when a packet collides as the interface attempts to receive a packet, but the local packet buffer is full. This error indicates that the network has more traffic than the interface can handle.

short frame
The counter increments when the interface receives a packet with a short frame.

buffer full warnings
The Buffer Full Warnings counter increments each time the local packet buffer is full.

packets missed
The Packets Missed counter increments when the interface attempts to receive a packet, but the local packet buffer is full. This error indicates that the network has more traffic than the interface can handle.

internal mac rcv errors
Receive errors that are not late, excessive, or carrier check collisions. This data is exported via SNMP as the dot3StatsInternalMacReceiveErrors counter. This statistic is the sum of the FIFO Overruns.

Output statistics:

initially deferred or deferred transmission
The Initially Deferred counter increments when the carrier sense

mechanism detects line activity causing the interface to defer transmission. This data is exported via SNMP as the dot3StatsDeferredTransmissions counter.

single collision
The Single Collision counter increments when a packet has a collision on the first transmission attempt, and then successfully sends the packet on the second transmission attempt. This data is exported via SNMP as the dot3StatsSingleCollisionFrames counter.

multiple collisions
The Multiple Collisions counter increments when a packet has multiple collisions before being successfully transmitted. This data is exported via SNMP as the dot3MultipleCollisionFrames counter.

total collisions
The Total Collisions counter increments by the number of collisions a packet incurs.

failed, excess collisions
The Failed, Excess Collisions counter increments when a packet transmission fails due to 16 successive collisions. This error indicates a high volume of network traffic or hardware problems with the network. This data is exported via SNMP as the dot3StatsExcessiveCollisions counter.

failed, FIFO underrun
The Failed, FIFO Underrun counter increments when packet transmission fails due to the inability of the interface to retrieve packets from the local packet buffer fast enough to transmit them onto the network.

failed, carrier check or failed, carrier sense error
The Failed, Carrier Check counter increments when a packet collides because carrier sense is disabled. This error indicates a problem between the interface and its Ethernet transceiver. This data is exported via SNMP as the dot3StatsCarrierSenseErrors counter.

CD heartbeat error or SQE test error
The CD (Collision Detection) Heartbeat Error or SQE (Signal Quality Error) counter increments when the interface sends a packet but detects that the transceiver has no heartbeat. The packet is treated as successfully transmitted because some transceivers do not generate heartbeats. This data is exported via SNMP as the dot3StatsSQETestErrors counter.

internal mac tx errors or internal MAC trans errors
Transmit errors that are not late, excessive, or carrier check collisions. This data is exported via SNMP as the dot3StatsInternalMacTransmitErrors counter. This statistic is the sum of the FIFO Underruns.

RISC Microcode Version:
This gives the version of the microcode running in the RISC controller of the communications processor module.

Chapter 26. Configuring and Monitoring the Ethernet Network Interface

This chapter describes Ethernet interface configuration and operational commands. It includes the following sections:

- "Accessing the Ethernet Interface Operating Process" on page 325
- "Ethernet Interface Monitoring Commands" on page 325

Accessing the Ethernet Interface Configuration Process

Use the following procedure to access the configuration process. This process gives you access to an Ethernet interface's *configuration* process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to "What is the OPCON Process?" on page 69.) For example:

   ```
   * talk 6
   Config>
   ```

   The CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the router is currently configured.
3. Record the interface numbers.
4. Enter the **network** command and the number of the Ethernet interface you want to configure. For example:

   ```
   Config> network 0
   ETH Config>
   ```

   The Ethernet configuration prompt (`ETH Config>`), is displayed.

Ethernet Configuration Commands

This section summarizes and then explains the Ethernet configuration commands. Enter the commands at the `ETH config>` prompt.

Table 47. Ethernet Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 22.
Connector-Type	Sets the connector type.
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type X'0800') or IEEE (802.3 with SNAP).
List	Displays the current connector-type, NetWare IPX encapsulation, and IP encapsulation.
Physical-Address	Sets the physical MAC address.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 23.

Connector-Type

Use the **connector-type** command to set the connector type. MSS Family Clients ignore this command.

Syntax:

connector-type *name*

IP-Encapsulation

Use the **IP-encapsulation** command to select Ethernet (Ethernet type X'0800') or IEEE 802.3 (Ethernet 802.3 with SNAP). Enter **e** or **i**.

Syntax:

ip-encapsulation *type*

List

Use the **list** command to display the current configuration for the Ethernet interface including the connector-type, IPX encapsulation type, and IP encapsulation type.

Syntax:

list all

Example:

```
list all

Connector type:          AUI (10BASE5)
MAC Address:             12:15:00:FA:00:FE
```

Physical-Address

Use the **physical-address** command to set the physical (MAC) address.

Syntax: physical-address ***address***

physical-address

This command lets you indicate whether you want to define a locally administered address for the Ethernet interface's MAC sublayer address, or use the default burned-in address (indicated by all zeros). The MAC sublayer address is the address that the Ethernet interface uses to receive and transmit frames.

Note: Pressing **Enter** leaves the value the same. Entering **0** causes the router to use the burned-in address. The default is to use the burned-in address.

Valid Values: Any 12-digit hexadecimal address.

Default Value: burned-in address (indicated by all zeros).

Example:

```
physical-address

MAC address in 00:00:00:00:00:00 form []? 12:15:00:FA:00:FE
```

Accessing the Ethernet Interface Operating Process

To monitor information related to the Ethernet Network Interface, access the interface monitoring process by doing the following:

1. At the OPCON prompt, enter **talk 5**. For example:

   ```
   * talk 5
   ```

   The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Return** again.

2. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the router is configured. For example:

   ```
   + configuration
   ```

   See page “Configuration” on page 120 for sample output of the **configuration** command.

3. Enter the **network** command and the number of the Ethernet interface. In this example:

   ```
   + network 0
   ETH>
   ```

   The Ethernet monitoring prompt is displayed. You can now view information about the Ethernet interface by entering monitoring commands.

Ethernet Interface Monitoring Commands

This section summarizes and explains the Ethernet monitoring commands. Enter commands at the ETH> prompt. Table 48 lists the monitoring commands.

Table 48. Ethernet monitoring command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 22.
Collisions	Displays collision statistics for the specified Ethernet interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 23.

Collisions

This command shows the counts of transmissions for packets that incurred collisions before successful transmission. Counters are given for packets sent after the collision XXXXx packets sent after 15 collisions. Increasing numbers of packets transmitting with collisions and higher numbers of collision per packet are signs of transmitting onto a busy Ethernet.

These counters are cleared by the OPCON **clear** command. This data is exported via SNMP as the dot3CollTable counter.

Syntax:

collisions

Example:

```
Eth> coll
Transmitted with  1 collisions:0
Transmitted with  2 collisions:0
Transmitted with  3 collisions:0
Transmitted with  4 collisions:0
Transmitted with  5 collisions:0
Transmitted with  6 collisions:0
Transmitted with  7 collisions:0
Transmitted with  8 collisions:0
Transmitted with  9 collisions:0
Transmitted with 10 collisions:0
Transmitted with 11 collisions:0
Transmitted with 12 collisions:0
Transmitted with 13 collisions:0
Transmitted with 14 collisions:0
Transmitted with 15 collisions:0
```

Part 4. Appendixes

Appendix A. Quick Configuration Reference

> **Important**
>
> If you are attempting to configure or monitor your IBM MSS Family Client and your service terminal is unreadable, see "Service Terminal Display Unreadable" in IBM Multiprotocol Switched Services Family Client Service and Maintenance Manual.

Quick Configuration Tips

Making Selections

On the panels that you view when using the Quick Configuration program, the information shown in brackets, `[ ]`, is the default. For example:

```
Configure Bridging? (Yes, No, Quit): [Yes]
```

- To use the default `Yes`, press **Enter**.
- To use a value other than the default, such as `No` or `Quit`, choose from the values in the parentheses.
- If no value appears in the brackets, there is no default and you must type a value.

Exiting and Restarting

- To restart the current Quick Configuration section at any time, type **r**. For example, if you are in the Interface Configuration section, type **r** and press **Enter** to return to the beginning of that section.
- To exit Quick Configuration, type **q** and press **Enter**. The `Config>` prompt will appear.
- To restart Quick Configuration from the `Config>` prompt, type **qc** and press **Enter**.

When You're Done

- Once you have completed your configuration, you must restart the IBM MSS Family Client for the configuration to take effect. At the end of the Quick Configuration program, you are given this option.

Starting the Quick Configuration Program

The following sections describe sample configurations using the Quick Configuration program (**qconfig**).

To start the quick configuration program, enter **qc** at the `Config>` prompt.

