Nways Multiprotocol Switched Services

Configuring Protocols and Features Volume 2

SC30-3994-00

Nways Multiprotocol Switched Services

Configuring Protocols and Features Volume 2

SC30-3994-00

First Edition (February 1999)

This edition applies to Version 2.2 of the IBM 8210 Multiprotocol Switched Services Server 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:

Department CGF
Design & Information Development
IBM Corporation
P.O. Box 12195
RESEARCH TRIANGLE PARK NC 27709
USA

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

Contents

Figures

Tables

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	CUA	Operating System/2
AIX	IBM	RS/6000
AIXwindows	Micro Channel	System/370
APPN	NetView	VTAM
BookManager	Nways	Web Explorer
Common User Access	OS/2	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 interface for configuration and operation of the IBM Nways Multiprotocol Switched Services (MSS) or your A-MSS Server Module, hereafter referred to as “the router”, installed on your IBM Multiprotocol Switched Services (MSS). With the help of this manual, you should be able to perform the following processes and operations:

- Configure, monitor, and use the Multiprotocol Switched Services (MSS) base code on your IBM Nways Multiprotocol Switched Services (MSS) or your A-MSS Server Module
- Configure, monitor, and use the interfaces and Link Layer software supported by your 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 (re).
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. Three periods following an option mean that you enter additional data (for example, a variable) after the option. For example:

   time host ...

   In this example, you enter the IP address of the host in place of the periods, as explained in the description of the command.
4. 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.
5. Keyboard key combinations are indicated in text in the following ways:
   - – **Ctrl-P**
   - – **Ctrl -**

The key combination **Ctrl -** indicates that you should press the Ctrl key and the hyphen simultaneously. In certain circumstances, this key combination changes the command line prompt.

- Names of keyboard keys are indicated like this: **Enter**

MSS Server Library

The following hard copy publications are shipped with the product. The manuals in this list are also included in displayable softcopy form on the Multiprotocol Switched Services (MSS) Softcopy Library CD-ROM (SK2T-0378). This CD-ROM is shipped with initial orders for the MSS Server.

The reference cards and the safety information booklet are shipped in hard copy only and are not included on the CD-ROM.

- *Multiprotocol Switched Services (MSS) Server Installation and Initial Configuration Guide*, GA27-4140
- *IBM 8210 Nways Multiprotocol Switched Services (MSS) Server Operations Reference Card*, GX27-4017
- *Multiprotocol Switched Services (MSS) Server Module Installation and Initial Configuration Guide*, GA27-4141
- *IBM 8210 Nways Multiprotocol Switched Services (MSS) Server Module Operations Reference Card*, GX27-4018
- *8210 Multiprotocol Switched Services (MSS) Server User's Feature Removal and Replacement Guide*, GY27-0359
- *CAUTION: Safety Information - Read This First,* SD21-0030

The following publications are not shipped in hard copy, but are offered in soft copy form on the Multiprotocol Switched Services (MSS) Softcopy Library CD-ROM (SK2T-0378). All of these manuals can be separately ordered in hard copy form through your IBM marketing representative.

- *Multiprotocol Switched Services (MSS) Server Introduction and Planning Guide*, GC30-3820
- *Mulitprotocol Switched Services (MSS) Server Service and Maintenance Manual*, GY27-0354
- *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide*, SC30-3818
- *Multiprotocol Switched Services (MSS) Configuring Interfaces and Features Volume 1*, SC30-3819
- *Multiprotocol Switched Services (MSS) Configuring Protocols and Features Vol. 2*, SC30-3994
- *Event Logging System Messages Guide*, SC30-3682
- *User's Guide for Nways Multiprotocol and Access Services Products*, GC30-3830

Summary of Changes For Version 2.2

The following are the new functions in this release:

- LES/BUS Enhanced Redundancy
- LES/BUS Peer Redundancy
- BUS Data Packet Filtering
- LECS Database Synchronization

- LEC Persistant Data Direct VCCs
- Rapid LES/BUS Failure Detection
- Multiple LECS Configuration Requests
- LEC Fast Path support for 802.3 IP and Source Routed Packets
- MPOA support for IPX
- Additional Dynamic Reconfiguration function
- Bridging and Routing the same protocol within one device
- IPXWAN for multiple DLCIs
- IP Filter Enhancements
- IP Routing/Bridging on the same interface
- Bootp Enhancements
- DLSw Currency
- IPv4 enhancements
- OSPF currency
- New DVMRP configuration menus
- MOS-IP
- Increased number of interfaces
- Logging enhancements
- Event Logging System Enhancements
- Report CPU Utilization function
- Packet tracing for interfaces other than ATM
- Type of Service (TOS)
- Policy-based routing
- Console Usability and Command Completion Enhancements

The technical changes and additions are indicated by a vertical line (|) to the left of the change.

Editorial Changes

This edition begins a number of editorial changes to this book and the other software books that will:

- Reorganize the material
- Remove any unnecessary and redundant information
- Improve retrievability
- Add additional clarification to some information

This effort will take a number of editions. Please help us during this effort by reporting any corrections using the Reader's Comment Form in the back of the book.

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 8210. 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).

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	yes	yes
FasTR over ATM	yes	no
Protocols and Features		
Classical IP	yes	no
IP	yes	yes
Banyan VINES	yes	yes
AppleTalk	yes	yes

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

Feature	MSS Client	MSS Domain Client
IPX	yes	yes
Source-Route Bridging	yes	yes
NHRP	yes	no
LAN Network Manager	yes	yes
MPOA	yes	no
PVLAN	yes	yes (on Token-Ring only)
CIP ARP Server Redundancy	yes	no
QoS LAN Emulation Client	yes	no
MARS Client	yes	no
OSPF/MOSPF	yes	yes
RIP	yes	yes
RIP2	yes	yes
DVMRP	yes	yes
BGP	yes	yes

Chapter 1. Using SNMP

This chapter describes SNMP. It contains the following sections:

- "Network Management"
- "SNMP Management"

Network Management

Refer to the *Planning and Setup Guide* for information about Network Management.

SNMP Management

The IBM 8210 Nways Multiprotocol Switched Services (MSS) Server provides a Simple Network Management Protocol (SNMP) interface to network management platforms and applications, such as the Nways Campus Manager products.

SNMP is used for monitoring and managing IP hosts in an IP network and uses software called an SNMP agent to enable network hosts to read and modify some of the IBM 8210 Nways Multiprotocol Switched Services (MSS) Server's operational parameters. In this way, SNMP establishes network management for the IP community.

You need to consider the following aspects of SNMP when you configure SNMP for your IBM 8210 Nways Multiprotocol Switched Services (MSS) Server.

Community

The community allows you to define the IP address of the SNMP management station that is allowed to access the information in the SNMP agent's Management Information Base (MIB). You define a community name for use in accessing the MIB.

Authentication

The community name is used as an authentication scheme to prevent unauthorized users from learning information about an SNMP agent or modifying its characteristics.

This scheme involves defining one or more sets of MIB data (referred to as MIB views) and associating an access privilege (read-only, read-write), an IP mask, and a community name with each MIB view. The IP mask establishes which IP addresses can originate access requests for a given MIB view and the community name serves as a password that must be matched by the SNMP requests. The community name is included in each SNMP message and verified by the IBM 8210 SNMP agent. An SNMP request will be rejected if it does not provide the correct community name, does not match the IP mask, or attempts an access that is inconsistent with the assigned access privilege.

MIB Support

A MIB is a virtual information store that provides access to management information. This information is defined as MIB objects which can be accessed and, in some cases, be modified using network management tools.

Using SNMP

IBM 8210 provides a comprehensive set of standard and enterprise-specific MIBs for monitoring and managing resources

You can find readme files documenting IBM 8210 MIB support by accessing the appropriate release directory on the World Wide Web at URL:

- **ftp://ftp.nways.raleigh.ibm.com/pub/netmgmt/mss/**

To receive a copy of a specific MIB, enter the **get** command with the name of the MIB. For example, the command,**get ibm.mib** places a copy of the specified MIB in the directory from which you connected to the FTP server.

You can access the following information from the ftp site:

- Standard MIBs
- Enterprise MIBs
- SNMP generic traps
- Enterprise-specific MIBs
- Settable values

Except for the settable values, all supported MIB attributes are in READ-ONLY mode.

Trap Messages

Trap messages are unsolicited messages sent from the SNMP agent in the server to an SNMP manager in response to a server or network condition, such as a server reload or network down.

Chapter 2. Configuring and Monitoring SNMP

This chapter describes the SNMP configuring and monitoring commands. It includes the following sections:

Accessing the SNMP Configuration Environment

To access the SNMP configuration environment, enter the following command at the `Config>` prompt:

```
Config> protocol snmp
SNMP user configuration
SNMP Config>
```

SNMP Configuration Commands

This section describes the SNMP configuration commands.

Table 2 lists the SNMP configuration commands. The SNMP configuration commands allow you to specify parameters that define the relationship between the SNMP agent and the network management station. The information you specify takes effect immediately after a restart or reload of the IBM 8210.

Enter the SNMP configuration commands at the `SNMP Config>` prompt.

Table 2. SNMP 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 xxi.
Add	Adds a community to the list of SNMP communities, an IP address with mask to a community, or a subtree to a MIB view.
Delete	Removes a community from the list of SNMP communities, an IP address with mask from a community, or a subtree from a MIB view.
Enable/Disable	Enables/disables SNMP protocol and traps associated with named communities.
List	Displays the current communities with their associated access modes, enabled traps, IP addresses, and views. Also displays all views and their associated MIB subtrees.

Table 2. SNMP Configuration Commands Summary (continued)

Command	Function
Set	Sets a community's access mode or view. A community's access mode is one of the following: Read and trap generation Read, write and trap generation Trap generation only This command is also used to set a trap UDP port.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxii.

Add

Use the **add** command to add a community name to the list of SNMP communities, add an address to a community, or assign a portion of the MIB (subtree) to a view.

Syntax:

add community

address

sub_tree

community

Use the **add community** command to create a community. It will be created with a default access of read_trap, a view of all, all traps disabled, and all IP addresses allowed.

Note: The **add community** command no longer allows you to select access type or trap control. Use the set community access command to assign access types to existing SNMP communities and use the **enable trap** or the **disable trap** command for trap control.

The *community name* parameter provides the community name used by the SNMP client. This community name is used when accessing the management information base (MIB) in the device from the host specified by the Community IP address parameter.

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: public

Example: `add community <community_name>`

```
Community Name  []?
```

address

Use the **add address** command to add to the community definition an address of a network management station in the network that should be allowed to communicate with this box. You must supply the name of the community and the network address (in standard a.b.c.d notation). You also may supply a net mask to restrict access to either an individual host (mask

= 255.255.255.255) or to a network of hosts. More than one address can be added to a community; enter the command each time you want to add another address.

If you do not specify an address for a community, requests are handled from any host.

Addresses also specify hosts that receive the traps. If no address is specified, no trap is generated.

1. The *community name* has:

   Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

   Default Value: none

2. The *IP address* has:

   Valid Values: Any valid IP address.

   Default Value: none

3. You also may supply a *net mask* to restrict access to either an individual host (mask = 255.255.255.255) or to a network of hosts.

   Valid Values: 0.0.0.0 - 255.255.255.255

   Default Value: none

Example: `add address <community_name> <ipAddress> <ipMask>`

```
Community Name []?
New Address [0.0.0.0]?
```

sub_tree

Use the **add sub_tree** command to add a portion of the MIB to a view or to create a new view. The default is the entire MIB. The **add sub_tree** command is used to manage MIB views. More than one subtree can be added to a view defined by <view_text_name>. To create a new MIB view, issue the **add sub_tree** command with the new view name.

Note: You must assign a view to one or more communities using the **set community view** command to have it take effect. The subtree definitions are inclusive; that is, the subtree OID specified and any OID that is lexicographically greater than the specified OID is considered part of the MIB view.

Valid Values:

- All - Assigns all supported MIB views to the named community.
- View - Assigns a specified MIB view to the named community.

Default Value: All

The *MIB OID name* is the parameter that specifies the MIB Object ID for the sub_tree. This must be entered as a numeric value, not a symbolic value.

This parameter contains a MIB subtree name included in the view defined with the View name parameter. All children of a specified MIB subtree are also included in the view.

For example, to provide a view that would give access to the system group in MIB-II, specify **1.3.6.1.2.1.1**.

Valid Values:

An object identifier in the form of <element1>.<element2>.<element3>. . ., where:

- You need a minimum of 3 elements.
- You can define a maximum of 49 elements.
- element1 is 0, 1, or 2.
- element2 is an integer between 1 and 40.
- element3 and subsequent elements are integers between 1 and the size of an unsigned byte integer.

Default Value: None

Example: `add sub_tree`

```
View Name  []?
MIB OID name []?
```

View Name	Specify the name of the view (32 visual characters maximum). Characters such as spaces, tabs, or <Esc> key sequences are not accepted.
MIB OID	Specifies the MIB Object ID for the sub_tree. This must be entered as a numeric value in dotted notation, *not* a symbolic value.

Delete

Use the **delete** command to delete:

- a specific address.
- a community and all of its addresses.
- a subtree from a view.

Syntax:

delete	community
	address
	sub_tree

community

Removes a community and its IP addresses. You must supply the community name.

The *community name*.

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: public

This parameter provides a community name used by the SNMP client. This community name is used when accessing the management information base (MIB) in the device from the host specified by the Community IP address parameter.

Example: `delete community <community_name>`

address

Removes an address from a community. You must supply the name.

1. The *community name* has:

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: public

This parameter provides a community name used by the SNMP client. This community name is used when accessing the management information base (MIB) in the device from the host specified by the Community IP address parameter.

2. The *IP address* has:

   Valid Values: Any valid IP address.

   Default Value: none

3. You also may supply a *net mask* to restrict access to either an individual host (mask = 255.255.255.255) or to a network of hosts.

   Valid Values: 0.0.0.0 - 255.255.255.255

   Default Value: none

Example: `delete address <comm_name> <ipAddress> <ipMask>`

sub_tree

Removes a MIB or a portion of the MIB from a view. You must supply the name of the subtree. If all subtrees are deleted, the MIB view is also deleted and all references to it from any associated SNMP communities are removed.

1. The *view name* to be removed is the parameter that allows you to select the view used by the community defined in the Community name parameter. This view determines which MIB objects this community may access. If no view is specified, the community may access all objects known to the router's SNMP agent.

   This parameter should be answered if you decide to restrict a community from accessing the entire MIB managed by the router's SNMP agent.

   You must configure the View name parameter and the MIB Subtree parameter before you can configure this parameter.

   Valid Values:

   – All - Assigns all supported MIB views to the named community.

   – View - Assigns a specified MIB view to the named community.

   Default Value: All

2. The *MIB OID name* is the parameter that specifies the MIB Object ID for the sub_tree. This must be entered as a numeric value, not a symbolic value.

   This parameter contains a MIB subtree name included in the view defined with the View name parameter. All children of a specified MIB subtree are also included in the view.

   For example, to provide a view that would give access to the system group in MIB-II, specify **1.3.6.1.2.1.1**.

   Valid Values:

   An object identifier in the form of <element1>.<element2>.<element3>. . ., where:

   – You need a minimum of 3 elements.

   – You can define a maximum of 49 elements.

   – element1 is 0, 1, or 2.

– element2 is an integer between 1 and 40.
– element3 and subsequent elements are integers between 1 and the size of an unsigned byte integer.

Default Value: None

Example: `delete sub_tree <view_text_name> <oid>`

Disable

Use the **disable** command to disable the SNMP protocol or specified traps on the router.

Syntax:

disable snmp
trap

snmp Disables SNMP

The *community name* has:

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: public

Example: `disable snmp`

trap Disables specified traps or all traps. You must specify the trap type from the following options.

Example: `disable trap <trap_type> <community_name>`

Trap Type	Description
all	Disables all traps in a specified community. Specify the community name as part of the command line.
cold_start	Disables cold start traps in a specified community. A cold start trap means that the transmitting router is reinitializing and that the agent's configuration or the protocol entity implementation may be altered. Specify the community name as part of the command line.
link_down	Disables link_down traps in a specified community. A link_down trap recognizes a failure in one of the communication links represented in the agent's configuration. The link_down trap-PDU contains the name and value of the ifIndex instance for the affected link as the first element of its variable-bindings.
link_up	Disables link_up traps in a specified community. A link_up trap recognizes that a previously inactive link in the network has come up. The link_up trap-PDU contains the name and value of the ifIndex instance for the affected link as the first element of its variable-bindings.
auth_fail	Disables authentication failure traps for a specified community. Authentication failure traps indicate that the sender of the SNMP request does not have the proper permission to talk to this box's SNMP agent.
enterprise	Disables enterprise specific traps in a specified community. Enterprise specific traps indicate that some enterprise specific event has occurred. The specific-trap field identifies the particular trap that occurred. For example, when configured to do so, ELS event messages are sent in enterprise-specific traps.

Enable

Use the **enable** command to enable the SNMP protocol or specified traps on the router.

Syntax:

enable snmp

trap

snmp Enables SNMP

Example: `enable snmp`

trap Enables specified traps or all traps. You must specify the trap type from the options shown below.

The *community name* has:

Valid Values: A string of 1 to 31 alphanumeric characters.

Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: public

Example: `enable trap <trap_type> <community_name>`

Trap Type	Description
all	Enables all traps in a specified community. Specify the community name as part of the command line.
cold_start	Enables cold start traps in a specified community. A cold start trap means that the transmitting router is reinitializing and that the agent's configuration or the protocol entity implementation may be altered. Specify the community name as part of the command line.
link_down	Enables link_down traps in a specified community. A link_down trap recognizes a failure in one of the communication links represented in the agent's configuration. The link_down trap-PDU contains the name and value of the ifIndex instance for the affected link as the first element of its variable-bindings.
link_up	Enables link_up traps in a specified community. A link_up trap recognizes that a previously inactive link in the network has come up. The link_up trap-PDU contains the name and value of the ifIndex instance for the affected link as the first element of its variable-bindings.
auth_fail	Enables authentication failure traps for a specified community. Authentication failure traps indicate that the sender of the SNMP request does not have the proper permission to talk to this box's SNMP agent.
enterprise	Enables enterprise specific traps in a specified community. Enterprise specific traps indicate that some enterprise specific event has occurred. The specific-trap field identifies the particular trap that occurred. For example, when configured to do so, ELS event messages are sent in enterprise-specific traps.

List

Use the **list** command to display the current configuration of SNMP communities, access modes, traps, network addresses, and views.

Syntax:

list all
community
views

list all Displays the current configuration of SNMP communities for Access, Traps, Address, and View. See the description of the **list community** command for details on the options.

Example: `list all`

```
SNMP Config>list all

   SNMP is enabled
   Trap UDP port: 162
   SRAM write is enabled

            Community Name                Access
   -------------------------------  ------------------
   oxnard                           Read, Write, Trap
   public                           Read, Trap


           Community Name             IP Address         IP Mask
   -------------------------------  ---------------  ---------------
   oxnard                           1.1.1.2          255.255.255.255
   public                           All              N/A


           Community Name                Enabled Traps
   -------------------------------  -------------------------------
   oxnard                           Link Down, Cold Restart
   public                           None


            Community Name                    View
   -------------------------------  -------------------------------
   oxnard                           mib2
   public                           All

             View Name                    Sub-Tree
   -------------------------------  -------------------------------
   mib2                             1.3.6.1.2
```

list community *option*

Displays the current attributes of an SNMP community. Options are access, traps, address, view.

Option	Description
Access	Displays the access modes for the community.
Address	Displays the network address for the community.
Traps	Displays the types of traps generated for the community.
View	Displays the MIB view for the community.

list community access

Example: `list community access`

```
            Community Name   Access
            public           Read, Write, Trap
            oxnard           Read, Trap
```

list community traps

Example: `list community traps`

```
Community Name   Enabled Traps
public           Link Down, Cold Restart
oxnard           NONE
```

list community address

Example: `list community address`

```
Community Name   IP Address   IP Mask
public           All          N/A
oxnard           1.1.1.2      255.255.255.255
```

list community view

Example: `list community view`

```
Community Name   View
public           All
oxnard           mib2
```

list views

Displays the current views for a specified SNMP community.

Example: `list views`

```
View Name   Sub-Tree
mib2        1.3.6.1.2.1
```

Set

Use the **set** command to assign a MIB view to a community, to set the SNMP UDP trap port number, or set the access mode of the community.

Syntax:

set community access

community view

trap_port

community access

Use the **set community access** command to assign one of three access types to a community. You must supply the name of the community and the access type.

The *community name* has:

Valid Values: A string of 1 to 31 alphanumeric characters.

Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: public

Example: `set community access <options> <comm_name>`

Options	Description
read_trap	Allows read access and trap generation to the named community.
write_read_trap	Allows write and read access and trap generation to the community specified.
trap_only	Indicates the community is used only when sending an SNMP trap.

community view

Use the **set community view** command to assign a MIB view to a community.

SNMP Configuration Commands (Talk 6)

Example: `set community view <comm_name> <options>`

Options	Description
all	Allows access to all MIB objects for the named community. All is the default.
view_text_name	Assigns a specified MIB view to the named community.

trap_port

Use the **set trap_port** command to specify a UDP port number, other than the default standard port 162, to send traps to. The default is the standard port.

Example: `set trap_port <udpport#>`

UDP Port Number	Specifies a User Datagram Protocol port other than the standard UDP port (default # 162).

Monitoring SNMP

This section describes the SNMP monitoring commands.

Accessing the SNMP Monitoring Environment

To access the SNMP monitoring environment, enter the following command at the **+** (GWCON) prompt:

```
+ protocol snmp
SNMP>
```

SNMP Monitoring Commands

This section describes the SNMP monitoring commands.

Table 3 lists the SNMP monitoring commands. The SNMP monitoring commands allow you to view the parameters of the SNMP configuration and display some statistics relating to the SNMP agent.

Temporary changes to the runtime SNMP parameters can be made through the monitoring. They will immediately affect the operation of the SNMP agent. If you want to make the temporary changes permanent, then use the SAVE command. If the original SNMP configuration needs to be restored, use the **revert** command. This feature allows you to temporarily alter the behavior of the SNMP agent, without permanently changing the configuration. For the temporary changes to take affect, you must EXIT the SNMP monitoring process.

Enter the SNMP monitoring commands at the `SNMP>` prompt.

Table 3. SNMP 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 xxi.
Add	Adds a community to the list of SNMP communities, an IP address with mask to a community, or a subtree to a MIB view.
Delete	Removes a community from the list of SNMP communities, an IP address with mask from a community, or a subtree from a MIB view.

Table 3. SNMP Monitoring Command Summary (continued)

Command	Function
Enable/Disable	Enables/disables SNMP protocol and traps associated with named communities. These actions are only allowed in the SNMP Configuration environment.
List	Displays the current configuration of SNMP communities, views, access modes, traps, and network addresses.
Revert	Erases the specified changes and restores the settings to the values in the permanent SNMP configuration.
Save	Takes the specified changes and saves then permanently in the SNMP configuration.
Set	Sets a community's access mode or view. A community's access mode is one of the following: • Read and trap generation • Read, write and trap generation • Trap generation only Also allows setting of trap UDP port.
Statistics	Displays statistics about the SNMP agent.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxii.

Add

Use the **add** command to add a community name to the list of SNMP communities, add an address to a community, or assign a portion of the MIB (subtree) to a view.

For information on using the **add** command, see "Add" on page 4.

Delete

Use the **delete** command to delete:

- A specific address.
- A community and all of its addresses.
- A subtree from a view.

For information on using the **delete** command, see "Delete" on page 6.

Disable

Use the **disable** command to disable the SNMP protocol or specified traps on the router. This command is available only in the SNMP configuration environment.

For information on using the **disable** command, see "Disable" on page 8.

Enable

Use the **enable** command to enable the SNMP protocol or specified traps on the router. This command is available only in the SNMP configuration environment.

For information on using the **enable** command, see "Enable" on page 9.

List

Use the **list** command to display the current configuration of SNMP communities, views, access modes, traps, and network addresses.

Syntax:

list all

community

views

list all Displays the current configuration of SNMP communities for Access, Traps, Address, and View. See the description of the **list community** command for details on the options.

See "List" on page 9 for an example of the **list** command.

list community option
Displays the current attributes of a specified SNMP community. Options are access, traps, address, view.

Example: **`list community`** *`option`*

Option	Description
Access	Displays the access modes for the community.
Address	Displays the network address for the community.
Traps	Displays the types of traps generated for the community.
View	Displays the MIB view for the community.

list community access

Example: **`list community access`**

```
Community Name   Access
public           Read, Write, Trap
oxnard           Read, Trap
```

list community traps

Example: **`list community traps`**

```
Community Name   Enabled Traps
public           Link Down, Cold Restart
oxnard           None
```

list community address

Example: **`list community address`**

```
Community Name   IP Address   IP Mask
public           All          N/A
oxnard           1.1.1.2      255.255.255.255
```

list community view

Example: **`list community view`**

```
Community Name   View
public           All
oxnard           mib2
```

list views
Displays the current views for a specified SNMP community.

Example: **`list views`**

```
View Name   Sub-Tree
mib2        1.3.6.1.2.1
```

Revert

Use the **revert** command to erase the specified changes and restore the settings to the values in the permanent SNMP configuration.

Save

Use the **save** command to save the specified changes permanently.

Set

For information on using the **set** command, see “Set” on page 11.

Statistics

Use the **statistics** command to display statistics about the SNMP agent.

Syntax:

statistics

Example: `statistics`

```
SNMP memory in use = 9416
```

SNMP Monitoring Commands (Talk 5)

Chapter 3. Using BGP4

This chapter describes how to use the Border Gateway Protocol (BGP) using the BGP configuration commands.

This chapter contains the following sections:

- "Border Gateway Protocol Overview"
- "How BGP4 Works"
- "Setting Up BGP4" on page 21
- "Sample Policy Definitions" on page 22

Border Gateway Protocol Overview

BGP is an exterior gateway routing protocol used to exchange network reachability information among autonomous systems. An AS is essentially a collection of routers and end nodes that operate under a single administrative organization. Within each AS, routers and end nodes share routing information using an interior gateway protocol. The interior gateway protocol may be either RIP or OSPF.

BGP was introduced in the Internet in the loop-free exchange of routing information between autonomous systems. Based on Classless Inter-Domain Routing (CIDR), BGP has since evolved to support the aggregation and reduction of routing information.

In essence, CIDR is a strategy designed to address the following problems:

- Exhaustion of Class B address space
- Routing table growth

CIDR eliminates the concept of address classes and provides a method for summarizing *n* different routes into single routes. This significantly reduces the amount of routing information that BGP routers must store and exchange.

Note: IBM only supports the latest version of BGP, BGP4, which is defined in RFC 1654. All references to BGP in this chapter and on the interface of IBM's routers are to BGP4, and do not apply to previous versions of BGP.

How BGP4 Works

BGP is an inter-autonomous system routing protocol. In essence, BGP routers selectively collect and advertise reachability information to and from BGP neighbors in their own and other autonomous systems. Reachability information consists of the sequences of AS numbers that form the paths to particular BGP speakers, and the list of IP networks that can be reached via each advertised path. An AS is an administrative group of networks and routers that share reachability information using one or more Interior Gateway Protocols (IGPs), such as RIP or OSPF.

Routers that run BGP are called BGP speakers. These routers function as servers with respect to their BGP neighbors (clients). Each BGP router opens a passive TCP connection on port 179, and listens for incoming connections from neighbors at this well-known address. The router also opens active TCP connections to

enabled BGP neighbors. This TCP connection enables BGP routers to share and update reachability information with neighbors in the same or other autonomous systems.

Connections between BGP speakers in the same AS are called internal BGP (IBGP) connections, while connections between BGP speakers in different autonomous systems are called external BGP (EBGP) connections.

A single AS may have one or many BGP connections to outside autonomous systems. Figure 1 shows two autonomous systems. The BGP speaker in AS1 is attempting to establish a TCP connection with its neighbor in AS2. Once this connection is established, the routers will be able to share reachability information.

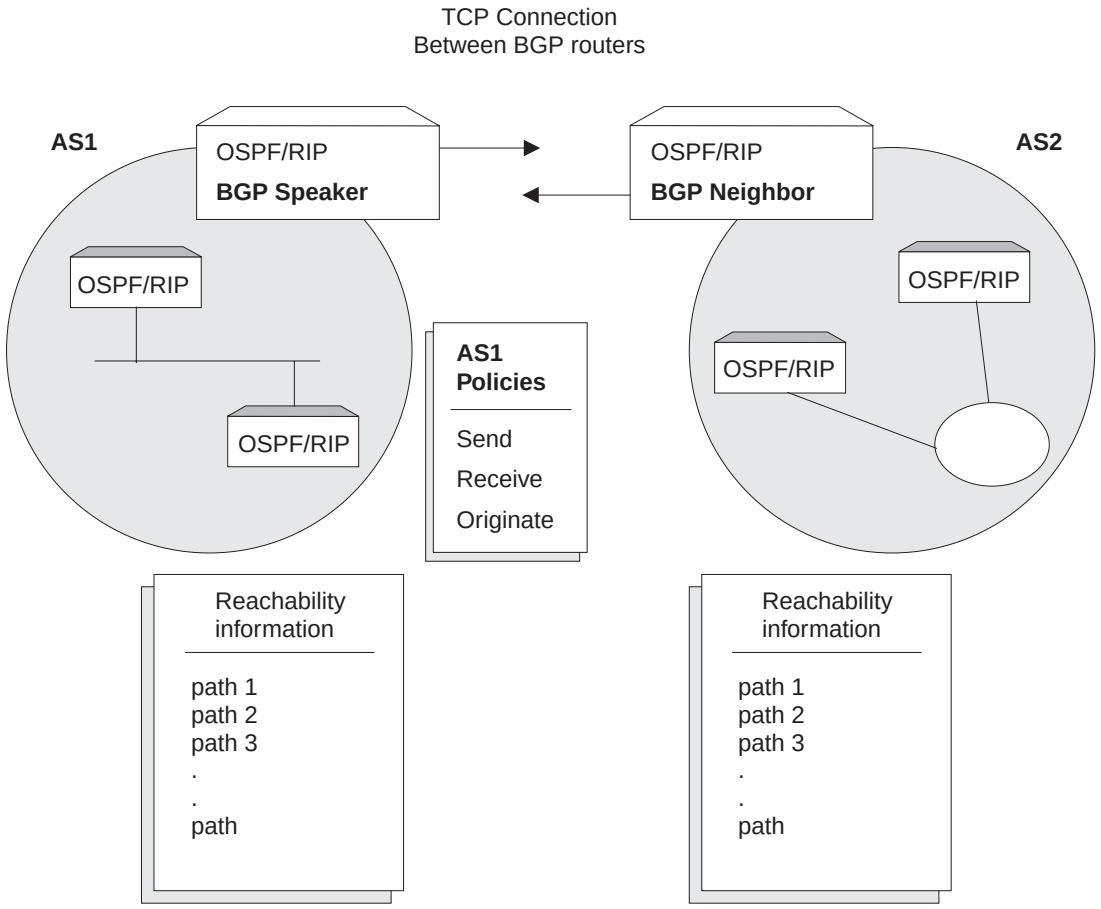

Figure 1. BGP Connections between Two Autonomous Systems. Once the BGP speaker in AS1 establishes a TCP connection with its BGP neighbor in AS2, the two routers can selectively exchange reachability information. The information each router sends or accepts is determined by policies defined for each router.

While the autonomous systems shown in Figure 1 have only one BGP router, each could have multiple connections to other autonomous systems. As an example of this, Figure 2 on page 19 shows three interconnected autonomous systems. AS1 has three BGP connections to outside autonomous systems: one to AS2, one to AS3 and one to ASx. Similarly, AS3 has connections to AS1, AS2 and to ASy.

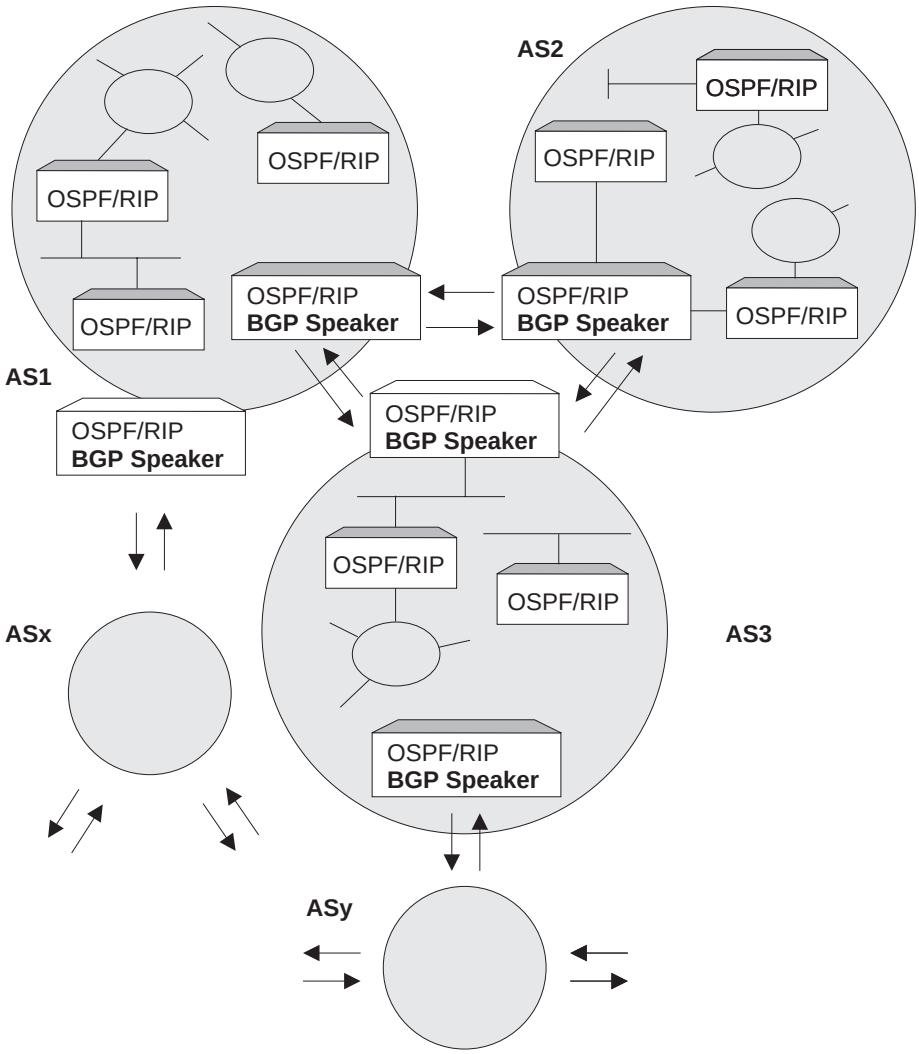

Figure 2. BGP Connections among Three Autonomous Systems. Note that AS1 and AS3 have two BGP speakers.

Once a TCP connection is established, the BGP speaker shown in Figure 1 on page 18 can send its entire routing table to its BGP neighbor in AS2. However, for security or other reasons, it may not be desirable to send reachability information on each network to AS2. Similarly, it may not be desirable for AS2 to receive reachability information on each network in AS1.