The program displays the following panel after starting.

```
Router Quick Configuration
for the following:

o   LAN Emulation
        LAN Emulation Client (LEC)
o   Bridging
        Source Routing Bridge (SRB)
o   Protocols
        IP (including OSPF, RIP, and SNMP)
        IPX

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note: Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
```

Event logging records system activity, status changes, data transmission and reception, data and internal errors, and service requests. The logging level is set to standard (the default). For more information about error logging, refer to the *Event Logging System Messages Guide*.

During Quick Configuration you can:

1. Configure LAN Emulation Clients
2. Configure bridging
3. Configure protocols
4. Restart the router

Configuring LAN Emulation

If you added an ATM device, you will see the following prompts:

```
**********************************************************
LAN Emulation Configuration
**********************************************************

Type 'Yes' to Configure LAN Emulation
Type 'No' to skip LAN Emulation Configuration
Type 'Quit' to exit Quick Config

Configure LAN Emulation? (Yes, No, Quit): [Yes]
```

You can configure either Token-Ring or Ethernet LAN Emulation clients from this question.

Configuring Bridging

```
**********************************************
Bridging Configuration
**********************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes]
```

1. In response to `Configure Bridging`, take one of the following actions:
   - Enter **y** to display the bridging configuration prompts. The prompts that appear depend on your network configuration.

- Enter **n** to skip the bridging configuration and continue with quick configuration.
- Enter **q** to exit quick configuration. This displays the `Config>` prompt. To reenter quick configuration, enter **qc** after this prompt.

2. Enter a bridge number, which is a hexadecimal value from 1 to F that is unique between two parallel segments.

```
Interface 0 (Port 1) is of type Token Ring
Configure Source Routing on this interface (Yes, No): [Yes]
```

3. Enter **y** to configure source routing on the interface. The console displays the next two lines.

```
Configuring Interface 0 (Port 1)
Segment Number (hex) of this Interface (1-FFF): [A1]
```

Note: The port number increases by one because source routing bridging does not allow a port number of zero.

A unique hexadecimal value from 1 to FFF is assigned to each interface. The interfaces on each ring (segment) have the same segment number, but the segment number is unique to each ring.

These prompts appear for each Token Ring interface.

```
Interface 1 (Port 2) is of type Token Ring
Configure Source Routing on this interface? (Yes, No): [Yes]
Configuring Interface 1 (Port 2)
Segment Number (hex) of this Interface (1-FFF): [A2]
```

If more than two interfaces are configured for source routing, enter a unique hexadecimal value from 1 to FFF unique for the internal virtual segment.

```
Virtual Segment Number (hex) of this Router (1-FFF): [A4]
```

4. A panel similar to the following is displayed:

```
This is all configured bridging information:

The Source Routing part of SRT Bridging has been enabled

Bridge Number of this Router: A

Interfaces configured for Source Routing:

       Interface #     Port#      Segment #   Interface Type

           0             1          A1        Token Ring
           1             2          A2        Token Ring
           2             3          A3        Token Ring

Virtual Segment Number of this Router:  A4

Save this Configuration? (Yes, No): [Yes]
```

5. Enter **y** to save the bridging configuration and continue with quick configuration. Enter **n** to re-display the bridging configuration prompts.

If you enter **y**, the following message appears:

```
Bridging configuration saved
```

Configuring Protocols

After you save the bridging configuration, you will see the following panel:

```
**********************************************
Protocol Configuration
**********************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
```

Take one of the following actions:

- Enter **y** to configure the protocols.
- Enter **n** to skip protocol configuration and continue with quick configuration.
- Enter **q** to exit quick configuration.

You will first configure IP, and then IPX.

Configuring IP

When you answer **y** to the Configure Protocol panel, quick configuration displays the following messages:

```
Type 'r' any time at this level to restart Protocol configuration

Configure IP? (Yes, No): [Yes]
```

1. Take one of the following actions:
   - Enter **y** to configure IP.
   - Enter **n** to skip IP configuration and continue with quick configuration.

The following lines appear for each interface.

```

Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [ ] 128.185.141.1
Address Mask: [255.255.0.0]
```

2. Enter the IP address in decimal notation for example, 128.185.142.20. The console displays one of the following error messages if you enter an invalid IP address:

   ```
   Bad address, please try again.

   This address has already been assigned.  Enter a different address
   ```

   Address mask is a decimal value that reflects the IP network or subnetwork to which this interface is attached.

For more information about IP addressing or address masks, refer to the *Protocol Configuration and Monitoring Reference*, or consult your network administrator.

```
Per-Interface IP Configuration complete

Configuring IP Routing Information
Enable Dynamic Routing (Yes, No): [Yes]
```

3. Enter **y** if you want the routing protocols (RIP or OSPF) to build the routing tables. Enter **n** to manually add IP address destinations to the routing tables (static routes).

```
Enable OSPF? (Yes, No): [Yes]
```

4. Enter **y** to enable the OSPF routing protocol as the primary dynamic IP routing protocol. RIP will be enabled only to send advertisements, not to receive them. Enter **n** if you do not want to use OSPF. RIP will be enabled to send and receive advertisements.

```
OSPF Enabled with Max routes = 1000  and Max routers = 50
```

Max routes is the maximum number of autonomous system (AS) external routes imported into the OSPF routing domain. Max routers is the maximum number of OSPF routers in the routing domain.

```
Routing Configuration Complete

SNMP will be configured with the following parameters:

Community: public
Access:    READONLY

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No):  [Yes]


This is the information you have entered:

          Interface #        IP Address     Address Mask

             0               128.185.141.1  255.255.255.0
             1               128.185.142.1  255.255.255.0
             2               128.185.143.1  255.255.255.0

OSPF is configured, and RIP is configured only for 'sending'

SNMP has been configured with the following parameters:

     Community: public
     Access:    read_trap

     Community: dana
     Access:    read_write_trap

Save this configuration? (Yes, No): [Yes]
```

5. Enter **y** to save the IP configuration and continue with quick configuration. Enter **n** to re-display the protocol configuration prompts.

Configuring IPX

After you save the IP configuration, you will see the following messages:

```
Configure IPX? (Yes, No): [Yes]
```

1. Enter **y** to configure IPX. Enter **n** to skip IPX configuration and continue with quick configuration.

   You will see messages similar to the following:

   ```
   Type 'r' any time at this level to restart IPX Configuration
   IPX Configuration is already present
   Configure IPX anyway? (Yes, No): [No] yes
   ```

2. Enter **y** to replace the existing configuration. Enter **n** to keep the current configuration and continue.

```
Configuring Per-Interface IPX Information

Configuring Interface 0 (Token Ring)
Configure IPX on this interface? (Yes, No): [Yes]
```

3. The next messages and your responses depend on whether you are configuring Token-Ring or Ethernet.

   Configuring IPX for Token-Ring:

   a. The following prompt is displayed:

      ```
      Token Ring encapsulation (frame) type? (TOKEN–RING MSB, TOKEN–RING LSB,
          TOKEN–RING_SNAP MSB, TOKEN–RING_SNAP LSB): [TOKEN–RING MSB]
      ```

   b. Enter the encapsulation type used by the IPX protocol on your Token-Ring end stations.

`Token–Ring MSB:` Most common encapsulation type and the default. The IBM MSS Family Client builds outgoing packets with a 3-byte 802.2 header, (0xE0, 0xE0, 0x03). It sends the source and destination addresses in MSB (most significant bit), or noncanonical, format, which is the native address format for Token-Ring.

`Token–Ring LSB` Same as Token-Ring MSB except the IBM MSS Family Client sends the addresses in LSB (least significant bit), or canonical, format.

`Token-Ring SNAP MSB` The IBM MSS Family Client builds outgoing packets with an 8-byte 802.2/SNAP header (0xAA, 0xAA, 0x03, 0x00, 0x00, 0x00, 0x81, 0x37). It sends the source and destination addresses in most significant bit (MSB), or noncanonical, format.

`Token-Ring SNAP LSB` Same as Token-Ring SNAP MSB except the IBM MSS Family Client sends the addresses in LSB, or canonical, format.

   Configuring IPX for Ethernet:

   a. The following prompts are displayed:

      ```
      Ethernet encapsulation type? (ETHERNET_8022, ETHERNET_8023, ETHERNET_ii,
      ETHERNET_SNAP): [ETHERNET_8023]
      ```

   b. Enter the encapsulation type used by the IPX protocol on your Ethernet end stations.

`Ethernet_8022` Packet includes an 802.2 header.

`Ethernet_8023` Uses an IEEE 802.3 packet format without the 802.2 header. This is the default and the default for NetWare versions prior to 4.0. Ethernet 802.3 does not conform to the IEEE 802 standards because it does not include an 802.2 header. It may cause problems with other nodes on the network.

`Ethernet_II` Uses Ethernet type 8137 as the packet format. This format is required if you are using NetWare VMS on the Ethernet. This is the default for NetWare Versions 4.0 and higher.