Originate, Send, and Receive Policies

Decisions on which reachability information to advertise (send), and which to accept (receive) are made on the basis of explicitly defined policy statements. IBM's BGP implementation supports three types of policy statements:

- Originate Policies
- Send Policies - There are two types of send policies
  - AS based send policies are applied only to a particular AS or all ASs. If no send policies are configured then the destination address is dropped.
  - Neighbor based send policies are applied only to a particular neighbor or neighbors. If there is no neighbor based send policies configured for a

particular neighbor, then AS based send policies are applied. If a neighbor based send policy is configured, then AS based send policy is ignored.

Each send policy statement contains the destination network advertisement classifier and a set of associated actions.

The destination network classification is based on:

– Exact destination network
– Range of destination networks
– Originating AS number
– Any AS number found in AS path attribute

The possible actions are:

– Exclude destination network for advertisement
– Include destination network for advertisement to specific AS or all ASs (using AS based policy) or to a specific neighbor (using neighbor based policy)
– Set the MED value
– ASpath padding

Note: MED and ASpath padding are only applicable to a neighbor based policy.

MED attribute value hints external BGP neighbor about its route preference. Route with the lowest MED attribute value will be preferred. See “Route Preference Process” on page 25 for more information.

- ASpath padding allows you to add additional local AS number multiple times (1 to 10) to the BGP route’s ASpath. Route with the lowest ASpath will be preferred. See “Route Preference Process” on page 25 for more information.
- Receive Policies - there are two types of receive policies.
  – AS based receive policies are applied only to a particular AS or all ASs. If no receive policies are configured then the destination address is dropped.
  – Neighbor based receive policies are applied only to a particular neighbor or neighbors. If there is no neighbor based receive policies configured for a particular neighbor then, AS based receive policies are applied. If neighbor based receive policies are configured then, AS based receive policies are ignored.

Each receive policy statement contains the destination network advertisement classifier and a set of associated actions.

The destination network classification is based on:

– Exact destination network
– Range of destination networks
– Originating AS number
– Any AS number found in AS path attribute

The possible actions are:

– Exclude destination network
– Include destination network from a specific AS or all ASs (using AS based policy) or from a specific neighbor (using neighbor based policy)

- Reset the MED value
- Set weight value
- Set IGP metric value
- Set local preferences value.

Note: MED, weight, and local preferences are only applicable to a neighbor based policy.

Weight value hints local BGP router to select the route based on highest weight value and ignores the route preference algorithm.

BGP Messages

BGP routers use four kinds of messages to communicate with their neighbors: OPEN, KEEP ALIVE, UPDATE, and NOTIFICATION messages.

OPEN

Open messages are the first messages transmitted when a link to a BGP neighbor comes up and establishes a connection.

KEEP ALIVE

Keep alive messages are used by BGP routers to inform one another that a particular connection is alive and working.

UPDATE

Update messages contain the interior routing table information. BGP speakers send update messages only when there is a change in their routing tables.

NOTIFICATION

Notification messages are sent whenever a BGP speaker detects a condition that forces it to terminate an existing connection. These messages are advertised before the connection is transmitted.

Setting Up BGP4

Setting up BGP involves three basic steps:

1. “Enabling BGP” on page 22.

   Enabling BGP requires you to specify the BGP router’s unique AS Number. AS numbers are assigned by Stanford Research Institute Network Information Center.

2. “Defining BGP Neighbors” on page 22.

   BGP Neighbors are BGP routers with which a BGP speaker establishes a TCP connection. Once neighbors are defined, connections to them are established by default.

3. “Adding Policies” on page 22.

   The *policies* you establish determine which routes will be imported and exported by the BGP speaker. You can set up policies for different purposes. See “Sample Policy Definitions” on page 22 for more information.

Enabling BGP

You enable BGP using the **enable BGP speaker** command as shown.

```
BGP Config> enable BGP speaker
AS [0]? 167
TCP segment size [1024]?
```

The *AS number* must be in the range 1 to 65535. The *TCP segment* size must be in the range 1 to 65535. The default value for *TCP segment* is 1024. This number represents the maximum segment size BGP will use for passive TCP connections.

After you have issued the **enable bgp** command you must reboot the device to enable BGP.

Defining BGP Neighbors

After enabling a BGP speaker, you must define its neighbors. BGP neighbors can be internal or external. Internal neighbors exist in the same AS and do not need to have a direct connection to one another. External neighbors exist in different autonomous systems. These must have a direct connection to one another.

To define internal or external BGP neighbors, use the **add neighbor** command. You must specify the IP address of the neighbor, and assign an AS number to the neighbor as shown below. Internal neighbors must have the same AS number as the BGP speaker.

```
BGP Config> add neighbor 192.0.190.178
AS [0]? 178
Init timer [12]? 30
Connect timer [120]?
Hold timer [90]? 30
TCP segment size [1024]? 512
```

Use the **reset neighbor** command to activate the specified BGP neighbor, based on the neighbor configuration parameters stored in the configuration memory.

Adding Policies

IBM's BGP implementation supports three policy commands:

- *Originate Policy*. This enables you to select the interior gateway protocol (IGP) networks to export.
- *Receive Policy*. This enables you to select the route information to import from BGP peers.
- *Send Policy*. This enables you to select the route information to export to peers. Note that exportable route information can include information collected from neighboring autonomous systems, as well as the routes that originate in the IGP.

If you added or modified a neighbor based policy use the **reset neighbor** command to activate the neighbor policy. If you added or modified an AS-based policy you must reboot the device.

Sample Policy Definitions

This section provides a set of examples of some specific policies you can set up for a BGP speaker. All policies are defined using the BGP **add** command. See "Add" on page 28 for the syntax of the **add** command.

Originate Policy Examples

Include All Routes for Advertisement

This example includes all routes in the BGP speaker's IGP routing table for advertisement. In this sense, you can view this command as the "default" originate policy statement for BGP.

Notice that the command specifies a range of addresses, rather than a single (exact) address.

```
BGP Config> add originate-policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

Exclude a Range of Routes

This example also specifies a range, but in this case the goal is to prevent the BGP Speaker from advertising addresses in this range to its neighbors.

This example excludes all routes in the range 194.10.16.0 to 194.10.31.255 from the IGP routing table, which in turn prevents them from being advertised.

```
BGP Config> add originate-policy exclusive
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

The tag is the received RIP information. You can select networks based on a particular tag value for advertisement. See the description of the **Set** command in Configuring and Monitoring IP in the *Multiprotocol Switched Services (MSS) Configuring Interfaces and Features Volume 1* for information on setting the tag value.

By default, only classfull routes from the BGP speaker's IGP routing table will be selected for advertisement. To select a classless route for advertisement use the bgp-subnets **patch** command. For information about the **patch** see the chapter "The Configuration Process (CONFIG - Talk 6) Commands" in *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide*.

AS Based Receive Policy Examples

Import all Routes from all BGP Neighbors

This example ensures that the BGP speaker will import all routes from all of its neighbors into its IGP routing table.

```
BGP Config> add receive-policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]?
Adjacent AS# [0]?
IGP-metric [0]?
```

IGP-metric specifies the metric value with which the accepted routes are imported into the speaker's IGP routing table. You are only prompted to enter a value for IGP-metric only when setting up a policy for route inclusion.

If *IGP-metric* is -1, these routes will not be imported into IGP; thus, routes are not re-advertisable.

Block Specific Routes from an Originating AS

This example will prevent the BGP speaker from importing any routes originating at AS 168 from neighboring AS 165. You might use this command if you do not want the BGP speaker to receive any routes from AS 168 for security reasons.

```
BGP Config> add receive-policy exclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]? 168
Adjacent AS# [0]? 165
```

Block Specific ASpath

This example will prevent the BGP speaker from importing any route that has AS 175 in its ASpath list.

```
BGP Config> add no-receive
Enter AS: [0]? 175
```

Neighbor Based Receive Policy Examples

Import all routes from a specific BGP neighbor, set weight = 100

This example will allow you to import all routes from BGP neighbor 192.0.190.178. All routes will have a weight value of 100 and IGP-metric value of 1.

Define the policy list name for receive policy.

```
BGP Config> add policy-list
Name[]?S1_100_r
Policy Type(Receive/Send)[Receive]?Receive
```

Attach the defined receive policy list name to a specific neighbor.

```
BGP Config> attach policy-to-neighbor
Neighbor address [0.0.0.0]?192.0.190.178
First receive policy list name (none for global AS based policy)[]?S1_100_r
Second receive policy list name (none for exit)[]?
```

Add receive policies for neighbor using **update** and **add** command.

```
BGP Config>update policy S1_100_r
Policy-list S1_100_r Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Weight [0]? 100
Local-Pref [0]?
IGP-metric [0]? 1
```

AS based Send Policy Examples

Restrict Route Advertisement to a Specific AS

This example restricts the BGP speaker. The speaker cannot advertise routes in the address range 143.116.0.0 to 143.116.255.255, that originate from AS 165, to autonomous system 168.

```
BGP Config> add send exclusive
Network Prefix [0.0.0.0]? 143.116.0.0
Network Mask [0.0.0.0]? 255.255.0.0
Address Match (Exact/Range) [Exact]? range
Tag [0]? 165
Adjacent AS# [0]? 168
```

Advertise All Known Routes

This example ensures that the BGP speaker will advertise all routes originated from its IGP, and all routes learned from its neighboring autonomous systems.

```
BGP Config> add send policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
Adjacent AS# [0]?
```

Neighbor Based Send Policy Examples

Advertise All Known Routes to a Specific Neighbor with MED Attribute value = 100

This example will allow you to advertise all routes to a BGP neighbor 192.0.190.178. All advertise routes will have a MED value of 100.

Define the policy list name for send policy.

```
BGP Config> add policy-list
Name[]?S1_100_s
Policy Type(Receive/Send)[Receive]?Send
```

Attach the defined send policy list name(s) to a specific neighbor.

```
BGP Config> attach policy-to-neighbor
Neighbor address [0.0.0.0]?192.0.190.178
First send policy list name (none for global AS based policy)[]?S1_100_s
Second send policy list name (none for exit)[]?
```

Add the send policies for neighbor using the **update** and **add** commands.

```
BGP Config>update policy S1_100_s
Policy-list S1_100_s Config>add
Policy type (Inclusive/Exclusive) [Exclusive]?
Network prefix [0.0.0.0]?
Network mask [0.0.0.0]?
Address match (exact/range) [range]?
Originating AS# [0]?
TAG [0]?
MED [0]? 100
# of AS to pad [0]?
```

Route Preference Process

When BGP speaker receives a path for particular destination from its peer, BGP goes through following process for selecting a best possible path.

- Apply receiving policies based on configuration.
- If a destination is permitted by receiving policies, then calculate Degree of Preference for the received destination, based on shorter ASpath length and Origin type.
- If there are several paths to the same destination then, execute the path selection process. Select best possible path by comparing the new path with existing selected best path. If the new path is selected as the best path then

install the new path in the IP forwarding table.

- Advertised the selected best path to its External/Internal BGP peers, subject to send policies.

Path Selection Process

The best path is selected based on the following order.

- Prefer the path that has been originated by this router.
- If path is not originated by this router then, prefer the path which has highest configured Weight value.
- If path have same weight value then, prefer the path which has highest configured local-preference value.
- If paths have same local-preference value then, prefer the path which has highest Degree of Preference.
  - The path, which has shortest ASpath length, is given higher degree of preference.
  - If paths have same ASpath length then, Origin type IGP is preferred over EGP and Incomplete.
- If paths have same Degree of Preference then, prefer the path which has the lowest MED attribute value.
- If paths have same MED attribute value then, prefer External(EBGP) over internal (IBGP) route.
- If paths are still same then, prefer the path with lowest BGP-ID.

Chapter 4. Configuring and Monitoring BGP4

This chapter describes the BGP configuring and monitoring commands and includes the following sections:

Accessing the BGP4 Configuration Environment

To access the BGP configuration environment, enter the following command at the `Config>` prompt:

```
Config> Protocol BGP
BGP Config>
```

BGP4 Configuration Commands

This section describes the BGP configuration commands. These commands allow you to modify the BGP protocol behavior to meet your specific requirements. Some amount of configuration is necessary to produce a fully functional BGP router. Enter BGP configuration commands at the `BGP config>` prompt.

Table 4. BGP 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 xxi.
Add	Add BGP neighbors and policies.
Attach	Attaches receive and send policy-list to a particular neighbor.
Change	Modifies information that was originally entered with the **add** command.
Delete	Deletes BGP configuration information that had been entered with the **add** command.
Disable	Disables certain BGP features that have been turned on by the **enable** command.
Enable	Enables BGP speakers, BGP neighbors or Classless BGP.
List	Displays BGP configuration items.
Move	Changes the order in which policies and aggregates are defined.
Set	Sets the IP-route-table-scan-timer.
Update	Manipulates a policy in a configured policy-list name using the submenu **add**, **delete**, **change** and **move** commands.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxii.

Add

Use the **add** command to add BGP information to your configuration.

Syntax:

add aggregate . . .
neighbor . . .
no-receive asnum . . .
originate-policy . . .
policy-list . . .
receive-policy . . .
send-policy. . .

aggregate *network prefix network mask*

The **add aggregate** command causes the BGP speaker to aggregate a block of addresses, and advertise a single route to its BGP neighbors. You must specify the network prefix common to all the routes being aggregated and its mask. The following example illustrates how to aggregate a block of addresses from 194.10.16.0 through 194.10.31.255.

1. The *Network Prefix* is the addresses being affected. The prefix is the first address in a range of addresses specified in a BGP policy.

   Valid Values: Any valid IP address.

   Default Value: none

2. The *Network Mask* applies to the address specified in Network Prefix to generate an address used in a BGP policy.

   Valid Values: Any valid IP address.

   Default Value: none

Example:

```
add aggregate
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
```

When you add an aggregate definition, remember to define a policy to block the aggregated routes from being exported. If you do not, the router will advertise both the individual routes and the aggregate you have defined. This does not apply when you are aggregating the routes, which are originated from it's IGP routing table.

neighbor *neighbor IP address as# init timer connect timer hold timer keep alive timer tcp segment size*

Use the **add neighbor** command to define a BGP neighbor. The neighbor can be internal to the BGP speaker's AS, or external.

1. The IP address is the address of the neighbor you wish to peer with. It could be within your own autonomous system or in another autonomous system. If it is an external neighbor, both BGP speakers must share the same network. There is no such restriction for internal neighbors. The address has:

   Valid Values: Any valid IP address.

   Default Value: none

2. The AS number is your own autonomous system number for internal neighbor or neighbor's autonomous system number. The AS number of the neighbor has:

   Valid Values: An integer in the range of 0 - 65535

   Default Value: none

3. The *Init timer* to specifies the amount of time the BGP speaker waits to initialize resources and reinitiate transport connection with the neighbor in case the speaker has previously changed to IDLE state due to an error. If the error persists, this timer increases exponentially.

   Valid Values: 0 to 65535 seconds.

   Default Value: 12 seconds

4. The *Connect timer* specifies the amount of time the BGP speaker waits to reinitiate transport connection to its neighbor, if the TCP connection fails while in either CONNECT or ACTIVE state. In the mean time, the BGP speaker continues to listen for any connection that may be initiated by its neighbor.

   Valid Values: 0 to 65535 seconds.

   Default Value: 120 seconds

5. Enter the *Hold timer* to specify the length of time the BGP speaker waits before assuming that the neighbor is unreachable. Both neighbors exchange the configured information in OPEN message and choose the smaller of the two timers as their negotiated Hold Timer value.

   Once neighbors have established BGP connection, they exchange Keepalive messages at frequent intervals to ensure that the connection is still alive and the neighbors are reachable. The Keep-Alive timer interval is calculated to be one-third of the negotiated hold timer value. Hence the hold timer value must be either zero or at least three seconds.

   Note that on switched lines, you may wish to have the Hold Timer value of zero to save bandwidth by not sending Keepalives at frequent intervals.

   Valid Values: 0 to 65535 seconds.

   Default Value: 90 seconds

6. The *TCP segment size* specifies the maximum data size that may be exchanged on the TCP connection with a neighbor. This value is used for active TCP connection with the neighbor.

   Valid Values: 0 to 65535 bytes.

   Default Value: 1024 bytes

Example:

```
        add neighbor

Neighbor address [0.0.0.0]? 192.0.251.165
AS [0]? 165
Init timer [12]?
Connect timer [120]?
Hold timer [90]?
TCP segment size [1024]?
```

no-receive *asnum*

Use the **add no-receive asnum** to exclude AS-paths if the particular AS number appears anywhere inside the AS-path list.

The *AS number* has:

Valid Values: 0 to 65535

Default Value: none

Example:

```
add no-receive
Enter AS: [0]? 178
```

originate-policy *(exclusive/ inclusive) network prefix network mask address match (Exact/Range) tag*

Use the **add originate-policy** command to create a policy that determines whether a specific address, or range of addresses, can be imported to the BGP speaker's routing table from the IGP routing table.

Exclusive
Exclusive policies prevent route information from being included in the BGP speaker's routing table.

Inclusive
Inclusive policies ensure that specific routes will be included in the BGP speaker's routing table.

Network prefix
The network prefix for the addresses being affected.

Address match
The address, or range of addresses, that will be affected by the policy statement.

Tag The value that has been set for a particular AS. All tag values match that of the AS from which they were learned.

Exclusive policies prevent route information from being included in the BGP speaker's routing table.

1. The *Network Prefix* is the addresses being affected.

   Valid Values: Any valid IP address.

   Default Value: none
2. Enter the *Network Mask* to be applied to the address specified in Network Prefix to generate an address used in a BGP policy.

   Valid Values: Any valid IP address.

   Default Value: none
3. Select whether the *Address match* is to be a range of addresses or an exact address.
4. A *TAG* is the value that has been set for a particular AS. Tag values match that of the AS from which they were learned.

   Valid Values: 0 to 65535

   Default Value: none

The following example includes all routes in the BGP speaker's IGP routing table to be advertised.