`Ethernet_SNAP` Uses the 802.2 format with a SNAP header. This encapsulation type is meant to be compatible with token-ring SNAP encapsulation. However, it violates IEEE standards and is not interoperable across conformal bridges.

4. Assign an IPX network number to the associated directly connected network. Every IPX interface must have a unique network number.
5. Host number is a unique 12-digit hexadecimal value assigned to an IPX router. It is required because serial lines do not have hardware node addresses from which to build a host number.

```
This is the information you have entered:

               Per-Interface Configuration Information

Cir   Ifc   IPX Net(hex)   Encapsulation       IPXWAN

1     1     10             ETHERNET_8023       Not Configured
2     3     300                                Not Configured
3     5     400                                Not Configured
4     6     600                                Enabled


  Host Number for Serial Lines: 0002210A0000
  IPXWAN Node ID = 2210A
  IPX Router Name = ipxwan_router-2210A


Save this configuration? (Yes, No): [Yes]
```

6. Enter **y** to save the IPX configuration and continue with quick configuration. Enter **n** to re-display the IPX configuration prompts.

   If you enter **y**, the following message appears:

```
IPX configuration saved
```

Restarting the IBM MSS Family Client

After configuring the protocols, you will receive the following message:

```
Quick Config Done
Do you want to write this configuration? (Yes, No): [Yes]
```

Enter **y** to save your changes and display the following information:

```
Default config file written successfully.

Configuration was written.
The system must be restarted for this configuration to take effect.
```

Enter **reload** at the OPCON prompt (*) to restart the IBM MSS Family Client with the new configuration. To change or view the current configuration, enter **qc**.

Appendix B. Abbreviations

AAL	ATM Adaptation Layer
AAL-5	ATM Adaptation Layer 5
AARP	AppleTalk Address Resolution Protocol
ABR	area border router
ack	acknowledgment
AIX	Advanced Interactive Executive
AMA	arbitrary MAC addressing
AMP	active monitor present
ANSI	American National Standards Institute
AP2	AppleTalk Phase 2
APPN	Advanced Peer-to-Peer Networking
ARE	all-routes explorer
ARI	ATM real interface
ARI/FCI	address recognized indicator/frame copied indicator
ARP	Address Resolution Protocol
AS	autonomous system
ASBR	autonomous system boundary router
ASCII	American National Standard Code for Information Interchange
ASN.1	abstract syntax notation 1
ASRT	adaptive source routing transparent
ASYNC	asynchronous
ATCP	AppleTalk Control Protocol
ATM	Asynchronous Transfer Mode
ATMARP	ARP in Classical IP
ATP	AppleTalk Transaction Protocol
AUI	attachment unit interface
AVI	ATM virtual interface
ayt	are you there
BAN	Boundary Access Node
BBCM	Bridging Broadcast Manager
BCM	BroadCast Manager
BECN	backward explicit congestion notification
BGP	Border Gateway Protocol
BGP	Border Growth Protocol

BNC	bayonet Niell-Concelman
BNCP	Bridging Network Control Protocol
BOOTP	BOOT protocol
BPDU	bridge protocol data unit
bps	bits per second
	bandwidth reservation
BSD	Berkeley software distribution
BTP	BOOTP relay agent
BTU	basic transmission unit
BUS	Broadcast and Unknown Server
CAM	content-addressable memory
CCITT	Consultative Committee on International Telegraph and Telephone
CD	collision detection
CGWCON	Gateway Console
CIDR	Classless Inter-Domain Routing
CIP	Classical IP
CIPC	Classical IP Client
CIR	committed information rate
CLNP	Connectionless-Mode Network Protocol
CPU	central processing unit
CRC	cyclic redundancy check
CRS	configuration report server
CTS	clear to send
CUD	call user data
DAF	destination address filtering
DB	database
DBsum	database summary
DCD	data channel received line signal detector
DCE	data circuit-terminating equipment
DCS	directly connected server
DDLC	dual data-link controller
DDN	Defense Data Network
DDP	Datagram Delivery Protocol
DDT	Dynamic Debugging Tool
DHCP	Dynamic Host Configuration Protocol

dir	directly connected
DL	data link
DLC	data link control
DLCI	data link connection identifier
DLS	data link switching
DLSw	data link switching
DMA	direct memory access
DNA	Digital Network Architecture
DNCP	DECnet Protocol Control Protocol
DNIC	Data Network Identifier Code
DoD	Department of Defense
DOS	Disk Operating System
DR	designated router
DRAM	Dynamic Random Access Memory
DSAP	destination service access point
DSE	data switching equipment
DSE	data switching exchange
DSR	data set ready
DSU	data service unit
DTE	data terminal equipment
DTR	data terminal ready
Dtype	destination type
DVMRP	Distance Vector Multicast Routing Protocol
E1	2.048 Mbps transmission rate
EDEL	end delimiter
EDI	error detected indicator
EGP	Exterior Gateway Protocol
EIA	Electronics Industries Association
ELAN	Emulated Local Area Network
ELAP	EtherTalk Link Access Protocol
ELS	Event Logging System
ESI	End System Identifier
EST	Eastern Standard Time
Eth	Ethernet
fa-ga	functional address-group address
FCS	frame check sequence
FECN	forward explicit congestion notification

FIFO	first in, first out
FLT	filter library
FR	Frame Relay
FRL	Frame Relay
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GOSIP	Government Open Systems Interconnection Profile
GTE	General Telephone Company
GWCON	Gateway Console
HDLC	high-level data link control
HEX	hexadecimal
HST	TCP/IP host services
HTF	host table format
IBD	Integrated Boot Device
ICMP	Internet Control Message Protocol
ICP	Internet Control Protocol
ID	identification
IDP	Initial Domain Part
IDP	Internet Datagram Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
Ifc#	interface number
IGP	interior gateway protocol
ILMI	Interim Local Management Interface
InARP	Inverse Address Resolution Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPPN	IP Protocol Network
IPX	Internetwork Packet Exchange
IPXCP	IPX Control Protocol
ISDN	integrated services digital network
ISO	International Organization for Standardization
Kbps	kilobits per second
LAN	local area network
LAPB	link access protocol-balanced
LAT	local area transport

LCP	Link Control Protocol
LE	LAN Emulation
LEC	LAN Emulation Client
LED	light-emitting diode
LECS	LAN Emulation Configuration Server
LES	LAN Emulation Server
LES-BUS	LAN Emulation Server - Broadcast and Unknown Server
LF	largest frame; line feed
LIS	Logical IP subnet
LLC	logical link control
LLC2	logical link control 2
LMI	local management interface
LRM	LAN reporting mechanism
LS	link state
LSA	link state advertisement
LSB	least significant bit
LSI	LAN Switch Integration
LSreq	link state request
LSrxl	link state retransmission list
LU	logical unit
MAC	medium access control
Mb	megabit
MB	megabyte
Mbps	megabits per second
MBps	megabytes per second
MC	multicast
MCF	MAC filtering
MIB	Management Information Base
MIB II	Management Information Base II
MILNET	military network
MOS	Micro Operating System
MOSDDT	Micro Operating System Dynamic Debugging Tool
MOSPF	Open Shortest Path First with multicast extensions
MSB	most significant bit
MSDU	MAC service data unit

MSS	Multiprotocol Switched Services
MTU	maximum transmission unit
nak	not acknowledged
NBMA	Non-Broadcast Multiple Access
NBP	Name Binding Protocol
NBR	neighbor
NCP	Network Control Protocol
NCP	Network Core Protocol
NetBIOS	Network Basic Input/Output System
NHRP	Next Hop Resolution Protocol
NIST	National Institute of Standards and Technology
NPDU	Network Protocol Data Unit
NRZ	non-return-to-zero
NRZI	non-return-to-zero inverted
NSAP	Network Service Access Point
NSF	National Science Foundation
NSFNET	National Science Foundation NETwork
NVCNFG	nonvolatile configuration
OPCON	Operator Console
OSI	open systems interconnection
OSICP	OSI Control Protocol
OSPF	Open Shortest Path First
OUI	organization unique identifier
PC	personal computer
PCR	peak cell rate
PDN	public data network
PING	Packet internet groper
PDU	protocol data unit
PID	process identification
P-P	Point-to-Point
PPP	Point-to-Point Protocol
PROM	programmable read-only memory
PU	physical unit
PVC	permanent virtual circuit

QoS	Quality of Service
RAM	random access memory
RD	route descriptor
REM	ring error monitor
REV	receive
RFC	Request for Comments
RI	ring indicator; routing information
RIF	routing information field
RII	routing information indicator
RIP	Routing Information Protocol
RISC	reduced instruction-set computer
RNR	receive not ready
ROM	read-only memory
ROpcon	Remote Operator Console
RPS	ring parameter server
RTMP	Routing Table Maintenance Protocol
RTP	RouTing update Protocol
RTS	request to send
Rtype	route type
rxmits	retransmissions
rxmt	retransmit
SAF	source address filtering
SAP	service access point
SAP	Service Advertising Protocol
SCR	sustained cell rate
SCSP	Server Cache Synchronization Protocol
sdel	start delimiter
SDLC	SDLC relay, synchronous data link control
SDU	Service Data Unit
SGID	server group id
seqno	sequence number
SGMP	Simple Gateway Monitoring Protocol
SL	serial line
SLIP	Serial Line IP
SMP	standby monitor present
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture

SNAP	Subnetwork Access Protocol SubNetwork Attachment Point
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SPF	OSPF intra-area route
SPE1	OSPF external route type 1
SPE2	OSPF external route type 2
SPIA	OSPF inter-area route type
SPID	service profile ID
SPX	Sequenced Packet Exchange
SQE	signal quality error
SRAM	static random access memory
SRB	source routing bridge
SRF	specifically routed frame
SRLY	SDLC relay
SRT	source routing transparent
SR-TB	source routing-transparent bridge
STA	static
STB	spanning tree bridge
STE	spanning tree explorer
STP	shielded twisted pair; spanning tree protocol
SVC	switched virtual circuit
SVN	Switched Virtual Networking
TB	transparent bridge
TCN	topology change notification
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEI	terminal point identifier
TFTP	Trivial File Transfer Protocol
TKR	token ring
TLV	Type/Length/Value
TMO	timeout
TOS	type of service
TSF	transparent spanning frames
TTL	time to live
TTY	teletypewriter

TX	transmit
UA	unnumbered acknowledgment
UDP	User Datagram Protocol
UI	unnumbered information
UNI	User-Network Interface
UTP	unshielded twisted pair
VCC	Virtual Channel connection
VINES	VIrtual NEtworking System
VIR	variable information rate
VL	virtual link
VNI	Virtual Network Interface
VR	virtual route
WAN	wide area network
WRS	WAN restoral
X.25	packet-switched networks
X.251	X.25 physical layer
X.252	X.25 frame layer
X.253	X.25 packet layer
XID	exchange identification
XNS	Xerox Network Systems
XSUM	checksum
ZIP	AppleTalk Zone Information Protocol
ZIP2	AppleTalk Zone Information Protocol 2
ZIT	Zone Information Table

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems* , ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology* Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing* , New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- The *Object-Oriented Interface Design: IBM Common User Access Guidelines* , Carmel, Indiana: Que, 1992.

The following cross-references are used in this glossary:

Contrast with:
This refers to a term that has an opposed or substantively different meaning.

Synonym for:
This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with:
This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also:
This refers the reader to terms that have a related, but not synonymous, meaning.

A

AAL. ATM Adaptation Layer, the layer that adapts user data to/from the ATM network by adding/removing headers and segmenting/reassembling the data into/from cells.

AAL-5. ATM Adaptation Layer 5, one of several standard AALs. AAL-5 was designed for data communications, and is used by LAN Emulation and Classical IP.

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also *abstract syntax notation 1 (ASN.1)* and *basic encoding rules (BER)*.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in the following standards:

- ITU-T Recommendation X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1994

See also *basic encoding rules (BER)*.

ACCESS. In the Simple Network Management Protocol (SNMP), the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active monitor. In a token-ring network, a function performed at any one time by one ring station that initiates the transmission of tokens and provides token error recovery facilities. Any active adapter on the ring has the ability to provide the active monitor function if the current active monitor fails.

address. In data communication, the unique code assigned to each device, workstation, or user connected to a network.

address mapping table (AMT). A table, maintained within the AppleTalk router, that provides a current mapping of node addresses to hardware addresses.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with *subnet mask* and *subnetwork mask*.

address resolution. (1) A method for mapping network-layer addresses to media-specific addresses. (2) See also *Address Resolution Protocol (ARP)* and *AppleTalk Address Resolution Protocol (AARP)*.

Address Resolution Protocol (ARP). (1) In the Internet suite of protocols, the protocol that dynamically maps an IP address to an address used by a supporting metropolitan or local area network such as Ethernet or token-ring. (2) See also *Reverse Address Resolution Protocol (RARP)*.

addressing. In data communication, the way in which a station selects the station to which it is to send data.

adjacent nodes. Two nodes connected together by at least one path that connects no other node. (T)

Administrative Domain. A collection of hosts and routers, and the interconnecting networks, managed by a single administrative authority.

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) end node. A node that provides a broad range of end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to a subarea network as a peripheral node or to other end nodes.

Advanced Peer-to-Peer Networking (APPN) network. A collection of interconnected network nodes and their client end nodes.

Advanced Peer-to-Peer Networking (APPN) network node. A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

Advanced Peer-to-Peer Networking (APPN) node. An APPN network node or an APPN end node.

alert. A message sent to a management services focal point in a network to identify a problem or an impending problem.

all-stations address. In communications, synonym for *broadcast address*.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

analog. (1) Pertaining to data consisting of continuously variable physical quantities. (A) (2) Contrast with *digital*.

AppleTalk. A network protocol developed by Apple Computer, Inc. This protocol is used to interconnect network devices, which can be a mixture of Apple and non-Apple products.

AppleTalk Address Resolution Protocol (AARP). In AppleTalk networks, a protocol that (a) translates AppleTalk node addresses into hardware addresses and (b) reconciles addressing discrepancies in networks that support more than one set of protocols.

AppleTalk Transaction Protocol (ATP). In AppleTalk networks, a protocol that provides client/server request and response functions for hosts accessing the Zone Information Protocol (ZIP) for zone information.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network*.

APPN network node. See *Advanced Peer-to-Peer Networking (APPN) network node*.

arbitrary MAC addressing (AMA). In DECnet architecture, an addressing scheme used by DECnet Phase IV-Prime that supports universally administered addresses and locally administered addresses.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

asynchronous (ASYNC). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

ATM. Asynchonous Transfer Mode, a connection-oriented, high-speed networking technology based on cell switching.

ATMARP. ARP in Classical IP.

attachment unit interface (AUI). In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (I) (A)

authentication failure. In the Simple Network Management Protocol (SNMP), a trap that may be generated by an authentication entity when a requesting client is not a member of the SNMP community.

autonomous system. In TCP/IP, a group of networks and routers under one administrative authority. These networks and routers cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. In TCP/IP, a number assigned to an autonomous system by the same central authority that also assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

BCM. BroadCast Manager, an IBM extension to LAN Emulation designed to limit the effects of broadcast frames.

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges or routers. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected.

backbone network. A central network to which smaller networks, normally of lower speed, connect. The backbone network usually has a much higher capacity than the networks it helps interconnect or is a wide-area network (WAN) such as a public packet-switched datagram network.

backbone router. (1) A router used to transmit data between areas. (2) One in a series of routers that is used to interconnect networks into a larger internet.

Bandwidth. The bandwidth of an optical link designates the information-carrying capacity of the link and is related to the maximum bit rate that a fiber link can support.

basic transmission unit (BTU). In SNA, the unit of data and control information passed between path control components. A BTU can consist of one or more path information units (PIUs).

bootstrap. (1) A sequence of instructions whose execution causes additional instructions to be loaded and executed until the complete computer program is in storage. (T) (2) A technique or device designed to bring itself into a desired state by means of its own action, for example, a machine routine whose first few instructions are sufficient to bring the rest of itself into the computer from an input device. (A)

baud. In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud. (A)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems. Contrast with *Exterior Gateway Protocol (EGP).*

border router. In Internet communications, a router, positioned at the edge of an autonomous system, that communicates with a router that is positioned at the edge of a different autonomous system.

bridge. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address.

bridge identifier. An 8-byte field, used in a spanning tree protocol, composed of the MAC address of the port with the lowest port identifier and a user-defined value.

bridging. In LANs, the forwarding of a frame from one LAN segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadcast. (1) Transmission of the same data to all destinations. (T) (2) Simultaneous transmission of data to more than one destination. (3) Contrast with *multicast*.

broadcast address. In communications, a station address (eight 1's) reserved as an address common to all stations on a link. Synonymous with *all-stations address*.

BUS. Broadcast and Unknown Server, a LAN Emulation Service component responsible for the delivery of multicast and unknown unicast frames.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. (4) To place, hide, or store in a cache.

call request packet. (1) A call supervision packet that a data terminal equipment (DTE) transmits to ask that a connection for a call be established throughout the network. (2) In X.25 communications, a call supervision packet transmitted by a DTE to ask for a call establishment through the network.

canonical address. In LANs, the IEEE 802.1 format for the transmission of medium access control (MAC) addresses for token-ring and Ethernet adapters. In canonical format, the least significant (rightmost) bit of each address byte is transmitted first. Contrast with *noncanonical address*.

carrier. An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system. (T)

carrier detect. Synonym for *received line signal detector (RLSD)*.

carrier sense. In a local area network, an ongoing activity of a data station to detect whether another station is transmitting. (T)

carrier sense multiple access with collision detection (CSMA/CD). A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again. (T) (A)

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) A functional unit, controlled by the processor, that handles the transfer of data between processor storage and local peripheral equipment.

channel service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal's performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loopback testing, which includes the transmission of test signals between the CSU and the network carrier's office channel unit. See also *data service unit (DSU)*.