Example:

```
add originate-policy exclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

See "Originate Policy Examples" on page 23 for detailed examples of this policy command.

policy-list

Use the **add policy-list** command to configure a group of policy, which can be attached to a specific neighbor using the **attach policy-to-neighbor**command.

Example: add policy-list

```
Name[]? nbr1-rcv
Policy Type(Receive/Send)[Receive]?Receive
```

Example: add policy-list

```
Name[]? nbr1-snd
Policy Type(Receive/Send)[Receive]?Send
```

Note: See “Neighbor Based Receive Policy Examples” on page 24 and “Neighbor Based Send Policy Examples” on page 25 for detailed examples of this policy command.

receive-policy *(exclusive/ inclusive) network prefix network mask address match originating as# adjacent as# igpmetric (inclusive only)*

Use the **add receive-policy** command to determine what routes will be imported to the BGP speaker’s routing table.

Exclusive policies prevent route information from being included in the BGP speaker’s routing table.

1. The *Network Prefix* is the addresses being affected.

   Valid Values: Any valid IP address.

   Default Value: none
2. The *Network Mask* applies to the address specified in Network Prefix to generate an address used in a BGP policy.

   Valid Values: Any valid IP mask.

   Default Value: none
3. The *Address match* is a range of addresses or an exact address.
4. An *Originating AS#* has:

   Valid Values: 0 to 65535

   Default Value: none
5. The *Adjacent AS#* to specifies the neighboring AS number.

   Valid Values: 0 to 65535

   Default Value: none

Example:

```
add receive-policy exclusive

Network Prefix [0.0.0.0]? 10.0.0.0
Network Mask [0.0.0.0]?  255.0.0.0
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]? 168
Adjacent AS# [0]? 165
```

See “AS Based Receive Policy Examples” on page 23 for detailed examples of this policy command.

send-policy *(exclusive/ inclusive) network prefix network mask address match tag adjacent as#*

Use the **add send-policy** command to create policies that determine which of the BGP speaker’s learned routes will be readvertised. These routes could be internal or external to the BGP speaker’s AS.

Exclusive policies prevent route information from being included in the BGP speaker's routing table.

1. The *Network Prefix* is for the addresses being affected.

   Valid Values: Any valid IP address.

   Default Value: none
2. The *Network Mask* applies to the address specified in Network Prefix to generate an address used in a BGP policy.

   Valid Values: Any valid IP address.

   Default Value: none
3. The *Address match* is a range of addresses or an exact address.
4. A *TAG*. is the value that has been set for a particular AS. Tag values match that of the AS from which they were learned.

   Valid Values: 0 to 65535

   Default Value: none
5. The *Adjacent AS#* specifies the neighboring AS number.

   Valid Values: 0 to 65535

   Default Value: none

Example:

add send exclusive

```
Network Prefix [0.0.0.0]? 180.220.0.0
Network Mask [0.0.0.0]? 255.255.0.0
Address Match (Exact/Range) [Exact]? range
Tag [0]?
Adjacent AS# [0]? 25
```

See "AS based Send Policy Examples" on page 24 for detailed examples of this policy command.

Attach

Use the **attach policy-to-neighbor** command to attach a configured policy-list name to a specific neighbor. You can attach up to three receive and three send policy-list names.

Syntax:

attach policy-to-neighbor

Example: attach policy-to-neighbor

```
Neighbor address [0.0.0.0]? 192.0.251.165
First receive policy list name (none for global AS based policy)[]? nbr1-rcv
Second receive policy list name (none for exit)[]?
First send policy list name (none for global AS based policy)[]? nbr1-snd
Second send policy list name (none for exit)[]?
```

Note: See "Neighbor Based Receive Policy Examples" on page 24 and "Neighbor Based Send Policy Examples" on page 25 for detailed examples of this policy command.

Change

Use the **change** command to change a BGP configuration item previously installed by the add command.

Syntax:

change aggregate . . .
neighbor . . .
originate-policy . . .
policy-to-neighbor
receive-policy . . .
send-policy. . .

aggregate *index# network prefix network mask*

This example changes the current aggregate (aggregate 1). The change causes aggregate 1 to use a different network prefix and mask to aggregate all routes in the address range from 128.185.0.0 to 128.185.255.255.

Example:

```
change aggregate 1

Network Prefix [128.185.0.0]? 128.128.0.0
Network Mask [255.255.0.0]? 255.192.0.0
```

neighbor *neighbor IP address as# init timer connect timer hold timer keep alive timer tcp segment size*

The following example changes the value of the hold timer to zero for neighbor 192.0.251.165.

The *neighbor address* to be modified has:

Valid Values: Any valid IP address.

Default Value: none

Example:

```
change neighbor 192.0.251.165

AS [165]?
Init timer [12]?
Connect timer [60]?
Hold timer [12]? 0
TCP segment size [1024]?
```

originate-policy *index# (exclusive/ inclusive) network prefix network mask address match tag*

Use the **change originate-policy** command to alter an existing originate policy definition.

This example alters the BGP speaker's originate policy. Rather than excluding networks with prefix 194.10.16.0 from the IGP routing table, the policy will now include all routes.

Example:

```
change originate-policy

Enter index of originate-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [194.10.16.0]? 0.0.0.0
Network Mask [255.255.240.0]? 0.0.0.0
Address Match (Exact/Range) [Range]?
Tag [0]?
```

policy-to-neighbor

Use the **change policy-to-neighbor** command to change a policy-list attachment to a particular neighbor.

Example:

```
change policy-to-neighbor

Neighbor address [0.0.0.0]? 192.0.251.165
First receive policy list name to be changed[nbr1-rcv]?
Second receive policy list name to be changed[]?
```

```
Third receive policy list name to be changed[]?
First send policy list name to be changed[nbr1-snd]?
Second send policy list name to be changed[]?
Third send policy list name to be changed[]?
```

receive-policy *index# (exclusive/inclusive) network prefix network mask address match originating as# adjacent as# igpmetric (inclusive only)*

Use the **change receive-policy** command to alter an existing receive policy definition.

This example adds a restriction to the BGP speaker's receive-policy. Rather than import route information from every BGP peer into its IGP routing table, it will now prevent routes from AS 165 from being imported.

Example:

```
change receive-policy

Enter index of receive-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Adjacent AS# [0]? 165
```

send-policy *index# (exclusive/ inclusive) network prefix network mask address match tag adjacent as#*

Use the **change send-policy** command to alter an existing send policy to one that is more inclusive, or more exclusive.

This example adds a restriction to the BGP speaker's send policy. The restriction ensures that all routes in the address range 194.10.16.0 to 194.10.31.255 will be excluded when advertising to autonomous system 165.

Example:

```
change send-policy

Enter index of send-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]? 165
```

Delete

Use the **delete** command to delete a BGP configuration item previously installed by the **add** command.

Syntax:

delete

- aggregate . . .
- neighbor . . .
- no-receive . . .
- originate-policy . . .
- policy-list . . .
- policy-to-neighbor
- receive-policy . . .
- send-policy. . .

aggregate *index#*

You must specify the index number of the aggregate you want to delete. The index number is equivalent to the AS number.

Example: `delete aggregate 1`

neighbor *neighbor IP address*

Use this command to delete a BGP neighbor. You must specify the neighbor's network address.

The *neighbor's network address to be deleted* has:

Valid Values: Any valid IP address.

Default Value: none

Example: `delete neighbor 192.0.251.165`

no-receive *as*

Use this command to delete the no-receive policy set up for a particular AS. You must specify the AS number.

The *AS number* has:

Valid Values: 0 to 65535

Default Value: none

Example: `delete no-receive 168`

originate-policy *index#*

Use this command to delete a specific originate policy. You must specify the index number associated with the policy.

Example: `delete originate-policy 2`

policy-list

Use the **delete policy-list** command to delete a policy-list.

Example: `delete policy-list`

```
Name of policy-list to delete []? nbr1-rcv
All policies defined for 'nbr1-rcv' will be deleted.
Are you sure you want to delete (Yes or [No]? Yes
Policy-list 'nbr1-rcv' is deleted.
```

The policy-to-neighbor attachment will be adjusted accordingly.

policy-to-neighbor

Use the **delete policy-to-neighbor** command to delete an existing policy-list name attachment to a particular neighbor.

Example: `delete policy-to-neighbor`

```
Neighbor address [192.0.251.165]?
Remove first receive policy-list name [nbr1-rcv]
Are you sure you want to remove (Yes or [No])? yes
Remove first send policy-list name [nbr1-snd]
Are you sure you want to remove (Yes or [No])? yes
```

receive-policy *index#*

Use this command to delete a specific receive policy. You must specify the index number associated with the policy.

Example: `delete receive-policy`

```
Enter index of receive-policy to be deleted [1]?
```

send-policy *index#*
Use this command to delete a specific send policy. You must specify the index number associated with the policy.

Example: `delete send-policy 4`

Disable

Use the **disable** command to disable a previously enabled BGP neighbor or speaker. Note that neighbors are implicitly enabled whenever added with the **add** command.

Syntax:

disable BGP speaker
classless-bgp
compare-med-from-diff-AS
neighbor . . .

bgp speaker
Use the **disable bgp speaker** command to disable the BGP protocol.

Example: `disable bgp speaker`

classless-bgp
Use this command to disable a classless route for advertisement.

Example: `disable classless-bgp`

Note: Be sure that the **patch bgp-subnets** command is disabled.

compare-med-from-diff-AS
Use this command to disable a MED comparison between different ASs.

Example: `disable compare-med-from-diff-AS`

neighbor *neighbor IP address*
The *neighbor address* has:

Valid Values: Any valid IP address.

Default Value: none

Example: `disable neighbor 192.0.190.178`

Enable

Use the **enable** command to activate the BGP features, capabilities, and information added to your BGP configuration.

Syntax:

enable BGP speaker
classless-bgp
compare-med-from-diff-AS
neighbor . . .

bgp speaker *as# tcp segment size*
Use the enable bgp speaker command to enable the BGP protocol.

Note: IBM only supports the latest version of BGP - BGP4, which is defined in RFC 1654.

1. The *AS number* is associated with this collection of routers and nodes.

   Valid Values: 0 to 65535

   Default Value: none

2. Enter the *TCP segment size* to specify the maximum segment size that BGP should use for passive TCP connections.

   Valid Values: 0 to 65535 bytes.

   Default Value: 1024 bytes

Example:

```
enable bgp speaker

AS [0]? 165
TCP segment size [1024]?
```

classless-bgp neighbor

Use this command to enable a classless route for advertisement.

Example: `enable classless-bgp`

compare-med-from-diff-AS

Use this command to enable MED comparison between different ASs.

Example: `enable compare-med-from-diff-AS`

neighbor *neighbor IP address*

Use this command to enable a BGP neighbor.

The *neighbor address* has:

Valid Values: Any valid IP address.

Default Value: none

Example: `enable neighbor 192.0.190.178`

List

Use the **list** command to display various pieces of the BGP configuration data, depending on the particular subcommand invoked.

Syntax:

list

- aggregate
- all
- BGP speaker
- neighbor
- no-receive
- originate-policy
- policy-list . . .
- policy-to-neighbor
- receive-policy
- send-policy

BGP4 Configuration Commands (Talk 6)

aggregate

Use the **list aggregate** command to all aggregated routes defined with the **add aggregate** command.

Example: `list aggregate`

```
Aggregation:
Index    Prefix              Mask
1         194.10.16.0        255.255.240.0
```

all

Use the **list all** command to list the BGP neighbors, policies, aggregated routes, and no-receive-as records in the current BGP configuration.

Example: `list all`

```
                 BGP Protocol:          Enabled
                 AS:                    167
                 TCP-Segment Size:      1024
                 Neighbors and their AS:

                                        Init    Conn    Hold    TCPSEG
Address          State     AS          Timer   Timer   Timer   Size
128.185.250.168  ENABLD    168         12      60      12      1024
192.0.251.165    ENABLD    165         12      60      12      1024

Receive-Policies:
Index  Type  Prefix       Mask       Match  OrgAS  AdjAS IGPmetric
1      INCL  0.0.0.0      0.0.0.0    Range  0      0      0

Send-Policies:
Index  Type  Prefix       Mask       Match  Tag    AdjAS
1      INCL  0.0.0.0      0.0.0.0    Range  0      0

Originate-Policies:
Index  Type  Prefix       Mask             Match  Tag
1      EXCL  194.10.16.0  255.255.240.0    Range  0

Aggregation:

Index  Prefix             Mask
1      194.10.16.0        255.255.240.0
No no-receive-AS records in configuration.
```

bgp speaker

Use the **list bgp speaker** command to derive information on the BGP speaker. The information provided is as follows:

Example:

`list BGP speaker`

```
BGP Protocol:          Enabled
AS:                    165
TCP-Segment Size:      1024
```

neighbor

Use the **list neighbor** command to derive information on BGP neighbors.

Example: `list neighbor`

```
Neighbors and their AS:

                                        Init    Conn    Hold    TCPSEG
Address          State     AS          Timer   Timer   Timer   Size

128.185.252.168  ENABLD    168         12      60      12      1024
192.0.190.178    DISBLD    178         12      60      12      1024
192.0.251.167    ENABLD    167         12      60      12      1024
```

no-receive

Use the **list no-receive** command to derive information on no-receive-AS definitions that have been added to the BGP configuration.

Example: `list no-receive`

```
AS-PATH with following autonomous systems will be discarded:
AS  178
AS  165
```

originate-policy *all index prefix*

Use the **list originate-policy** command to derive information on the originate policies that have been added to the BGP configuration.

Example: `list originate-policy`

```
Originate-Policies:
Index  Type  Prefix          Mask            Match  Tag
1      EXCL  194.10.16.0     255.255.240.0   Range  0
2      INCL  0.0.0.0         0.0.0.0         Range  0
```

policy-list

Use the **list policy-list** command to list configured policy-list names.

Example: `list policy-list`

```
BGP Config>li policy list
Policy list:
nbr1-rcv  Receive
nbr1-snd  Send
```

policy-to-neighbor

Use the **list policy-to-neighbor** command to list policies attached to neighbors.

Example: `list policy-to-neighbor`

```
Neighbor addrs  receive         send
192.0.251.165   nbr1-rcv        nbr1-snd
```

receive-policy adj-as-number *all* **or** *index* **or** *prefix*

Use the **list receive-policy** command to derive information on the receive policies that have been added to the BGP configuration. You can display all receive policies defined for an AS, or display policies by index or prefix number.

Example: `list receive-policy`

```
Receive-Policies:
Index  Type  Prefix      Mask        Match  OrgAS  AdjAS  IGPmetric
1      EXCL  0.0.0.0     0.0.0.0     Range  178    165
2      INCL  0.0.0.0     0.0.0.0     Range  0      0      0
```

send-policy adj-as-number *all* **or** *index* **or** *prefix*

Use the **list send-policy** command to display information on send policies defined for specified autonomous systems. You can display all send policies defined for an AS, or display policies by index or prefix number.

Example: `list send-policy`

```
Send-Policies:
Index  Type  Prefix      Mask           Match Tag    AdjAS
1      EXCL  194.10.16.0 255.255.240.0  Range   0    165
2      INCL   0.0.0.0    0.0.0.0        Range   0    0
```

Move

Use the **move** command to change the order in which policies and aggregates have been defined. This changes the order in which the router applies existing policies to route information. Before using this command, it is advisable to use the **list** command to see what policies have been defined.

Syntax:

move *aggregate* or *originate-policy* or *receive-policy* or *send-policy*

Example:

```
move originate-policy
Enter index of originate-policy to move [1]? 3
Move record AFTER record number [0]?
```

Set

Use the **set** command to set the IP-route-table-scan-timer. The IP-route-table-scan-timer value is used to set the IP forwarding table scanning time interval for BGP updates.

Syntax:

set ip-route-table-scan-timer

Example:

```
set ip-route-table-scan-timer
```

Update

Use the **update** command and sub-commands to manipulate policies.

Syntax:

update *policy-list*

Receive Policy Example:

```
update policy-list
Name[]? nbr1-rcv
```

Add

Use the **Add** command to add receive policies within the **update** command.

```
BGP nbr1-rcv: Receive Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Weight [0]?
Local-Pref [0]?
IGP-metric [0]?
```

Note: There will be no prompting for MED, Local-pref, Weight, and IGP-metric parameters for exclusive receive policy. MED and Local-pref values will be used from received advertisement if they are configured as value ’0’. The value ’0’ for the weight parameter indicates to ignore the weight value in the route selection process.

Change

Use the **Change** command to change policies within the **update** command.

Example:

```
Enter index of receive-policy to be modified [1]?
```

Delete

Use the **delete** command to delete policies within the **update** command.

Example:

```
Enter index of receive-policy to be deleted [1]?
```

Move

Use the **Move** command to move policies within the **update** command.

Example:

```
Enter index of receive-policy to move [1]?
Move record after record number [0]?
```

List

Use the **list policy-list** command to list receive policies within the **update** command.

Example: list policy-list

```
Receive policy list for 'name':
                  T Prefix            Match OrgAS AnyAS MED   Weight Lpref IGPmetric
               1  I 0.0.0.0/0         Range 0     0     0     0      0     1
```

Send Policy Example:

```
update policy-list
Name[]? nbr1-rcv
```

Add

Use the **Add** command to add send policies within the **update** command.

```
BGP nbr1-rcv: Send Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
TAG [0]
MED [0]?
# of AS to pad[0]?
```

Note: There will be no prompting for MED and ASpad parameters for exclusive send policy. The value 0 for the MED parameter indicates that MED attribute is not included in advertisement. The value 0 for the ASpad parameter indicates that there will be no additional local AS number inserted in the ASpath.

Change

Use the **Change** command to change policies within the **update** command.

Example:

```
Enter index of send-policy to be modified [1]?
```

Delete

Use the **delete** command to delete policies within the **update** command.

Example:

```
Enter index of send-policy to be deleted [1]?
```

Move

Use the **Move** command to move policies within the **update** command.

Example:

```
Enter index of send-policy to move [1]?
Move record after record number [0]?
```

List

Use the **list policy-list** command to list send policies within the **update** command.

Example: list policy-list

```
Send policy list for 'name':
                    T Prefix             Match OrgAS AnyAS Tag   MED    ASpad
                1   I 0.0.0.0/0          Range 0     0     0     0      0
```

Accessing the BGP Monitoring Environment

To access the BGP configuration environment, enter the following command at the Config> prompt:

```
Config> Protocol BGP
BGP>
```

BGP4 Monitoring Commands

This section describes the BGP monitoring commands. These commands allow you to modify the BGP protocol behavior to meet your specific requirements. Some amount of configuration is necessary to produce a fully functional BGP router. Enter BGP monitoring commands at the BGP> monitoring prompt.

Table 5. BGP 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 xxi.
Destinations	Displays all entries in the BGP routing table.
Dump routing tables	Lists the contents of the IP routing table.
Neighbors	Displays currently active neighbors.
Parameter	Displays installed BGP globals in the BGP system.
Paths	Displays all available paths in the database.
Ping	Sends ICMP Echo Requests to another host once a second and watch for a response. This command can be used to isolate trouble in an internetwork environment.
Policy-list	Displays the current installed policy for specific neighbor and usage statics of each policy.

Table 5. BGP Monitoring Command Summary (continued)

Command	Function
Traceroute	Displays the complete path (hop-by-hop) to a particular destination.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxii.

Destinations

Use the **destinations** command to dump all BGP routing table entries, or to display information on routes advertised to, or received from, specified BGP neighbor addresses (destinations).

Syntax:

destinations

net address/net address net mask

advertised-to *network address*

received-from *network address*

Example: destination

```
Network/MaskLen    NextHop         MED   Weight LPref AAG AGRAS ORG AS-Path
142.4.0.0/16       192.0.251.165   100   0      0     No  0     IGP seq[165-178]
```

destinations *net address*

Displays detailed information on the specified route or destination network. The command shows how a specific route was learned, the best path to a specific destination, the metric associated with the route, and other information.

Example: `destinations 142.4.0.0`

```
Network/MaskLen   NextHop        MED  Weight LPref     AAG AGRAS ORG ASPath
142.4.0.0/16      192.0.251.165  100  0      0         No  0     IGP seq[165-178]

Dest:142.4.0.0/16, Age:180, Upd#:13,LastSent:0001:53:32

Eligible paths: 2
PathID: 8  (Best Path)
        ASpath: seq[165-178]
        Origin: IGP, Pref: 507, LocalPref: 0
        Metric: 0, Weight: 0, MED: 100
        NextHop: 192.0.251.165, Neighbor: 192.0.251.165
        AtomicAggr: No

PathID: 21
        ASpath: seq[168-165-178]
        Origin: IGP, Pref: 505, LocalPref: 0
        Metric: 0, Weight: 0, MED: 0
        NextHop: 128.185.250.168, Neighbor: 128.185.250.168
        AtomicAggr: No
```

ASpath

Enumeration of autonomous systems along the path.

-seq: Sequence of autonomous systems in order in the path

-set: Set of autonomous systems in the path.

Origin The originator of the destination. This is EGP, IGP, or Incomplete (originated by some other means not known).

LocalPref

The originating router’s degree of preference for the destination.

Metric The path metric with which the route is imported.

Weight
The path weight.

MED A multi-exit discriminator value, used to discriminate among multiple entry/exit points to the same AS.

NextHop
The address of the router to use as the forwarding address for destinations reachable via the given path.

AtomicAggr
Indicates whether the router advertising the path has included the path in an atomic-aggregate.

destinations *net address net mask*
Displays detailed information on the specified route or destination network. The command shows how a specific route was learned, the best path to a specific destination, the metric associated with the route, and other information.

This command is useful in cases where multiple network addresses have the same prefix and different masks. In such cases, specifying the network mask narrows the scope of the information presented.

Example: `destinations 194.10.16.0 255.255.240.0`

```
Dest:194.10.16.0/21, Age:0, Upd#:3, LastSent:0002:00:00

Eligible paths: 1
PathID: 0 - (Best Path)
        ASpath:
        Origin: IGP, Pref: 0, LocalPref: 0
        Metric: 0, Weight: 0, MED: 0
        NextHop: 194.10.16.167, Neighbor: 194.10.16.167
        AtomicAggr: No, Aggregator AS167/194.10.16.167
```

destinations advertised-to *net address*
Lists all routes advertised to the specified BGP neighbor.

Example: `destinations advertised-to`

```
BGP neighbor address [0.0.0.0]? 192.0.251.165

        Destinations advertised to BGP neighbor 192.0.251.165

Network         NextHop         MED  Weight  LPref      AAG AGRAS ORG ASPath
194.10.16.0/20  194.10.16.167   0    0       0          No  167   IGP
192.0.190.0/24  192.0.251.165   0    0       0          No  0     IGP seq [165]
142.4.0.0/16    192.0.251.165   0    0       0          No  0     IGP seq [165-178]
143.116.0.0/16  128.185.250.168 0    0       0          No  0     IGP seq [168]
```

destinations received-from *net address*
Lists all routes received from the specified BGP neighbor.

Example: `destinations received-from`

```
BGP neighbor address [0.0.0.0]? 128.185.250.167

        Destinations obtained from BGP neighbor 128.185.250.167

Network             NextHop         MED Weight  LPref      AAG AGRAS ORG ASPath
194.10.16.0/20      128.185.250.167 0   0       0          No  167   IGP seq[167]
192.0.190.0/24      128.185.250.167 0   0       0          No  0     IGP seq[167-165]
142.4.0.0/16        128.185.250.167 0   0       0          No  0     IGP seq[167-165-178]
```

Dump Routing Tables

For a complete explanation of the **dump routing tables** command, refer to “Dump Routing Table” in the “Monitoring IP” chapter of *Multiprotocol Switched Services (MSS) Interface Configuration and Software User’s Guide*

Neighbors

Use the **neighbors** command to display information on all active BGP neighbors.

Syntax:

neighbors *internet address*

Example: **neighbors**

```
IP-Address       Status   State        DAY-HH:MM:SS  BGPID           AS     Upd#

128.185.252.168  ENABLD  Established  00000:48:52  128.185.142.168  168     16
192.0.190.178    ENABLD  Established  00002:01:49  142.4.140.178    178     16
192.0.251.167    DISBLD  Established  00002:01:45  194.10.16.167    167     16
```

IP-Address
Specifies the IP address of the BGP neighbor.

State Specifies the state of the connection. Possible states are:

Connect
Waiting for the TCP connection to the neighbor to be completed.

Active In the event of TCP connection failure, the state is changed to Active, and the attempt to acquire the neighbor continues.

OpenSent
In this state OPEN has been sent, and BGP waits for an OPEN message from the neighbor.

OpenConfirm
In this state a KEEPALIVE has been sent in response to neighbor's OPEN, and waits for a KEEPALIVE/NOTIFICATION from the neighbor.

Established
A BGP connection has been successfully established, and can now start to exchange UPDATE messages.

BGP-ID
Specifies the neighbor's BGP Identification number.

AS Specifies the neighbor's AS number.

Upd# Specifies the sequence number of the last UPDATE message sent to the neighbor.

internet-address
Use the **neighbor** command to display detailed data on a particular BGP neighbor.

Example: **neighbor 192.0.251.167**

```
Active Conn: Sprt:1026  Dprt:179    State: Established KeepAlive/Hold
Time: 4/12
Passve Conn: None
TCP connection errors: 0          TCP state transitions: 0

BGP Messages:     Sent       Received                    Sent
Received
Open:             1          1          Update:          11         11
Notification:     0          0          KeepAlive:       1828       1830
Total Messages:   1840       1842

Msg Header Errs:  Sent       Received                    Sent
Received
Conn sync err:    0          0          Bad msg length:  0          0
Bad msg type:     0          0

Open Msg Errs:    Sent       Received                    Sent
Received
```

```
Unsupp versions:  0          0          Unsupp auth code: 0          0
Bad peer AS ident:0          0          Auth failure:     0          0
Bad BGP ident:    0          0          Bad hold time:    0          0

Update Msg Errs:  Sent       Received                     Sent
Received
Bad attr list:    0          0          AS routing loop:  0          0
Bad wlkn attr:    0          0          Bad NEXT_HOP atr: 0          0
Mssng wlkn attr:  0          0          Optional atr err: 0          0
Attr flags err:   0          0          Bad netwrk field: 0          0
Attr length err:  0          0          Bad AS_PATH attr: 0          0
Bad ORIGIN attr:  0          0

Total Errors:     Sent       Received                     Sent
Received
Msg Header Errs:  0          0          Hold Timer Exprd: 0          0
Open Msg Errs:    0          0          FSM Errs:         0          0
Update Msg Errs:  0          0          Cease:            0          0
```

Parameter

Use the BGP **parameter** command to display installed BGP globals in the BGP system.

Syntax:

parameter

Example:

```
BGP> parameter

classless-bgp is enabled.
compare-med-from-diff-as is enabled.
IP-route-table-scan-timer value is 5 seconds.
```

Paths

Use the BGP **paths** command to display the paths stored in the path description data base.

Syntax:

paths

Example:

```
paths
PathId   NextHop    MED  AAG   AGRAS  RefCnt   ORG   ASPath
0        10.2.0.3    0   No     0      2       IGP
4        192.2.0.2   0   No     0      2       IGP    seq[2]
5        192.2.0.2   0   No     2      1       IGP    seq[2]
6        192.2.0.2   0   No     0      1       IGP    seq[2-1]
7        10.2.0.168  0   No     0      4       IGP
8        192.3.0.1   0   No     0      2       IGP    seq[1]
9        192.2.0.2   0   No     2      1       IGP    seq[2]
10       10.2.0.3    0   No     0      1       IGP
```

PathId
Path identifier

NextHop
The address of the router to use as the forwarding address for the destinations that can be reached via the given path.

MED The multi-exit discriminator used to discriminate among multiple entry/exit points to the same AS.

AAG Indicates if the path has been atomic-aggregated that is the router that is

advertising the given path has selected less specific route over the more specific one when presented with overlapping routes.

AGRAS
Indicates the AS number of the BGP speaker that aggregated the routes.

RefCnt
Indicates the number of path entities referring to the descriptor.

ORG Specifies the originator of the advertised destinations in the given path: either EGP, IGP, or Incomplete (originated by some other means not known).

AS Path
Enumeration of autonomous systems along the path.

seq: Sequence of autonomous systems in order in the path.

set: Set of autonomous systems in the path.

Ping

For a complete explanation of the **ping** command, see the IP Ping command in the "Monitoring IP" chapter in *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide*.

Policy-List

Use the **policy-list** command to display the current installed policy for specific neighbor and usage statistics of each policy.

Example: policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Receive
```

Display for neighbor based policy configuration:

```
Receive policy list for neighbor '192.0.251.167':
Idx T Prefix            Match OrgAS AnyAS MED   Weight LPref IGPmet Usage
1   I 0.0.0.0/0         Range 0     0     0     0      0     1      1
```

Display for AS based policy configuration:

```
Receive policy :
Idx Type  Prefix            Match OrgAS AdjAS IGPmetric Usage
1   INCL  0.0.0.0/0         Range 0     0     1         1
```

Example: policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Send
```

Display for neighbor based policy configuration:

```
send policy list for neighbor '0.0.0.0': 192.0.251.167
Idx T Prefix            Match OrgAS AnyAS TAG   MED   ASpad Usage
1   I 0.0.0.0/0         Range 0     0     0     0     0     1
```

Display for AS based policy configuration

```
send policy :
Idx Type  Prefix            Match OrgAS AdjAS TAG   Usage
1   INCL  0.0.0.0/0         Range 0     0     0     1
```

Example: policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Origin

Origin policy list for neighbor '0.0.0.0':
Idx T Prefix             Match TAG   Usage
1   I 0.0.0.0/0          Range 0     1
```

Sizes

Use the BGP **sizes** command to display the number of entries stored in the various data bases.

Syntax:

sizes

Example:

```
sizes

# Paths:                                11
# Path descriptors:                      7
  Update sequence#:                     22
# Routing tbl entries (allocated):       6
# Current tbl entries (not imported):    0
# Current tbl entries (imported to IGP): 3
```

Paths Total number of eligible paths for all the routes in the BGP routing table.

Path descriptors
Total number of path descriptors in the database used to hold common path information.

Update sequence#
Indicates the current update sequence number.

Routing tbl entries (allocated)
Indicates the number of entries in BGP routing table.

Current tbl entries (not imported)
Indicates the number of BGP routes not imported into IGP.

Current tbl entries(imported to IGP)
Indicates the number of BGP routes imported into IGP.

Traceroute

For a complete explanation of the **traceroute** command, see Configuring and Monitoring IP in the *Multiprotocol Switched Services (MSS) Configuring Interfaces and Features Volume 1*.

Chapter 5. Configuring and Monitoring DVMRP

This chapter describes configuring and monitoring for DVMRP (Distance Vector Multicast Routing Protocol) protocol activity. It includes the following sections:

- "Accessing the DVMRP Configuration Environment"
- "DVMRP Configuration Commands"
- "DVMRP Monitoring Commands" on page 54

Accessing the DVMRP Configuration Environment

To access the DVMRP configuration environment, enter the following command at the `Config>` prompt:

```
Config> protocol dvmrp
Distance Vector Multicast Routing Protocol config monitoring
DVMRP Config>
```

DVMRP Configuration Commands

This section describes the DVMRP configuration commands. The commands are entered at the `DVMRP Config>` prompt.

Table 6. DVMRP 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 xxi.
Add	Adds to already existing DVMRP information. You can add a physical interface or an IP-IP tunnel interface.
Change	Changes DVMRP information in SRAM. You can change the cost or threshold of a physical interface, IP-IP tunnel, the MOSPF interface, or the endpoints of an IP-IP tunnel.
Delete	Deletes DVMRP information from the static configuration.
Disable	Disables the entire DVMRP protocol or the MOSPF interface.
Enable	Enables the entire DVMRP protocol or the MOSPF interface.
List	Displays the DVMRP configuration.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxii.

Add

Use the **add** command to add to existing DVMRP information. You can add a physical interface or an IP-IP tunnel.

Syntax:

add interface *ip-address cost threshold*

tunnel *tunnel-source tunnel-destination cost threshold*

interface

Adds or updates a DVMRP interface

ip-address
Specifies the IP address of the DVMRP interface.

Valid Values: Any valid IP address

Default Value: None

cost Specifies the cost (in terms of hop-count) incurred for using the interface.

Valid Values: Any integer greater than 0

Default Value: 1

threshold
Specifies the time-to-live needed to reach the nearest neighbor on the interface.

Valid Values: Any integer greater than 0

Default Value: 1

tunnel Adds or updates an IP-IP tunnel across a non-multicast network. Tunnels need to be configured when multicast traffic needs to traverse a network which does not support multicast datagrams or are not running a multicast routing protocol.

source-address
Specifies the IP address of the tunnel source.

Valid Values: Any valid IP address

Default Value: None

destination-address
Specifies the IP address of the tunnel destination.

Valid Values: Any valid IP address

Default Value: None

cost Specifies the cost (in terms of hop-count) incurred for using the tunnel.

Valid Values: Any integer greater than 0

Default Value: 1

threshold
Specifies the time-to-live needed to reach the nearest neighbor on the interface.

Valid Values: Any integer greater than 0

Default Value: 1

Change

Use the **change** command to modify existing DVMRP information. You can modify the cost or threshold values of physical interface, IP-IP tunnels, or the MOSPF interface.

Syntax:

change interface *ip-address cost threshold*

tunnel *tunnel-source tunnel-destination cost threshold*

mospf *cost threshold*

interface
Changes a DVMRP interface

ip-address

Valid Values: Any valid IP address

Default Value: None

cost Specifies the cost (in terms of hop-count) incurred for using the interface.

Valid Values: Any integer greater than 0

Default Value: 1

threshold
Specifies the time-to-live needed to reach the nearest neighbor on the interface.

Valid Values: Any integer greater than 0

Default Value: 1

tunnel Changes an IP-IP tunnel.

source-address

Valid Values: Any valid IP address

Default Value: None

destination-address

Valid Values: Any valid IP address

Default Value: None

cost Specifies the cost (in terms of hop-count) incurred for using the interface.

Valid Values: Any integer greater than 0

Default Value: 1

threshold
Specifies the time-to-live needed to reach the nearest neighbor on the interface.

Valid Values: Any integer greater than 0

Default Value: 1

mospf Changes a MOSPF interface.

cost Specifies the cost (in terms of hop-count) incurred for using the interface.

Valid Values: Any integer greater than 0

Default Value: 1

threshold
Specifies the time-to-live needed to reach the nearest neighbor on the interface.

Valid Values: Any integer greater than 0

Default Value: 1

Delete

Use the **delete** command to remove existing DVMRP information from static memory.

Syntax:

delete interface *ip-address*

tunnel *tunnel-source tunnel-destination*

interface
Deletes a DVMRP interface.

ip-address

Valid Values: Any valid IP address

Default Value: None

tunnel Deletes an IP-IP tunnel.

source-address

Valid Values: Any valid IP address

Default Value: None

destination-address

Valid Values: Any valid IP address

Default Value: None

Disable

Use the **disable** command to disable the entire DVMRP protocol or the MOSPF interface.

Syntax:

disable dvmrp

mospf

dvmrp
Disables the DVMRP protocol. When disabled, the device will not participate as a DVMRP multicast router.

mospf Disables the interface to the MOSPF routing protocol. When disabled, the DVMRP protocol will not forward/receive multicast datagrams to/from the MOSPF routing protocol.