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

CIP. Classical IP.

CIPC. Classical IP Client.

Classical IP. An IETF standard for ATM-attached hosts to communicate using IP over ATM.

Classical IP Client. A Classical IP component that represents users of the Logical IP Subnet.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with *line switching*.

class A network. In Internet communications, a network in which the high-order (most significant) bit of the IP address is set to 0 and the host ID occupies the three low-order octets.

class B network. In Internet communications, a network in which the two high-order (most significant and next-to-most significant) bits of the IP address are set to 1 and 0, respectively, and the host ID occupies the two low-order octets.

class of service (COS). A set of characteristics (such as route security, transmission priority, and bandwidth) used to construct a route between session partners. The class of service is derived from a mode name specified by the initiator of a session.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

clocking. (1) In binary synchronous communication, the use of clock pulses to control synchronization of data and control characters. (2) A method of controlling the number of data bits sent on a telecommunication line in a given time.

collision. An unwanted condition that results from concurrent transmissions on a channel. (T)

collision detection. In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

Committed information rate. The maximum amount of data in bits that the network agrees to deliver.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

compression. (1) The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. (2) Any encoding to reduce the number of bits used to represent a given message or record.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

configuration file. A file that specifies the characteristics of a system device or network.

configuration parameter. A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

configuration report server (CRS). In the IBM Token-Ring Network Bridge Program, the server that accepts commands from the LAN Network Manager (LNM) to get station information, set station parameters, and remove stations on its ring. This server also collects and forwards configuration reports generated by stations on its ring. The configuration reports include the new active monitor reports and the nearest active upstream neighbor (NAUN) reports.

congestion. See *network congestion*.

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

control point management services (CPMS). A component of a control point, consisting of management services function sets, that provides facilities to assist in performing problem management, performance and accounting management, change management, and configuration management. Capabilities provided by the CPMS include sending requests to physical unit management services (PUMS) to test system resources, collecting statistical information (for example, error and performance data) from PUMS about the system resources, and analyzing and presenting test results and statistical information collected about the system resources. Analysis and presentation responsibilities for problem determination and performance monitoring can be distributed among multiple CPMSs.

control point management services unit (CP-MSU). The message unit that contains management services data and flows between management services function sets. This message unit is in general data stream (GDS) format. See also *management services unit (MSU)* and *network management vector transport (NMVT)*.

D

D-bit. Delivery-confirmation bit. In X.25 communications, the bit in a data packet or call-request packet that is set to 1 if end-to-end acknowledgment (delivery confirmation) is required from the recipient.

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

data carrier detect (DCD). Synonym for *received line signal detector (RLSD)*.

data circuit. (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (I) (2) In SNA, synonym for *link connection*. (3) See also *physical circuit* and *virtual circuit*.

Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.
2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

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

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link layer. In the Open Systems Interconnection reference model, the layer that provides services to transfer data between entities in the network layer over a communication link. The data link layer detects and possibly corrects errors that may occur in the physical layer. (T)

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. See also *packet level* and *physical level*. (2) In X.25 communications, synonym for *frame level*.

data link switching (DLSw). A method of transporting network protocols that use IEEE 802.2 logical link control (LLC) type 2. SNA and NetBIOS are examples of protocols that use LLC type 2. See also *encapsulation* and *spoofing*.

data packet. In X.25 communications, a packet used for the transmission of user data on a virtual circuit at the DTE/DCE interface.

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

data set ready (DSR). Synonym for *DCE ready*.

data switching exchange (DSE). The equipment installed at a single location to provide switching functions, such as circuit switching, message switching, and packet switching. (I)

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (I)

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.
2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (I) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram consists of an IP header followed by the transport layer data. (3) See also *packet* and *segment*.

Datagram Delivery Protocol (DDP). In AppleTalk networks, a protocol that provides network connectivity by means of connectionless socket-to-socket delivery service on the internet layer.

DCE ready. In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that the local data circuit-terminating equipment (DCE) is connected to the communication channel and is ready to send data. Synonymous with *data set ready (DSR)*.

DECnet. A network architecture that defines the operation of a family of software modules, databases, and hardware components typically used to tie Digital Equipment Corporation systems together for resource sharing, distributed computation, or remote system configuration. DECnet network implementations follow the Digital Network Architecture (DNA) model.

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

designated router. A router that informs end nodes of the existence and identity of other routers. The selection of the designated router is based upon the router with the highest priority. When several routers share the highest priority, the router with the highest station address is selected.

destination node. The node to which a request or data is sent.

destination port. The 8-port asynchronous adapter that serves as a connection point with a serial service.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. Contrast with *source service access point (SSAP)*.

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

digital. (1) Pertaining to data that consist of digits. (T) (2) Pertaining to data in the form of digits. (A) (3) Contrast with *analog*.

Digital Network Architecture (DNA). The model for all DECnet hardware and software implementations.

direct memory access (DMA). The system facility that allows a device on the Micro Channel bus to get direct access to the system or bus memory without the intervention of the system processor.

directory. A table of identifiers and references to the corresponding items of data. (I) (A)

directory service (DS). An application service element that translates the symbolic names used by application processes into the complete network addresses used in an OSI environment. (T)

directory services (DS). A control point component of an APPN node that maintains knowledge of the location of network resources.

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies. (3) See *Administrative Domain* and *domain name*.

domain name. In the Internet suite of protocols, a name of a host system. A domain name consists of a sequence of subnames separated by a delimiter character. For example, if the fully qualified domain name (FQDN) of a host system is `ralvm7.vnet.ibm.com`, each of the following is a domain name:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

domain name server. In the Internet suite of protocols, a server program that supplies name-to-address translation by mapping domain names to IP addresses. Synonymous with *name server*.

Domain Name System (DNS). In the Internet suite of protocols, the distributed database system used to map domain names to IP addresses.

dotted decimal notation. The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent IP addresses.

dump. (1) Data that has been dumped. (T) (2) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

dynamic reconfiguration (DR). The process of changing the network configuration (peripheral PUs and LUs) without regenerating complete configuration tables or deactivating the affected major node.

Dynamic Routing. Routing using learned routes rather than routes statically configured at initialization.

E

echo. In data communication, a reflected signal on a communications channel. For example, on a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

EIA 232. In data communication, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

ELAN. Emulated Local Area Network, a LAN segment implemented with ATM technology.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

encapsulation. (1) In communications, a technique used by layered protocols by which a layer adds control information to the protocol data unit (PDU) from the layer it supports. In this respect, the layer encapsulates the data from the supported layer. In the Internet suite of protocols, for example, a packet would contain control information from the physical layer, followed by control information from the network layer, followed by the application protocol data. (2) See also *data link switching*.

encode. To convert data by the use of a code in such a manner that reconversion to the original form is possible. (T)

end node (EN). (1) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node.* (2) In communications, a node that is frequently attached to a single data link and cannot perform intermediate routing functions.

entry point (EP). In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

ESI. End System Identifier, a 6-byte component of an ATM address.

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

exception. An abnormal condition such as an I/O error encountered in processing a data set or a file.

exception response (ER). In SNA, a protocol requested in the form-of-response-requested field of a request header that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, can be returned. Contrast with *definite response* and *no response*.

exchange identification (XID). A specific type of basic link unit that is used to convey node and link characteristics between adjacent nodes. XIDs are exchanged between link stations before and during link activation to establish and negotiate link and node characteristics, and after link activation to communicate changes in these characteristics.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR)*.

explorer frame. See *explorer packet*.

explorer packet. In LANs, a packet that is generated by the source host and that traverses the entire source routing part of a LAN, gathering information on the possible paths available to the host.

exterior gateway. In Internet communications, a gateway on one autonomous system that communicates with another autonomous system. Contrast with *interior gateway*.

Exterior Gateway Protocol (EGP). In the Internet suite of protocols, a protocol, used between domains and autonomous systems, that enables network reachability information to be advertised and exchanged. IP network addresses in one autonomous system are advertised to another autonomous system by means of EGP-participating routers. Contrast with *Border Gateway Protocol (BGP)*.

F

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

flow control. (1) In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the rate of flow of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units. (2) See also *pacing*.

fragment. See *fragmentation*.

fragmentation. (1) The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted. (2) See also *segmenting*.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures.

frame level. Synonymous with *data link level*. See *link level*.