Enable

Use the **enable** command to enable the entire DVMRP protocol or the MOSPF interface.

Syntax:

enable dvmrp

mospf *cost threshold*

dvmrp
Enables the DVMRP protocol. All interfaces configured for IP and do not have MOSPF enabled on them, and the MOSPF interface are enabled.

mospf Enables the interface to the MOSPF routing protocol for DVMRP. This interface allows DVMRP to forward multicast datagrams to the MOSPF routing protocol. This interface is treated as a physical interface.

cost Specifies the cost (in terms of hop-count) incurred for using the interface.

Valid Values: Any integer greater than 0

Default Value: 1

threshold
Specifies the time-to-live needed to reach the nearest neighbor on the interface.

Valid Values: Any integer greater than 0

Default Value: 1

List

Use the **list** command to display the current DVMRP configuration. The output displays the current DVMRP state (disabled or enabled), physical interface configuration information, tunnel configuration information, and MOSPF configuration information.

Syntax:

list

Example:

```
DVMRP config> list

          DVMRP on
          phyint 128.185.138.19 1 1
          phyint 128.185.177.19 2 4
          tunnel 128.185.138.19 128.185.138.21 4 4
```

The following information are displayed for each listed interface:

DVMRP protocol
Displays whether DVMRP is enabled or disabled

DVMRP physical interfaces
For each physical interface, its IP address and values for cost and threshold are displayed.

DVMRP tunnel interfaces
For each tunnel interface, the configured tunnel endpoints, cost and threshold are displayed.

DVMRP MOSPF interface
For the MOSPF interface, cost and threshold are displayed.

DVMRP Monitoring Commands

The DVMRP monitoring commands allow you to view the parameters and statistics of networks that have enabled DVMRP.

Enter the DVMRP monitoring commands at the **DVMRP>** prompt.

Table 7. DVMRP 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 xxi.
Dump routing tables	Displays the DVMRP routes contained in the routing table.
Interface summary	Displays DVMRP interface statistics and parameters.
Join	Configures the router to belong to one or more multicast groups.
Leave	Removes the router from membership in multicast groups.
Mcache	Displays a list of currently active multicast forwarding cache entries.
Mgroups	Displays the group membership of the router’s attached interfaces.
Mstats	Displays various multicast routing statistics.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxii.

Dump Routing Tables

Use the **dump routing tables** command to display the set of known DVMRP multicast sources. Each source is listed together with the DVMRP router it was learned from, an associated cost, and the number of seconds since the routing table entry was refreshed.

Syntax:

dump

Example: dump

```
Multicast Routing Table
Type   Origin-Subnet   From-Gateway    Metric  Age  In  Out-Vifs
Direct 18.26.0.0       192.35.82.97      10     30   1    0  2*
Direct 18.58.0.0       192.35.82.97       4     30   1    0  2*
DVMRP  18.85.0.0       192.35.82.97       4     30   1    0  2*
DVMRP  18.180.0.0      192.35.82.97       3     30   1    0  2*
DVMRP  36.8.0.0        192.35.82.97       9     30   1    0  2*
DVMRP  36.56.0.0       192.35.82.97       7     30   1    0  2*
DVMRP  36.103.0.0      192.35.82.97       9     30   1    0  2*
DVMRP  128.61.0.0      192.35.82.97       8     30   1    0  2*
DVMRP  128.89.0.0      192.35.82.97      10     30   1    0  2*
DVMRP  128.109.0.0     192.35.82.97       4     30   1    0  2*
DVMRP  128.119.0.0     192.35.82.97       4     30   1    0  2*
DVMRP  128.150.0.0     192.35.82.97       6     30   1    0  2*
```

Type Displays the type of multicast sources (i.e., DVMRP)

Origin-Subnet
Displays the IP address of the originating subnet.

From-Gateway
Displays the IP address of the gateway from which the entry came.

Metric Displays the associated cost of that route.

Age Displays the age of routing table entry as the number of seconds since the routing table entry was refreshed.

In Displays the DVMRP VIF that multicast datagram from the source must be received on.

Out-Vifs
Displays those VIFs that will send the multicast datagrams. VIFs marked with an asterisk indicate that a datagram will only be forwarded if there are group members on the attached network.

Interface Summary

Use the **interface summary** command to display current list of DVMRP interfaces (or VIFs).

Syntax:

interface *interface-ip-address*

Example: `interface`

```
Virtual Interface Table
Vif  Local-Address                          Metric  Thresh  Flags
0   10.1.153.22      subnet: 10.1.153.0        1       1    querier
1   10.1.154.22      subnet: 10.1.154.0        1       1    down
```

Vif Displays the number assigned to DVMRP interfaces (or VIFs). Each VIF is assigned a number, which is used to identify the VIF in other commands.

Local Address
Displays the local IP address of the DVMRP interface.

Metric The associated cost of the route.

Threshold
Reflects the ability of a network to control external flow of multicast packets outside of the network.

Flags Displays whether the VIF is down or that the router is the sender of IGMP Host Membership Queries on the interface.

Join

Use the **join** command to establish the router as a member of a multicast group.

This command is similar to the join command in the OSPF configuration monitoring with two differences:

- The effect on group membership is immediate when the commands are given from the monitor (i.e., a restart/reload is not required).
- The command keeps track of the number of times a particular group is “joined.”

When the router is the member of a multicast group, it responds to pings and SNMP queries sent to the group address.

Syntax:

join *multicast-group-address*

Example: `join 224.185.00.00`

Leave

Use the **leave** command to remove a router's membership in a multicast group. This will keep the router from responding to pings and SNMP queries sent to the group address.

This command is similar to the **leave** command in the OSPF configuration monitoring with two differences:

- The effect on group membership is immediate when the commands are given from the monitor (i.e., a restart/reload is not required).
- The command will not delete group membership until the "leaves" executed equals the number of "joins" previously executed.

Syntax:

leave *multicast-group-address*

Example: `leave 224.185.00.00`

Mcache

Use the **mcache** command to display a list of currently active multicast cache entries. Multicast cache entries are built on demand, whenever the first matching multicast datagram is received. There is a separate cache entry (and therefore a separate route) for each datagram source network and destination group combination.

Cache entries are cleared on topology changes (e.g., a point-to-point line in the DVMRP system going up or down), and on group membership changes.

Note: The numbers displayed in the legend at the top of the output do NOT refer directly to VIFs, but instead refer to physical interfaces (which may be running either DVMRP or MOSPF) and tunnels.

Note:

Syntax:

mcache

Example:

```
mcache
0: Eth/0          1: TKR/0          2: Internal
3: 128.185.246.17  4: 192.35.82.97

Source          Destination     Count   Upst    Downstream
128.185.146.0   239.0.0.1       1       0       2,4
128.119.0.0     224.2.199.198   9       4       3
128.9.160.0     224.2.127.255   1       4       3
13.2.116.0      224.2.0.1       27      4       3
140.173.8.0     224.2.0.1       31      4       3
128.165.114.0   224.2.0.1       25      4       3
132.160.3.0     224.2.158.99    11      4       3
132.160.3.0     224.2.170.143   56      4       3
128.167.254.0   224.2.199.198   27      4       3
129.240.200.0   224.2.0.1       21      4       3
131.188.34.0    224.2.0.1       28      4       3
131.188.34.0    224.2.199.198   28      4       3
```

Source

Source network/subnet of matching datagrams.

Destination
Destination group of matching datagrams.

Count Displays the number of entries processed for that multicast group.

Upstream
Displays the neighboring network/router from which the datagram must be received in order to be forwarded. When this reads as "none", the datagram will never be forwarded.

Downstream
Displays the total number of downstream interfaces/neighbors to which the datagram will be forwarded. When this is *none*, the datagram will not be forwarded.

There is more information in a multicast forwarding cache entry. A cache entry can be displayed in detail by providing the source and destination of a matching datagram on the command line. If a matching cache entry is not found, one is built. A sample of this command is shown below:

Example:

```
mcache 128.185.182.9  224.0.1.2
source Net:     128.185.182.0
Destination:    224.0.1.2
Use Count:      472
Upstream Type:  Transit Net
Upstream ID:    128.185.184.114
Downstream:     128.185.177.11 (TTL = 2)
```

In addition to the information shown in the short form of the mcache command, the following fields are displayed:

Upstream Type
Indicates the type of node from which the datagram must be received to be forwarded. Possible values for this field are "none" (indicating that the datagram will not be forwarded), "router" (indicating that the datagram must be received over a point-to-point connection), "transit network", "stub network", and "external" (indicating that the datagram is expected to be received from another Autonomous System).

Downstream
Prints a separate line for each interface or neighbor to which the datagram will be sent. A TTL value is also given, indicating that datagrams forwarded out of or to this interface must have at least the specified TTL value in their IP header. When the router is itself a member of the multicast group, a line specifying *internal application* appears as one of the downstream interfaces/neighbors.

Mgroups

Use the **mgroups** command to display the group membership of the router's attached interfaces. Only the group membership for those interfaces on which the router is either designated router or backup designated router are displayed.

Syntax:

mgroups

Example:

DVMRP Monitoring Commands (Talk 5)

```
mgroups
Local Group Database
Group             Interface                Lifetime (secs)

224.0.1.1         128.185.184.11 (Eth/1)       176
224.0.1.2         128.185.184.11 (Eth/1)       170
224.1.1.1         Internal                     1
```

Group Displays the group address as it has been reported (via IGMP) on a particular interface.

Interface
Displays the interface address to which the group address has been reported (via IGMP).

The router's internal group membership is indicated by an value of "internal". For these entries, the lifetime field (see below) indicates the number of applications that have requested membership in the particular group.

Lifetime
Displays the number of seconds that the entry will persist if Membership Reports cease to be heard on the interface for the given group.

Mstat

Use the **mstat** command to display various multicast routing statistics. The command indicates whether multicast routing is enabled and whether the router is an inter-area and/or inter-AS multicast forwarder.

Syntax:

mstats

Example:

```
mstats
              MOSPF forwarding:       Enabled
              Inter-area forwarding:  Enabled
              DVMRP forwarding:       Enabled

Datagrams received:           45476  Datagrams (ext source):    0
Datagrams fwd (multicast):        0  Datagrams fwd (unicast):   0
Locally delivered:                0  No matching rcv interface: 0
Unreachable source:               4  Unallocated cache entries: 0
Off multicast tree:               0  Unexpected DL multicast:   0
Buffer alloc failure:             0  TTL scoping:               0

# DVMRP routing entries:          0  # DVMRP entries freed:     0
# fwd cache alloc:                5  # fwd cache freed:         0
# fwd cache GC:                   0  # local group DB alloc:    6
# local group DB free:            0
```

MOSPF forwarding
Displays whether the router will forward IP multicast datagrams.

Inter-area forwarding
Displays whether the router will forward IP multicast datagrams between areas.

DVMRP forwarding
Displays whether the router will forward IP multicast datagrams.

Datagrams received
Displays the number of multicast datagrams received by the router (datagrams whose destination group lies in the range 224.0.0.1 - 224.0.0.255 are not included in this total).

Datagrams (ext source)
Displays the number of datagrams that have been received whose source is outside the AS.

Datagrams fwd (multicast)
Displays the number of datagrams that have been forwarded as datalink multicasts (this includes packet replications, when necessary, so this count could very well be greater than the number received).

Datagrams fwd (unicast)
Displays the number of datagrams that have been forwarded as datalink unicasts.

Locally delivered
Displays the number of datagrams that have been forwarded to internal applications.

No matching rcv interface
Displays the count of those datagrams that were received by a non-inter-AS multicast forwarder on a non-MOSPF interface.

Unreachable source
Displays a count of those datagrams whose source address was unreachable.

Unallocated cache entries
Displays a count of those datagrams whose cache entries could not be created due to resource shortages.

Off multicast tree
Displays a count of those datagrams that were not forwarded either because there was no upstream neighbor or no downstream interfaces/neighbors in the matching cache entry.

Unexpected DL multicast
Displays a count of those datagrams that were received as datalink multicasts on those interfaces that have been configured for datalink unicast.

Buffer alloc failure
Displays a count of those datagrams that could not be replicated because of buffer shortages.

TTL scoping
Indicates those datagrams that were not forwarded because their TTL indicated that they could never reach a group member.

DVMRP routing entries:
Displays the number of DVMRP routing entries.

DVMRP entries freed:
Indicates the number of DVMRP entries that have been freed. The size will be the number of routing entries minus the number of entries freed.

 # fwd cache alloc
Indicates the number of cache entries allocated. The current forwarding cache size is the number of entries allocated (“# fwd cache alloc”) minus the number of cache entries freed (“# fwd cache freed”).

 # fwd cache freed
Indicates the number of cache entries freed. The current forwarding cache size is the number of entries allocated (“# fwd cache alloc”) minus the number of cache entries freed (“# fwd cache freed”).

DVMRP Monitoring Commands (Talk 5)

 # fwd cache GC

Indicates the number of cache entries were cleared because they were not recently used and the cache overflowed.

 # local group DB alloc

Indicates the number of local group database entries allocated. The number allocated (“# local group DB alloc”) minus the number freed (“# local group DB free”) equals the current size of the local group database.

 # local group DB free

Indicates the number of local group database entries freed. The number allocated (“# local group DB alloc”) minus the number freed (“# local group DB free”) equals the current size of the local group database.

The number of cache hits can be calculated as the number of datagrams received (“Datagrams received”) minus the total of datagrams discarded due to “No matching rcv interface,” “Unreachable source” and “Unallocated cache entries”, and minus “# local group DB alloc.” The number of cache misses is simply “# local group DB alloc”+.

Chapter 6. Using AppleTalk Phase 2

This chapter describes the AppleTalk Phase 2 (AP2) configuration commands and includes the following sections:

Basic Configuration Procedures

This section outlines the initial steps required to get the AppleTalk Phase 2 protocol up and running. Information on how to make further configuration changes will be covered in the command sections of this chapter. For the new configuration changes to take effect, the router must be restarted.

Enabling Router Parameters

When you configure a router to forward AppleTalk Phase 2 packets, you must enable certain parameters regardless of the number or type of interfaces in the router. If you have multiple routers transferring AppleTalk Phase 2 packets, specify these parameters for each router.

- Globally Enable AppleTalk Phase 2 - To begin, you must globally enable the AppleTalk Phase 2 software using the AppleTalk Phase 2 configuration **enable ap2** command. If the router displays an error in this step, there is no AppleTalk Phase 2 software present in your load. If this is the case, contact your customer service representative.
- Enable Specific Interfaces - You must then enable the specific interfaces over which AppleTalk Phase 2 is to send the packets. Use the **enable interface** *interface number* command to do this.

  Note: When enabling AppleTalk over ATM, you must enable the specific emulated LAN interfaces over which AppleTalk is to send packets. You must not enable AppleTalk over the physical ATM interface. All further uses of the word "interface" in this chapter refer to the emulated LAN interface, not the ATM physical interface.
- Enable Checksumming - You can then determine whether the router will compute DDP checksums of packets it originates. Checksum software does not work correctly in some AppleTalk Phase 2 implementations, so you may not want to originate packets with checksums for compatibility with these implementations. Normally, however, you will want to enable the generation of checksums. Any packet forwarded with a checksum will have its checksum verified.

Setting Network Parameters

You must also specify certain parameters for each network and interface that sends and receives AppleTalk Phase 2 packets. After you have specified the parameters, use the AppleTalk Phase 2 list configuration command to view the results of the configuration.

- Set the Network Range for Seed Routers - Coordinating network ranges and zone lists for all routers on a network is simplified by having specific routers

designated as seed routers. Seed routers are configured with the network range and zone list while all other routers are given null values. Null values indicate that the router should query the network for values from the seed routers. For every network (segment) of your interconnected AppleTalk internet, at least one router interface must be configured as the seed router for that network. There are usually several seed routers on a network in case one of them fails. Also, a router can be a seed router for some or all of its network interfaces. Use the **set net-range** command to assign the network range in seed routers.

- Set the Starting Node Number - Use the **set node** command to assign the starting node number for the router. The router will AARP for this node, but if it is already in use, a new node will be chosen.
- Add a Zone Name - You can add one or more zone names for each network in the internetwork. You can add a zone name for a given network in any router connected to that network; however, only the seed router needs to contain the zone name information for a connected network. Attached routers dynamically acquire the zone name from adjacent routers using the ZIP protocol. Apple recommends that, for a given network, you choose the same seed router for the network number and the zone name. The zone name cannot be configured for a network unless the network number is also configured. To add a zone name for each network number, use the AppleTalk Phase 2 configuration **add zone** *name* command.

AppleTalk 2 Zone Filters

ZoneName filtering, although not required for AppleTalk, is a very desirable feature for the security and administration of large AppleTalk Internetworks. There are also provisions for restricting access to networks by net numbers.

General Information

AppleTalk is structured so that every network is identified in two ways. The first is a network number or range of consecutive network numbers that must be unique throughout the internet. The network number combined with the node number uniquely identifies any end station in the internet.

The second identifier for the network is one or more ZoneNames. These ZoneName strings are not unique throughout the internet. The end station is uniquely identified by a combined **object:type:ZoneName-string**.

A router first learns about a network when the new net range appears in the RTMP routing update from a neighboring router. The router then queries the neighbor for the ZoneNames of the new network. Note that the net range is repeated in every new RTMP update but that the ZoneNames are requested only once.

The end stations obtain the network numbers from the broadcasted RTMP (routing information) packets and then choose a node number. This net/node pair is then AARP'd for (AARP Probe) to see if any other end station has already claimed its use. If another station responds, another net/node pair is chosen by the end station and the process repeated until no responses are received.

Why ZoneName Filters?