Frame Relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols. (3) In TCP/IP, synonym for *router*.

general data stream (GDS). The data stream used for conversations in LU 6.2 sessions.

general data stream (GDS) variable. A type of RU substructure that is preceded by an identifier and a length field and includes either application data, user control data, or SNA-defined control data.

H

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

heap memory. The amount of RAM used to dynamically allocate data structures.

Hello. A protocol used by a group of cooperating, trusting routers to allow them to discover minimal delay routes.

hello message. (1) A message sent periodically to establish and test reachability between routers or between routers and hosts. (2) In the Internet suite of protocols, a message defined by the Hello protocol as an Interior Gateway Protocol (IGP).

heuristic. Pertaining to exploratory methods of problem solving in which solutions are discovered by evaluation of the progress made toward the final result.

high-level data link control (HDLC). In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

hop. (1) In APPN, a portion of a route that has no intermediate nodes. It consists of only a single transmission group connecting adjacent nodes. (2) To the routing layer, the logical distance between two nodes in a network.

hop count. (1) A metric or measure of distance between two points. (2) In Internet communications, the number of routers that a datagram passes through on its way to its destination. (3) In SNA, a measure of the number of links to be traversed in a path to a destination.

host. In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe.

hysteresis. The amount the temperature must change past the set alert threshold before the alert condition is cleared.

I

I frame. Information frame.

IETF. Internet Engineering Task Force, an organization that produces Internet specifications.

ILMI. Interim Local Management Interface, SNMP-based procedures for managing the User-Network Interface (UNI).

information (I) frame. A frame in I format used for numbered information transfer.

input/output channel. In a data processing system, a functional unit that handles transfer of data between internal and peripheral equipment. (I) (A)

integrated services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data.

Note: ISDNs are used in public and private network architectures.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interior gateway. In Internet communications, a gateway that communicates only with its own autonomous system. Contrast with *exterior gateway*.

Interior Gateway Protocol (IGP). In the Internet suite of protocols, a protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

intermediate node. A node that is at the end of more than one branch. (T)

intermediate session routing (ISR). A type of routing function within an APPN network node that provides session-level flow control and outage reporting for all sessions that pass through the node but whose end points are elsewhere.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

International Telecommunication Union (ITU). The specialized telecommunication agency of the United Nations, established to provide standardized communication procedures and practices, including frequency allocation and radio regulations worldwide.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Architecture Board (IAB). The technical body that oversees the development of the Internet suite of protocols that are known as TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Control Protocol (ICP). The VIrtual NEtworking System (VINES) protocol that provides exception notifications, metric notifications, and PING support. See also *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet.

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.

Internetwork Packet Exchange (IPX). (1) The network protocol used to connect Novell’s servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology. (2) See also *Xerox Network Systems (XNS)*.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units. (T)

intra-area routing. In Internet communications, the routing of data within an area.

Inverse Address Resolution Protocol (InARP). In the Internet suite of protocols, the protocol used for locating a protocol address through the known hardware address. In a frame-relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comments (RFC) 791. It is usually represented in dotted decimal notation.

IP datagram. In the Internet suite of protocols, the fundamental unit of information transmitted through an internet. It contains source and destination addresses, user data, and control information such as the length of the datagram, the header checksum, and flags indicating whether the datagram can be or has been fragmented.

IP router. A device in an IP internet that is responsible for making decisions about the paths over which network traffic will flow. Routing protocols are used to gain information about the network and to determine the best route over which the datagram should be forwarded toward the final destination. The datagrams are routed based on IP destination addresses.

IPXWAN. A Novell protocol that is used to exchange router-to-router information before exchanging standard Internetwork Packet Exchange (IPX) routing information and traffic over wide area networks (WANs).

L

LAN bridge server (LBS). In the IBM Token-Ring Network Bridge Program, the server that keeps statistical information about frames forwarded between two or more rings (through a bridge). The LBS sends these statistics to the appropriate LAN managers through the LAN reporting mechanism (LRM).

LAN Emulation (LE). An ATM Forum standard that supports legacy LAN applications over ATM networks.

LAN Emulation Client (LEC). A LAN Emulation component that represents users of the Emulated LAN.

LAN Emulation Configuration Server (LECS). A LAN Emulation Service component that centralizes and disseminates configuration data.

LAN Emulation Server (LES). A LAN Emulation Service component that resolves LAN Destinations to ATM Addresses.

LAN Network Manager (LNM). An IBM licensed program that enables a user to manage and monitor LAN resources from a central workstation.

LAN segment. (1) Any portion of a LAN (for example, a bus or ring) that can operate independently, but that is connected to other parts of the network by means of bridges. (2) A ring or bus network without bridges.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture. (T) (2) In the Open Systems Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols, that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions in other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

LE. LAN Emulation.

LEC. LAN Emulation Client.

LECS. LAN Emulation Configuration Server.

LES. LAN Emulation Server.

line switching. Synonym for *circuit switching*.

link. The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

link access protocol balanced (LAPB). A protocol used for accessing an X.25 network at the link level. LAPB is a duplex, asynchronous, symmetric protocol, used in point-to-point communication.

link-attached. (1) Pertaining to devices that are connected to a controlling unit by a data link. (2) Contrast with *channel-attached*. (3) Synonymous with *remote*.

link connection. (1) The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). (2) In SNA, synonymous with *data circuit*.

link level. (1) A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber’s machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT. (2) See *data link level*.

link-state. In routing protocols, the advertised information about the usable interfaces and reachable neighbors of a router or network. The protocol’s topological database is formed from the collected link-state advertisements.

link station. (1) The hardware and software components within a node representing a connection to an adjacent node over a specific link. For example, if node A is the primary end of a multipoint line that connects to three adjacent nodes, node A will have three link stations representing the connections to the adjacent nodes. (2) See also *adjacent link station (ALS)*.

LIS. Logical IP Subnet, an IP subnet implemented with ATM technology Virtual Networking (SVN) framework.

local. (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with *remote*. (3) Synonym for *channel-attached*.

local area network (LAN). (1) A computer network located on a user’s premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. (3) See also *Ethernet* and *token ring*. (4) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local bridging. A function of a bridge program that allows a single bridge to connect multiple LAN segments without using a telecommunication link. Contrast with *remote bridging*.

local management interface (LMI). See *local management interface (LMI) protocol*.

local management interface (LMI) protocol. In NCP, a set of frame-relay network management procedures and messages used by adjacent frame-relay nodes to exchange line status information over DLCI X'00'. NCP supports both the American National Standards Institute (ANSI) and International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) versions of LMI protocol. These standards refer to LMI protocol as *link integrity verification tests (LIVT)*.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

logical channel. In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

logical link. A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network.

logical link control (LLC). The data link control (DLC) LAN sublayer that provides two types of DLC operation for the orderly exchange of information. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery.

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T) The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical link control (LLC) protocol data unit. A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP), a source service access point (SSAP), a control field, and user data.

logical unit (LU). A type of network accessible unit that enables users to gain access to network resources and communicate with each other.

loopback test. A test in which signals from a tester are looped at a modem or other network element back to the tester for measurements that determine or verify the quality of the communications path.

low-entry networking (LEN). A capability of nodes to attach directly to one another using basic peer-to-peer protocols to support multiple and parallel sessions between logical units.

low-entry networking (LEN) end node. A LEN node receiving network services from an adjacent APPN network node.

low-entry networking (LEN) node. A node that provides a range of end-user services, attaches directly to other nodes using peer protocols, and derives network services implicitly from an adjacent APPN network node, that is, without the direct use of CP-CP sessions.

M

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

management station. In Internet communications, the system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol, such as the Simple Network Management Protocol (SNMP).

mapping. The process of converting data that is transmitted in one format by the sender into the data format that can be accepted by the receiver.

mask. (1) A pattern of characters used to control retention or elimination of portions of another pattern of characters. (I) (A) (2) To use a pattern of characters to control retention or elimination of portions of another pattern of characters. (I) (A)

maximum transmission unit (MTU). In LANs, the largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for Ethernet is 1500 bytes.

medium access control (MAC). In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

medium access control (MAC) protocol. In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T)

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

metric. In Internet communications, a value, associated with a route, which is used to discriminate between multiple exit or entry points to the same autonomous system. The route with the lowest metric is preferred.

metropolitan area network (MAN). A network formed by the interconnection of two or more networks which may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with *local area network (LAN)* and *wide area network (WAN)*.

MIB object. Synonym for *MIB variable*.

MIB variable. In the Simple Network Management Protocol (SNMP), a specific instance of data defined in a MIB module. Synonymous with *MIB object*.

MIB view. In the Simple Network Management Protocol (SNMP), the collection of managed objects, known to the agent, that is visible to a particular community.