When the typical AppleTalk end station wants to use a service (printer, file server) on the Apple Internet, it first looks at all available Zones and selects one. It then

chooses a service type and requests a list of all names advertising the type in the chosen Zone. Several problems arise from this mechanism.

- A large internet may have many Zones. Presenting the user with a long list to choose from obscures the needed ones (thereby inhibiting usability of the list).
- The server may not want to make itself available throughout the internet (for security reasons). If the Zone that the service is in is not visible to the client, security is enhanced.
- Restricting the Zones that are visible from a department to the rest of the internet will allow the internet administration to let the department control (or not) its own domain while not increasing the overhead for the rest of the internet (reducing administration).

The filtering of network numbers further enhances the security and administration of the internet. Network access is only indirectly controlled by Zone filtering. An unregulated department could add networks with the same Zone names but new net numbers that conflict with other departments. Network number filtering can be used to prevent these random additions of zone names and net numbers from impacting the rest of the network.

How Do You Add Filters?

The router is configured with an exclusive (meaning block the specified zones) or inclusive (meaning allow only these zones) list of Zones for each direction on each interface. The specified interface will not readvertise filtered Zone information in the defined direction. If all Zones in a network's Zonelist are filtered, network information will also be filtered across the interface.

- Use configuration commands **add** and **delete**, to create the filter list for an interface.
- Use configuration commands **enable** and **disable** to specify how the filter list is applied.

  Use similar commands to create network number filters.

Other Commands:

You can use the `AP2 CONFIG>` **list** command to display all filter information for the interfaces. In addition, the **list** command accepts an *interface#* as an argument so that you can list information for only an interface.

Sample Configuration Procedures

This section covers the steps required to get AP2 up and running. For information on how to make further configuration changes, see "AppleTalk Phase 2 Configuration Commands" on page 69. For the configuration changes to take effect, you must restart the router.

To access the AP2 configuration environment, enter **protocol ap2** at the `Config>` prompt.

Enabling AP2

When you configure a router to forward AP2 packets, you must enable certain parameters. If you have multiple routers transferring AP2 packets, specify these parameters for each router. To enable AP2:

1. Use the **enable ap2** command to globally enable AP2 on the router. For example:

```
AP2 config>enable ap2
```

2. Enable the specific interfaces over which AP2 is to send packets. For example:

```
AP2 config>enable interface 1
```

Setting Network Parameters

To set up your router as a seed router, you must set the network range, a starting node number, and at least one zone name. You can configure some interfaces on a router as seed routers and leave other interfaces as non-seed routers. You must have at least one seed router for each AppleTalk network, and you should configure several seed routers on a network in case one of them fails.

1. Use the **set net-range** command to set the Network Range. For example:

```
AP2 config>set net-range
Interface #  [0]? 1
First Network range number (1-65279, or 0 to delete) []? 1
Last Network range number (1-165279) []? 5
```

   Enter the same first and last values for a single-numbered network.

2. Use the **set node-number** command to set the Starting Node Number for the interface. The router will AARP for this node. If the number is already in use, the router will choose a new number. For example:

```
AP2 config>set node-number
Interface #  [0]? 1
Node number (1-253, or 0 to delete) []? 1
```

3. Use the **add zone** command to add one or more zone names for the network attached to the interface. If you define a network range for an interface, you should also define the zone names for the interface. If you did not define a network number, do not define zone names. For example:

```
AP2 config>add zone
Interface # [0]? 1
Zone name []? Finance
```

After you have specified the parameters, you can use the **list** command at the `AP2 config>` prompt to view your configuration.

Setting Up Zone Filters

Zone filtering lets you filter zones in each direction on each interface. To filter incoming packets, set up an input filter. To filter outgoing packets, set up an output filter. The interface will not readvertise filtered zone information in the direction that you define. Follow these steps to set up a zone filter:

1. Add zone filters to an interface. Use the **add zfilter in** command to add an input zone filter to an interface. Use the **add zfilter out** command to add an output zone filter to an interface. For example:

```
AP2 config>add zfilter in
Interface # [0]? 1
Zone name []? Admin
```

2. Enable the zone filters that you added. This turns on the filter and controls whether the filter is inclusive or exclusive. Inclusive filters forward only the zone information in that filter. Exclusive filters block only the zone information in that filter. For example:

```
AP2 config>enable zfilter in exc
Interface # [0]? 1
```

The following are some examples that explain how to set up zone filters in the internet shown in Figure 3.

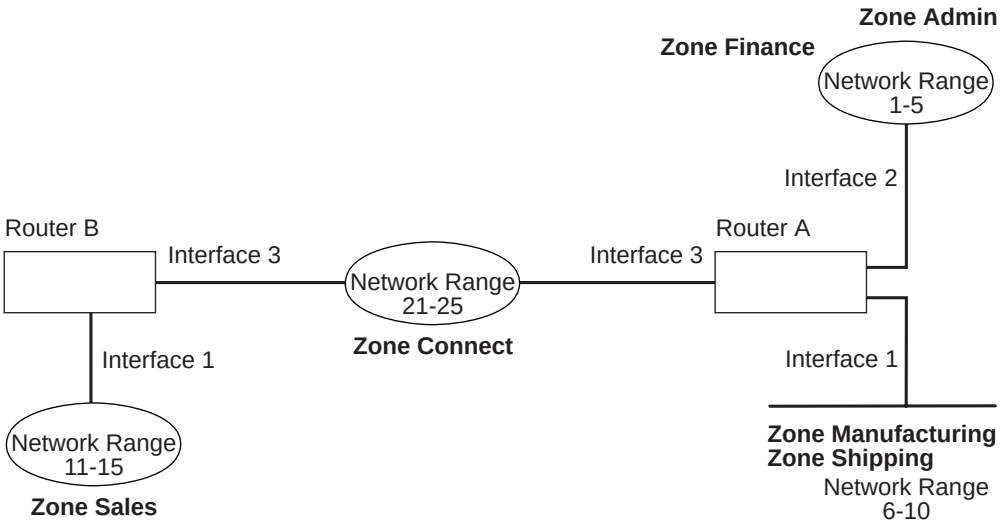

Figure 3. Example of Zone Filtering

Example 1

The following is an example of how to filter the Manufacturing zone from all other networks. To do this, you would set up an input filter on Interface 1 of Router A to exclude the Manufacturing zone.

1. On Router A, add an input zone filter to Interface 1.

```
AP2 config>add zfilter in
Interface # [0]? 1
Zone name []? Manufacturing
```

2. Enable the input zone filter and make the filter exclusive.

```
AP2 config>enable zfilter in exc
Interface # [0]? 1
```

   This excludes Manufacturing zone information from entering Router A, thereby filtering the zone from the rest of the internet.

Example 2

The following example shows how to filter the Manufacturing zone from Network 11-15, but still allow the Manufacturing zone to be visible on Network 1-5. To do this, you would set up an output filter on Interface 3 of Router A to exclude Manufacturing zone information from being forwarded out of Interface 3. The interface will continue to advertise Manufacturing zone information over interfaces 1 and 2 on Router A, making it visible on Network 1-5.

1. Add an output zone filter to Interface 3.

```
AP2 config>add zfilter out
Interface # [0]? 3
Zone name []? Manufacturing
```

2. Enable the output zone filter and make the filter exclusive.

```
AP2 config>enable zfilter out exc
Interface # [0]? 3
```

   This filter excludes Manufacturing zone information from the output of Interface 3.

Example 3

The next example shows how to set up a filter so that the Admin zone is visible on all networks, but the Finance zone is not visible to the rest of the internet.

1. Add an input zone filter to Interface 2 on Router A.

```
AP2 config>add zfilter in
Interface # [0]? 2
Zone name []? Admin
```

2. Enable the input zone filter and make it inclusive.

```
AP2 config>enable zfilter in inc
Interface # [0]? 2
```

   By setting up this input filter as inclusive, only Admin zone information is forwarded through Interface 2 to the rest of the internet.

Setting Up Network Filters

Network filters are similar to zone filters, except they let you filter an entire network. To set up a network filter:

1. Add a network filter. Use the **add nfilter in** command to add an input network filter to an interface. Use the **add nfilter out** command to add an output network filter to an interface. For example:

```
AP2 config>add nfilter out
Interface # [0]? 2
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 15
```

   The network range you enter here must match the range that you assigned to that network.

2. Enable the network filter that you added and make it either inclusive or exclusive. Inclusive filters forward only network information in that filter. Exclusive filters block only network information in a filter, and they allow all other network information to be forwarded.

```
AP2 config>enable nfilter in exc
Interface # [0]? 2
```

Following are some examples that explain how to set up network filters in the internet, as shown in Figure 4 on page 67.

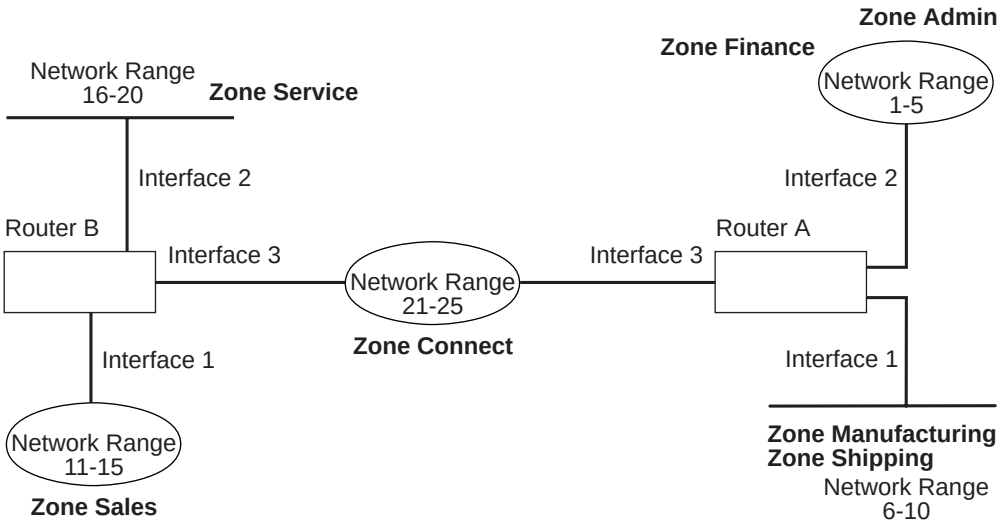

Figure 4. Example of Network Filtering.

Note: Interfaces refer to emulated LAN interfaces , not ATM physical interfaces.

The following steps show how to filter Network 6-10 so that it is not visible to Network 16-20 as shown in Figure 4.

1. Add an output network filter for Network 6-10 to Interface 2 on Router B.

```
AP2 config>add nfilter out
Interface # [0]? 2
First Network range number (decimal) [0]? 6
Last Network range number (decimal) [0]? 10
```

2. Enable the output network filter as exclusive.

```
AP2 config>enable nfilter out exc
Interface # [0]? 2
```

   This filter excludes all information on Network 6-10 from being forwarded through Interface 2 to Network 16-20.

Using AppleTalk Phase 2

Chapter 7. Configuring and Monitoring AppleTalk Phase 2

This chapter describes the AppleTalk Phase 2 (AP2) configuring and monitoring commands. It includes the following sections:

Accessing the AppleTalk Phase 2 Configuration Environment

To access the AppleTalk Phase 2 configuration environment, enter the following command at the `Config>` prompt:

```
Config> ap2
AP2 Protocol user configuration
AP2 Config>
```

AppleTalk Phase 2 Configuration Commands

This section describes the AppleTalk Phase 2 configuration commands.

The AppleTalk Phase 2 configuration commands allow you to specify network parameters for router interfaces that transmit AppleTalk Phase 2 packets. The information you specify with the configuration commands becomes activated when you restart the router.

Enter the AppleTalk Phase 2 configuration commands at the `AP2 config>` prompt. Table 8 shows the commands.

Table 8. AppleTalk Phase 2 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 xxi.
Add	Adds zone names, network filters, and zone filters to an interface.
Delete	Deletes the zone names, interfaces, network filters, and zone filters.
Disable	Disables interfaces, checksumming, split-horizon routing, network filters, or zone filters, or globally disables AppleTalk Phase 2.
Enable	Enables interfaces, checksumming, split-horizon routing, network filters, zone filters, or globally enables AppleTalk Phase 2.
List	Displays the current AppleTalk Phase 2 configuration.
Set	Sets the cache size, network range, and node number.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxii.

Add

Use the **add** command to add the zone name to the interface zone list or to add the zone name to the interface zone list as the default for the interface or to add network and zone filters.

Syntax:

add zone . . .
defaultzone . . .
nfilter in . . .
nfilter out . . .
zfilter in . . .
zfilter out . . .

zone *interface# zonename*

Adds the zone name to the interface zone list. If you define a network number for an interface, you should also define the zone names for the interface. If you did not define a network number, do not define zone names.

Example:

```
ap2config>add zone
Interface # [0]? 0
Zone name []? Finance
```

defaultzone *interface# zonename*

Adds a default zone name for the interface. If a node on the network requests a zone name that is invalid, the router assigns the default zone name to the node until another zone name is chosen. If you add more than one default to an interface, the last one added overrides the previous default. If you do not add a default, the first zone name added using the **zone** command is the default.

Example:

```
ap2config>add defaultzone
Interface # [0]? 0
Zone name []? Headquarters
```

nfilter in *interface# first network# last network#*

Adds a network filter to the input of the interface. The network range that you enter must match the network range you set for that interface. You cannot filter only a portion of a network range. For example, if you set a network range of 1–10, and you set up a filter for 5–8, the router filters the full network range of 1–10.

Example:

```
ap2config>add nfilter in
Interface # [0]? 0
First Network range number (decimal) [0]? 1
Last Network range number (decimal) [0]? 10
```

nfilter out *interface# first network# last network#*

Adds a network filter to the output of the interface. The network range that you enter must match the network range you set for that interface. You cannot filter only a portion of a network range. For example, if you set a network range of 1–0, and you set up a filter for 5–8, the router filters the full network range of 1–10.

Example:

```
ap2config>add nfilter out
Interface # [0]? 0
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 20
```

zfilter in *interface# zone name*

Adds a zone name filter to the input or output of the interface.

Example:

```
ap2config>add zfilter in
Interface # [0]? 1
Zone name []? Marketing
```

zfilter out *interface# zone name*

Adds a zone name filter to the output of the interface.

Example:

```
ap2config>add zfilter out
Interface # [0]? 0
Zone name []? Corporate
```

Delete

Use the **delete** command to delete a zone name from the interface zone list, network or zone name filters, or all AppleTalk Phase 2 information from an interface.

Syntax:

delete

- zone . . .
- nfilter in . . .
- nfilter out . . .
- zfilter in . . .
- zfilter out . . .
- interface

zone *interface# zonename*

Deletes a zone name from the interface zone list.

Example:

```
ap2config>delete zone 2 newyork
```

nfilter in *interface# first network# last network#*

Deletes a network filter from the input of the interface. You must enter the same network range numbers you set using the **add nfilter in** command.

Example:

```
ap2config>delete nfilter in
Interface # [0]? 0
First Network range number (decimal) [0]? 1
Last Network range number (decimal) [0]? 12
```

nfilter out *interface#*

Deletes a network filter from the output of the interface. You must enter the same network range numbers you set using the **add nfilter out** command.

Example:

```
ap2config>delete nfilter out
Interface # [0]? 0
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 20
```

zfilter in *interface# zone name*

Deletes a zone name filter from the input of the interface.

Example:

```
ap2config>delete nfilter in
Interface # [0]? 1
Zone name []? Marketing
```

zfilter out *interface# zone name*

Deletes a zone name filter from the output of the interface.

Example:

```
delete zfilter out
Interface # [0]? 1
Zone name []? Marketing
```

interface

Use this command to delete an interface. This is the only way to delete zone names that have non-printing characters.

Example:

```
ap2config>delete interface 1
```

Disable

Use the **disable** command to disable AP2 on all interfaces or on a specified interface, checksumming, filtering, APL/AP2 translation, or split horizon routing.

Syntax:

disable ap2
checksum
interface . . .
nfilter in . . .
nfilter out . . .
zfilter in . . .
zfilter out . . .
split-horizon-routing . . .

ap2 Disables the AppleTalk Phase 2 packet forwarder for all interfaces.

Example:

```
ap2config>disable ap2
```

checksum

Specifies that the router will not compute the checksum in packets it generates. The router usually checksums all packets it forwards. This is the default.

Example:

```
ap2config>disable checksum
```

interface *interface#*

Disables all AP2 functions on the specified network interface. The network continues to remain available for all other protocols.

Example:

```
ap2config>disable interface 2
```

nfilter in *interface#*

Disables, but does not delete, the input network filters on this interface.

Example:

```
ap2config>disable nfilter in
Interface # [0]? 2
```

nfilter out *interface#*

Disables, but does not delete, the output network filters on this interface.

Example:

```
ap2config>disable nfilter out
Interface # [0]? 2
```

zfilter in *interface#*

Disables, but does not delete, the input zone filters on this interface.

Example:

```
ap2config>disable zfilter in
Interface # [0]? 1
```

zfilter out *interface#*

Disables, but does not delete, the output zone filters on this interface.

Example:

```
ap2config>disable zfilter out 0
Interface # [0]? 1
```

split-horizon-routing *interface#*

Disables split-horizon-routing on this interface. You need to disable split-horizon routing only on Frame Relay interfaces that are on a hub in a partially-meshed Frame Relay network. Disabling split-horizon routing causes all of the routing tables to be propagated on this interface.

Example:

```
ap2config>disable split-horizon-routing 0
```

Enable

Use the **enable** command to enable the checksum function, to enable a specified interface, to enable AppleTalk 2 gateway function, or to globally enable the AppleTalk Phase 2 protocol.

Syntax:

enable

- ap2
- checksum
- interface . . .
- nfilter in . . .
- nfilter out . . .
- split-horizon-routing . . .
- zfilter . . .

ap2 Enables the AppleTalk Phase 2 packet forwarder over all of the interfaces.