MILNET. The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

modulo. (1) Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. (2) See also *modulus*.

modulus. A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 (9 - 4 = 5; 4 - 9 = -5; and 5 divides both 5 and -5 without leaving a remainder).

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

MSS. Multiprotocol Switched Services, a component of IBM’s Switched Virtual Networking (SVN) framework.

multicast. (1) Transmission of the same data to a selected group of destinations. (T) (2) A special form of broadcast in which copies of a packet are delivered to only a subset of all possible destinations.

multiple-domain support (MDS). A technique for transporting management services data between management services function sets over LU-LU and CP-CP sessions. See also *multiple-domain support message unit (MDS-MU)*.

multiple-domain support message unit (MDS-MU). The message unit that contains management services data and flows between management services function sets over the LU-LU and CP-CP sessions used by multiple-domain support. This message unit, as well as the actual management services data that it contains, is in general data stream (GDS) format. See also *control point management services unit (CP-MSU)*, *management services unit (MSU)*, and *network management vector transport (NMVT)*.

N

Name Binding Protocol (NBP). In AppleTalk networks, a protocol that provides name translation function from the AppleTalk entity (resource) name (character string) into an AppleTalk IP address (16-bit number) on the transport layer.

name resolution. In Internet communications, the process of mapping a machine name to the corresponding Internet Protocol (IP) address. See also *Domain Name System (DNS)*.

name server. In the Internet suite of protocols, synonym for *domain name server*.

nearest active upstream neighbor (NAUN). In the IBM Token-Ring Network, the station sending data directly to a given station on the ring.

neighbor. A router on a common subnetwork that has been designated by a network administrator to receive routing information.

NetBIOS. Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) A group of nodes and the links interconnecting them.

network accessible unit (NAU). A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the destination of information transmitted by the path control network. Synonymous with *network addressable unit*.

network address. According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU). Synonym for *network accessible unit*.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion. An undesirable overload condition caused by traffic in excess of what a network can handle.

network identifier. (1) In TCP/IP, that part of the IP address that defines a network. The length of the network ID depends on the type of network class (A, B, or C). (2) A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

Network Information Center (NIC). In Internet communications, local, regional, and national groups throughout the world who provide assistance, documentation, training, and other services to users.

network layer. In Open Systems Interconnection (OSI) architecture, the layer that is responsible for routing, switching, and link-layer access across the OSI environment.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management station. In the Simple Network Management Protocol (SNMP), a station that executes management application programs that monitor and control network elements.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network node (NN). See *Advanced Peer-to-Peer Networking (APPN) network node*.

Next Hop Resolution Protocol (NHRP). A routing protocol, specified in Internet Draft Version 10 which has been submitted for RFC status. The Next Hop Resolution Protocol defines a method for a source station to determine the Non-Broadcast Multi-Access (NBMA) address of the “NBMA next hop” towards a destination. The NBMA next hop may be the destination itself or the router in the NBMA network that is “nearest” to the destination. The source station can then establish an NBMA virtual circuit directly with the destination or the router and reduce the number of routing hops through the NBMA network.

network user address (NUA). In X.25 communications, the X.121 address containing up to 15 binary code digits.

NHRP. Next Hop Resolution Protocol

node. (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data.

noncanonical address. In LANs, a format for the transmission of medium access control (MAC) addresses for token-ring adapters. In noncanonical format, the most significant (leftmost) bit of each address byte is transmitted first. Contrast with *canonical address*.

nonseed router. In AppleTalk networks, a router that acquires network number range and zone list information from a seed router attached to the same network.

O

Open Shortest Path First (OSPF). In the Internet suite of protocols, a function that provides intradomain information transfer. An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

Open Systems Interconnection (OSI). (1) The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) (2) The use of standardized procedures to enable the interconnection of data processing systems.

Note: OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

Open Systems Interconnection (OSI) architecture. Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

Open Systems Interconnection (OSI) reference model. A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

origin. An external logical unit (LU) or application program from which a message or other data originates. See also *destination*.

orphan circuit. A non-configured circuit whose availability is learned dynamically.

P

pacing. (1) A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. (2) See also *flow control*, *receive pacing*, *send pacing*, *session-level pacing*, and *virtual route (VR) pacing*.

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet mode operation. Synonym for *packet switching*.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with *packet mode operation*. See also *circuit switching*.

parallel bridges. A pair of bridges connected to the same LAN segment, creating redundant paths to the segment.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also *explicit route (ER)*, *route extension*, and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path cost. In link-state routing protocols, the sum of the link costs along the path between two nodes or networks.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment.

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with *global character* and *wildcard character*.

permanent virtual circuit (PVC). In X.25 and frame-relay communications, a virtual circuit that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with *switched virtual circuit (SVC)*.

physical circuit. A circuit established without multiplexing. See also *data circuit*. Contrast with *virtual circuit*.

physical layer. In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain, and release physical connections over the transmission medium. (T)

physical unit (PU). (1) The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. (2) See also *peripheral PU* and *subarea PU*.

ping command. The command that sends an Internet Control Message Protocol (ICMP) echo-request packet to a gateway, router, or host with the expectation of receiving a reply.

Point-to-Point Protocol (PPP). A protocol that provides a method for encapsulating and transmitting packets over serial point-to-point links.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (6) Synonymous with *socket*.

port number. In Internet communications, the identification of an application entity to the transport service.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with *line control discipline* and *line discipline*. See *bracket protocol* and *link protocol*.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

Q

Quality of Service (QoS). The user-oriented performance of an end-to-end service which is accessed using performance parameters. In ATM networks, the following performance parameters determine the QoS of an end-to-end ATM connection: cell loss ratio, cell transfer delay, and cell delay variation.

R

Rapid Transport Protocol (RTP) connection. In high-performance routing (HPR), the connection established between the endpoints of the route to transport session traffic.

reachability. The ability of a node or a resource to communicate with another node or resource.

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

reassembly. In communications, the process of putting segmented packets back together after they have been received.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See *RNR packet*.

received line signal detector (RLSD). In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE). Synonymous with *carrier detect* and *data carrier detect (DCD)*.

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Synonym for *link-attached*. (3) Contrast with *local*.

remote bridging. The function of a bridge that allows two bridges to connect multiple LANs using a telecommunication link. Contrast with *local bridging*.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any host in the network. The local host receives the results of the command execution.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

reset request packet. In X.25 communications, a packet transmitted by the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE) to request that a virtual call or a permanent virtual circuit be reset. The reason for the request can also be specified in the packet.

ring. See *ring network*.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

ring segment. A section of a ring that can be isolated (by unplugging connectors) from the rest of the ring. See *LAN segment*.

rlogin (remote login). A service, offered by Berkeley UNIX-based systems, that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes information about the user's environment (for example, terminal type) to the remote machine.

RNR packet. A packet used by a data terminal equipment (DTE) or by a data circuit-terminating equipment (DCE) to indicate a temporary inability to accept additional packets for a virtual call or permanent virtual circuit.

root bridge. The bridge that is the root of a spanning tree formed between other active bridges in the bridging network. The root bridge originates and transmits bridge protocol data units (BPDUs) to other active bridges to maintain the spanning tree topology. It is the bridge with the highest priority in the network.

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunication link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

Route Selection control vector (RSCV). A control vector that describes a route within an APPN network. The RSCV consists of an ordered sequence of control vectors that identify the TGs and nodes that make up the path from an origin node to a destination node.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. (3) In OSI terminology, a function that determines a path by which an entity can be reached. (4) In TCP/IP, synonymous with *gateway*. (5) Contrast with *bridge*.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing domain. In Internet communications, a group of intermediate systems that use a routing protocol so that the representation of the overall network is the same within each intermediate system. Routing domains are connected to each other by exterior links.

Routing Information Protocol (RIP). In the Internet suite of protocols, an interior gateway protocol used to exchange intradomain routing information and to determine optimum routes between internet hosts. RIP determines optimum routes on the basis of route metrics, not link transmission speed.

routing loop. A situation that occurs when routers circulate information among themselves until convergence occurs or until the networks involved are considered unreachable.

routing protocol. A technique used by a router to find other routers and to remain up to date about the best way to get to reachable networks.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). In AppleTalk networks, a protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

RouTing update Protocol (RTP). The VIrtual NEtworking System (VINES) protocol that maintains the routing database and allows the exchange of routing information between VINES nodes. See also *Internet Control Protocol (ICP).*

rsh. A variant of the rlogin command that invokes a command interpreter on a remote UNIX machine and passes the command-line arguments to the command interpreter, skipping the login step completely.

S

SDU. Service Data Unit, data as it appears at the interface between a layer and the layer immediately above.

seed router. In AppleTalk networks, a router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed router must be initially set up using the configurator tool. Contrast with *nonseed router*.

segment. (1) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

segmenting. In OSI, a function performed by a layer to map one protocol data unit (PDU) from the layer it supports into multiple PDUs.

sequence number. In communications, a number assigned to a particular frame or packet to control the transmission flow and receipt of data.

server. A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

Service Advertising Protocol (SAP). In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and IP address recorded in all file servers running NetWare.
- A mechanism that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type.
- A mechanism that allows a workstation to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session.

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).

SLIP. Serial Line IP, an IETF standard for running IP over serial communication links.

SNA management services (SNA/MS). The services provided to assist in management of SNA networks.

SNAP. (1) SubNetwork Access Protocol. (2) SubNetwork Attachment Point.

socket. An endpoint for communication between processes or application programs.

source route bridging. In LANs, a bridging method that uses the routing information field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The routing information field is inserted into the MAC header by the source node. The information in the routing information field is derived from explorer packets generated by the source host.

source routing. In LANs, a method by which the sending station determines the route the frame will follow and includes the routing information with the frame. Bridges then read the routing information to determine whether they should forward the frame.

source service access point (SSAP). In SNA and TCP/IP, a logical address that allows a system to send data to a remote device from the appropriate communications support. Contrast with *destination service access point (DSAP)*.

spanning tree. In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topology to ensure that there is only one route between any two LANs in the bridged network. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

sphere of control (SOC). The set of control point domains served by a single management services focal point.

sphere of control (SOC) node. A node directly in the sphere of control of a focal point. A SOC node has exchanged management services capabilities with its focal point. An APPN end node can be a SOC node if it supports the function to exchange management services capabilities.

split horizon. A technique for minimizing the time to achieve network convergence. A router records the interface over which it received a particular route and does not propagate its information about the route back over the same interface.

spoofing. For data links, a technique in which a protocol initiated from an end station is acknowledged and processed by an intermediate node on behalf of the final destination. In IBM 6611 data link switching, for example, SNA frames are encapsulated into TCP/IP packets for transport across a non-SNA wide area network, unpacked by another IBM 6611, and passed to the final destination. A benefit of spoofing is the prevention of end-to-end session timeouts.

standard MIB. In the Simple Network Management Protocol (SNMP), a MIB module that is located under the management branch of the Structure of Management Information (SMI) and that is considered a standard by the Internet Engineering Task Force (IETF).

static route. The route between hosts, networks, or both that is manually entered into a routing table.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

StreetTalk. In the VIrtual NEtworking System (VINES), a unique network-wide naming and addressing system that allows users to locate and access any resource on the network without knowing the network topology. See also *Internet Control Protocol (ICP)* and *RouTing update Protocol (RTP)*.

Structure of Management Information (SMI). (1) In the Simple Network Management Protocol (SNMP), the rules used to define the objects that can be accessed by means of a network management protocol. (2) In OSI, the set of standards relating to management information. The set includes the *Management Information Model* and the *Guidelines for the Definition of Managed Objects*

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for *subnetwork*.

subnet address. In Internet communications, an extension to the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use `$AA` as their service access point (SAP) value.

SubNetwork Attachment Point (SNAP). An LLC header extension that identifies the protocol type of a frame.

subnetwork mask. Synonym for *address mask*.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

SVN. Switched Virtual Networking, the name of IBM's framework for building and managing switch-based networks.

switched virtual circuit (SVC). An X.25 circuit that is dynamically established when needed. The X.25 equivalent of a switched line. Contrast with *permanent virtual circuit (PVC)*.

synchronous. (1) Pertaining to two or more processes that depend upon the occurrence of specific events such as common timing signals. (T) (2) Occurring with a regular or predictable time relationship.

Synchronous Data Link Control (SDLC). (1) A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I) (2) Contrast with *binary synchronous communication (BSC)*.

SYNTAX. In the Simple Network Management Protocol (SNMP), a clause in the MIB module that defines the abstract data structure that corresponds to a managed object.

system configuration. A process that specifies the devices and programs that form a particular data processing system.

system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for users of the network. Multiple SSCPs, cooperating as peers with one another, can divide the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a “threshold exceeded” occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

throughput class. In packet switching, the speed at which data terminal equipment (DTE) packets travel through the packet switching network.

time to live (TTL). A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

TLV. Type/Length/Value, a generalized information element in a LAN Emulation packet.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

topology database update (TDU). A message about a new or changed link or node that is broadcast among APPN network nodes to maintain the network topology database, which is fully replicated in each network node. A TDU contains information that identifies the following:

- The sending node
- The node and link characteristics of various resources in the network
- The sequence number of the most recent update for each of the resources described.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

transceiver (transmitter-receiver). In LANs, a physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and that sense collisions.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission group (TG). (1) A connection between adjacent nodes that is identified by a transmission group number. (2) In a subarea network, a single link or a group of links between adjacent nodes. When a transmission group consists of a group of links, the links are viewed as a single logical link, and the transmission group is called a *multilink transmission group (MLTG)*. A *mixed-media multilink transmission group (MMMLTG)* is one that contains links of different medium types (for example, token-ring, switched SDLC, nonswitched SDLC, and frame-relay links). (3) In an APPN network, a single link between adjacent nodes. (4) See also *parallel transmission groups*.

transmission header (TH). Control information, optionally followed by a basic information unit (BIU) or a BIU segment, that is created and used by path control to route message units and to control their flow within the network. See also *path information unit*.

transparent bridging. In LANs, a method for tying individual local area networks together through the medium access control (MAC) level. A transparent bridge stores the tables that contain MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

transport layer. In the Open Systems Interconnection reference model, the layer that provides a reliable end-to-end data transfer service. There may be relay open systems in the path. (T) See also *Open Systems Interconnection reference model*.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

tunneling. To treat a transport network as though it were a single communication link or LAN. See also *encapsulation*.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The European version (E1) transmits 2.048 Mbps. The Japanese version (J1) transmits 1.544 Mbps.

U

UNI. User-Network Interface, the interface between user equipment and an ATM switch network.

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with *locally administered address*.

User Datagram Protocol (UDP). In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

V.24. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

V.25. In data communication, a specification of the CCITT that defines the automatic answering equipment and parallel automatic calling equipment on the General Switched Telephone Network, including procedures for disabling of echo controlled devices for both manually and automatically established calls.

V.35. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

V.36. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at rates of 48, 56, 64, or 72 kilobits per second.

VCC. Virtual Channel Connection, a connection between parties.

VINES. VIrtual NEtworking System.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit*. Contrast with *physical circuit*. (2) A logical connection established between two DTEs.

virtual link. In Open Shortest Path First (OSPF), a point-to-point interface that connects border routers that are separated by a non-backbone transit area. Because area routers are part of the OSPF backbone, the virtual link connects the backbone. The virtual links ensure that the OSPF backbone does not become discontinuous.

Virtual Local Area Network (VLAN). A logical grouping of one or more LANs based on protocol and subnet and used to isolate network traffic within these groups.

VIrtual NEtworking System (VINES). The network operating system and network software from Banyan Systems, Inc. In a VINES network, virtual linking allows all devices and services to appear to be directly connected to each other, when they may actually be thousands of miles apart. See also *StreetTalk*.

virtual route (VR). (1) In SNA, either (a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or (b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). (2) Contrast with *explicit route (ER)*. See also *path* and *route extension (REX)*.

W

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communication network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. (3) Contrast with *local area network (LAN)* and *metropolitan area network (MAN)*.

wildcard character. Synonym for *pattern-matching character*.

X

X.21. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for a general-purpose interface between data terminal equipment and data circuit-terminating equipment for synchronous operations on a public data network.

X.25. (1) An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. (2) See also *packet switching*.

Xerox Network Systems (XNS). The suite of internet protocols developed by the Xerox Corporation. Although similar to TCP/IP protocols, XNS uses different packet formats and terminology. See also *Internetwork Packet Exchange (IPX)*.

Z

zone. In AppleTalk networks, a subset of nodes within an internet.

Zone Information Protocol (ZIP). In AppleTalk networks, a protocol that provides zone management service by maintaining a mapping of the zone names and network numbers across the internet on the session layer.

zone information table (ZIT). A listing of network numbers and their associated zone name mappings in the internet. This listing is maintained by each internet router in an AppleTalk internet.

Index

© Copyright IBM Corp. 1998

Readers' Comments — We'd Like to Hear from You

Nways Multiprotocol Switched Services Family Clients
Interface Configuration and
Software User's Guide

Publication No. SC30-3966-01

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

SC30-3966-01

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

IBM Corporation
Design & Information Development
Department CGF/Bldg. 656
PO Box 12195
Research Triangle Park, NC 27709-9990

Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC30-3966-01

Spine information:

Nways Multiprotocol Switched
Services Family Clients

MSS Family Clients Interface Configuration