Example:

```
ap2config>enable ap2
```

checksum

Specifies that the router will compute the checksum in packets it generates. The router checksums all AP2 packets it forwards.

Example:

```
ap2config>enable checksum
```

interface *interface#*
Enables the router to send AppleTalk Phase 2 packets over specific interfaces.

Example:

```
ap2config>enable interface 3
```

nfilter in *exclusive* **or** *exclusive interface#*
Enables network input filters and controls how the filter is applied to the interface. Inclusive forwards matches. Exclusive drops matches.

Example:

```
ap2config>enable filter in inc
Interface # [0]? 1
```

nfilter out *exclusive* **or** *exclusive interface#*
Enables network output filters and controls how the filter is applied to the interface. Inclusive forwards matches. Exclusive drops matches.

Example:

```
ap2config>enable filter out exec
Interface # [0]? 1
```

split-horizon-routing *interface #*
Enables split-horizon routing on the interface. The default is *enabled*.

Example:

```
ap2config>enable split-horizon-routing 1
```

zfilter Enables zone filters assigned to an interface. Must specify if filter is “in” or “out” and if the filter is inclusive or exclusive. Inclusive means that only packets matching the filter will be routed. Exclusive means that all packets matching the filter will be discarded.

Example:

```
ap2config>enable zfilter in inc
Interface # [0]?
```

Example:

```
ap2config>enable zfilter out exec
Interface # [0]? 0
```

List

Use the **list** command to display the current AP2 configuration. In the example, the router is a seed router on

Note: The **list** command accepts an *interface#* as an argument.

Syntax:

list

Example:

```
ap2config>list
APL2 globally  enabled
Checksumming  disabled
Cache size 500

List of configured interfaces:

Interface       netrange         /  node        Zone
```

APL2 globally
Indicates whether AppleTalk Phase 2 is globally enabled or disabled.

Checksumming
Indicates whether checksum is enabled or disabled.

Cache size
Number of fastpath cache entries.

List of configured interfaces
Lists each interface number and its network range, node number, and zone name(s) as well as the default zone.

For each interface also lists whether or not input and output zone filters and network filters and enabled or disabled. If they are enabled, indicates whether or not they are inclusive or exclusive.

Input/output Zfilters
Indicates zone filters assigned to an interface. Inclusive means that only packets matching the filter will be routed. Exclusive means that all packets matching the filter will be discarded. The name of the zone filtered is displayed. Input means that the filter is applied to traffic coming into the interface. Output means that filter is applied to traffic going out to the interface.

Input/output Nfilters
Indicates net filters assigned to an interface. Inclusive means that only packets matching the filter will be routed. Exclusive means that all packets matching the filter will be discarded. The range of networks filtered is displayed. Input means that the filter is applied to traffic coming into the interface. Output means that filter is applied to traffic going out to the interface.

Split-horizon-routing
Shows whether or not split-horizon routing is enabled or disabled on each interface.

Set

Use the **set** command to define the cache-size of fastpath or specific AppleTalk Phase 2 parameters, including the network range in seed routers and the node number.

Syntax:

set	cache-size . . .
	net-range . . .
	node . . .

cache-size *value*
Cache-size corresponds to the total number of AppleTalk networks and nodes that can simultaneously communicate through this router using the fastpath feature. (Fastpath is a method of precalculating MAC headers to forward packets more quickly.) The default is 500, which allows up to 500 networks and nodes to simultaneously communicate through the router and still use fastpath. If the number of networks and nodes becomes greater

than the cache size, the router still forwards the packets, but it does not use fastpath. Valid values for cache size are: 0 (disable), 100 to 10 000. Although not recommended, setting the cache-size to zero disables the fastpath feature and no memory is used for the cache. You need to change this default only for very large networks. Each cache-size entry uses 36 bytes of memory.

Example:

```
ap2config>set cache-size 700
```

net-range *interface# first# last#*

Assigns the network range in seed routers using the following:

- interface# - Designates the router interface to operate on.
- first# - Assigns the lowest number of the network range. Legal values are 1 to 65279 (10xFEFF hexadecimal).
- last# - Sets the highest number of the network range. Legal values are *first#* to 65279.

A single numbered network has the same first and last values. A first value of zero deletes the netrange for the interface and turn the “seeded” interface into an “unseeded” interface. First# and last# are inclusive in the network range.

Example:

```
ap2config>set Net-Range 2 43 45
```

node *interface# node#*

Assigns the starting node number for the router. The router will AARP for this node but if it is already in use, a new node will be chosen. The following explains each argument that is entered after this command:

- interface# - Designates the router interface to operate on.
- node# - Designates the first attempted node number. Legal values are 1 to 253. A node# value of zero deletes the node number for the interface and forces the router to choose one at random.

Example:

```
ap2config>set node 2 2
```

Accessing the AppleTalk Phase 2 Monitoring Environment

To access the AppleTalk Phase 2 monitoring environment, enter the following command at the + (GWCON) prompt:

```
+ protocol ap2
AP2>
```

AppleTalk Phase 2 Monitoring Commands

This section describes the AppleTalk Phase 2 monitoring commands which allow you to view the parameters and statistics of the interfaces and networks that transmit AppleTalk Phase 2 packets. Monitoring commands display configuration values for the physical, frame, and packet levels. You also have the option of viewing the values for all three protocol levels at once.

Enter the AppleTalk Phase 2 monitoring commands at the AP2> prompt. Table 9 on page 77 shows the commands.

Table 9. AppleTalk Phase 2 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 xxi.
Atecho	Sends echo requests and watches for responses.
Cache	Displays the cache table entries.
Clear Counters	Clears all cache usage counters and packet overflow counters.
Counters	Displays the overflow count of AP2 packets for each interface.
Dump	Displays the current state of the routing table for all networks in the internet and their associated zone names.
Interface	Displays the current addresses of the interfaces.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxii.

Atecho

The **atecho** command sends AppleTalk Echo Requests to a specified destination and watches for a response. This command can be used to verify basic AppleTalk connectivity and to isolate trouble in the AppleTalk internetwork.

Syntax:

atecho *dest_net dest_node*

dest_net
Specifies the destination AppleTalk network number, in decimal. This is a required parameter.

dest_node
Specifies the destination AppleTalk node number, in decimal. This is a required parameter.

Note: For many AppleTalk nodes, the network address (network number and node number) is dynamically assigned and might not be readily available. However, there are still a number of ways to use the **atecho** command effectively:

1. The AppleTalk address for router nodes is statically configured in many cases. Connectivity between router nodes is critical to overall network connectivity.
2. By setting the atecho destination node number to 255, you can query all nodes on the specified network number on a directly attached AppleTalk network. The received responses will indicate the node’s node number. These node numbers can then be used to echo these nodes from distant routers to verify connectivity.

src_net
Source AppleTalk network number. This is an optional parameter. If not specified, the router uses its interface network number on the outgoing interface leading to the destination network.

src_node
Source AppleTalk node number. This is an optional parameter. If not specified, the router uses its interface node number on the outgoing interface leading to the destination network.

size Number of bytes to use in the AppleTalk echo requests. This is an optional parameter. Default is 56 bytes.

rate Rate of sending AppleTalk echo requests. This is an optional parameter. Default is one second.

Note: If you enter **atecho** with no parameters, you are prompted for all the parameters. Enter values for the required parameters and either enter values for the optional parameters or accept defaults.

Cache

The **cache** command displays information about the cache-size entries.

Syntax:

cache

Example: `cache`

```
Destination  Interface   Usage  Next Hop
122/22        1          1       27/5
138/51        0          1       27/5
23/7          1          1       Direct
```

Destination
AppleTalk node address (network number/node number).

Net Number of the interface used to forward to the destination node.

Usage Number of times this cache entry has been used in this aging period, which is five seconds. An unused entry is deleted after 10 seconds.

Next Hop
The AppleTalk address of the next hop router used to forward a packet to the destination node, or Direct if the destination node is directly connected to the interface.

Clear Counters

The clear-counters command clears all cache usage counters and packet overflow counters.

Syntax:

clear-counters

Counters

Use the **counters** command to display the number of packet overflows on each network that sends and receives AppleTalk Phase 2 packets. This command displays the number of times the AppleTalk Phase 2 forwarder input queue was full when packets were received from the specified network.

Syntax:

counters

Example: `counters`

```
AP2 Input Packet Overflows

Net            Count

Eth/0            4
```

Dump

Use the **dump** command to obtain routing table information about the interfaces on the router that forwards AppleTalk Phase 2 packets.

Note: `dump` *interface#* displays the part of the overall network and zone information that is visible on that interface.

Syntax:

dump

Example: `dump`

```
Dest Net    Cost     State   Next hop        Zone
  10-19       0       Dir    0/0       "Ethertalk", "Sales"
  40-49       1      Good    10/13     "Marketing", "CustomerSer",
                                       "TokenTalk"
  20-29       2      Sspct   10/13     "Fuchsia", "Backbone",
                                       "Engineering", "MKTING"

3 entries
```

You can also use the **dump** command with a specific interface to display the routes that are visible on that interface. You can use this feature to make sure filters are configured correctly because it shows whether or not filtered zones or networks are visible to an interface.

Example: `dump 0`

```
View for interface 0

Dest net   Cost  State   Next hop   Zone
 214-214   1     Good     152/152   "eth-214"
 153-153   0      Dir               "eth153"
 152-152   0      Dir               "ser152"

3 entries
```

Dest Net
Specifies the destination network number, in decimal.

Cost Specifies the number of router hops to this destination network.

State Specifies the state of the entry in the routing table. It includes the following:

Next hop
Specifies the next hop for packets going to networks that are not directly connected. For directly-connected networks, this is node number 0.

Zone(s)
Specifies the human-understandable name for that network. The zone name(s) is enclosed in double quotes in case there are embedded spaces or non-printing characters. If the zone name contains characters beyond the 7-bit ASCII character set (they are 8-bit), the zone name that displays will depend on the characteristics of your monitoring terminal.

Interface

Use the **interface** command to display the addresses of all the interfaces in the router on which AppleTalk Phase 2 is enabled. If the interface is present in the router but is disabled, this command shows that status.

Note: `interface` *interface#* displays the active filtering for that interface. It displays net, node, default zone, and active filters for one interface.

Syntax:

interface

Example: `interface`

```
Interface     Addresses

  Eth/0       10/52 on net 10-19    default zone  "Sales"
```

You can also enter the interface command followed by a specific interface number to view the AP2 configuration of that interface.

Example: `interface 1`

```
Eth/0   1/30 on net 1-5   default zone "marketing"

Input Net filters inclusive   1-5
Output Zone filters inclusive "finance"
Output Net filters exclusive  1-5
```

Chapter 8. Using VINES

This chapter describes the commands to configure the Banyan VINES protocol and includes the following sections:

Note: If you need more detailed information on VINES Protocols, consult the Banyan publication: *VINES Protocol Definition,* order number: 003673

VINES Overview

VINES Over Router Protocols and Interfaces

The VINES protocol routes VINES packets over the following interfaces and protocols:

- PPP Banyan Vines Control Protocol (PPP BVCP)
- Frame Relay
- Ethernet/802.3
- 802.5 Token Ring
- X.25
- Ethernet ATM LAN Emulation Client
- Token-Ring ATM LAN Emulation Client
- FDDI

It also supports packets across an 802.5 Source Routing Bridge (SRB).

The VINES protocol is implemented at the network layer (layer 3) of the OSI model. VINES routes packets from the transport layer in one node to the transport layer in another node. As VINES routes the packets to their destination nodes, the packets pass through the network layers of the intermediate nodes where they are checked for bit errors. A VINES IP packet can contain up to 1500 bytes including the network layer header and all higher layer protocol headers and data.

Service and Client Nodes

The VINES network consists of service nodes and client nodes. A service node provides address resolution and routing services to the client nodes. A client node is a physical neighbor on the VINES network. All routers are service nodes. A Banyan node can be a service node or client node.

Each service node has a 32-bit network address and a 16-bit subnetwork address. The IBM 8210 has a configurable network address. This address identifies the

router as a service network node for Vines. Banyan has assigned the range30800000 to 309FFFFF to IBM for use in its routers. This router uses the range 30900000 to 3097FFFF.

Note: It is extremely important that no two routers be assigned the same network address. The network address for a Banyan service node is the 32-bit hexadecimal serial number of the service node. The subnetwork address for all service nodes is 1.

The network address for each client node is generally the network address of the service node on the same network. However, if a client node is on a LAN that has more than one service node, it is assigned the network address of the service node that responds first to the client node's address assignment request. The subnetwork address for each client node is a hexadecimal value of 8000 to FFFE.

VINES Network Layer Protocols

This implementation of VINES consists of the following four network layer protocols. The next sections describe these protocols and their implementations.

- "VINES Internet Protocol (VINES IP)". Routes packets through the network.
- "Routing Update Protocol (RTP)" on page 83. Distributes topological information to support the routing services provided by VINES IP.
- "Internet Control Protocol (ICP)" on page 86. Provides diagnostics and support functions to certain transport layer protocol entities, such as providing notification on some network errors and topological conditions.
- "VINES Address Resolution Protocol (VINES ARP)" on page 86. Assigns VINES internet addresses to client nodes that do not already have addresses.

VINES Internet Protocol (VINES IP)

The VINES IP protocol routes packets through the network using the destination network number in the VINES IP header. VINES IP consists of an 18-byte network layer header which prefixes each packet. Table 10 on page 83 summarizes the fields within this header.

VINES IP Implementation

When VINES IP receives a packet, it checks the packet for size and exception errors. A size error is a packet that is less than 18 bytes or greater than 1500 bytes. If it contains a size error, VINES IP discards the packet. An exception error is, for example, a bad checksum or a hop count that has expired.

If the packet does not contain size or exception errors, VINES IP checks the destination address and forwards the packet as follows:

- If the destination address equals the local VINES IP address and the checksum is valid, the local node accepts the packet.
- If the destination address equals the broadcast address and the checksum is valid, VINES IP accepts the packet, processes it locally, and checks the hop count field of the IP header. If the hop count is greater than 0, VINES IP decrements the hop count by one and rebroadcasts the packet on all local media except the one on which the packet was received.

- If the destination address does not equal the local VINES IP address or the broadcast address, VINES IP checks its routing tables for the next hop. If the hop count equals 0, VINES IP discards the packet. Otherwise, it decrements the hop count by one and forwards the packet to the next hop.

  If the destination VINES IP address is not in the routing table and the error bit in the transport control field is set, VINES IP drops the packet and returns an ICP Destination Unreachable message to the source. If the error bit in the transport control field is not set, VINES IP discards the packet and does not return a message to the source.

Table 10. Vines IP Header Fields Summary

VINES IP Header Field	# of Bytes	Description
Checksum	2	Detects bit-error corruption of a packet.
Packet Length	2	Indicates the number of bytes in the packet including the VINES IP header and data.
Transport Control	1	Consists of the following five subfields: **Class** Determines the type of nodes to which VINES IP broadcast packets are sent. **Error** If the error bit is set, an exception notification packet is sent to the transport layer protocol entity when a packet cannot be routed to a service or client node. **Metric** Requests that the service node of the destination client node return to the source a routing cost from the service node to the destination client node. **Redirect** Indicates whether the packet contains an RTP message specifying a better route to use. **Hop Count** Specifies the range a packet can travel. The hop count can range from 0x0 to 0xf.
Protocol Type	1	Specifies the VINES network layer protocol of the packet as VINES IP, RTP, ICP, or VINES ARP.
Destination Network Number	4	A 4-byte network number in the VINES IP address of the destination.
Destination Subnetwork Number	2	A 2-byte subnetwork number in the VINES IP address of the destination.
Source Network Number	4	A 4-byte network number in the VINES IP address of the source.
Source Subnetwork Number	2	A 2-byte subnetwork number in the VINES IP address of the source.

Routing Update Protocol (RTP)

RTP gathers and distributes routing information that VINES IP uses to compute routes throughout the network. RTP enables each router to periodically broadcast routing tables to all of its neighbors. The router then determines the destination neighbor it will use to route the packet.

Service nodes maintain two tables: a routing table and a neighbor table. Both of these tables have timers that age their contents to eliminate out-of-date entries. Routing updates for X.25 interfaces occur when there is a change in the routing database, for example, when a node goes up/down or the metric changes.

Routing Table

The routing table contains information about the service nodes. Figure 5 shows a sample routing table. Descriptions of the fields in this table follow the figure.

```
Net Address  Next Hop Nbr Addr Nbr Intf   Metric   Age (secs)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

  S  30622222       30622222:0001    Eth/0       20       30

  H  0027AA21       0027AA21:0001    Eth/1       2        120

  P  0034CC11       0034CC11:0001    X.25/0      45       0

  3 Total Routes
```

S ⇒ Entry is suspended, H ⇒ Entry is in Hold-down, P ⇒ Entry is permanent

Figure 5. Sample Routing Table

Routing Table Field
Description

Net Address
The Net Address is a unique 32-bit number. An S, H, or P preceding the Net Address field indicates the following:

- **S** Indicates the service node is in suspended state and is advertised, for 90 seconds, as being down. After 90 seconds, the router removes the entry for this service node from the routing table.
- **H** Indicates the service node is in hold-down state and is advertised, for 2 minutes, as being down. After 2 minutes, the router advertises the service node as operational. If a service node is in suspended state and it receives an RTP packet, the service node enters the hold-down state.
- **P** Indicates that the X.25 interface enters permanent state for 4-1/2 minutes after initialization. After 4-1/2 minutes, the neighbor enters the permanent state and its age stays at 0 while in this state. If the X.25 interface goes down, the entry is removed from the routing table.

Next Hop Nbr Addr
The address of the neighbor service node that is the next hop on the least-cost path to the network.

Nbr Intf
The medium to which the next hop neighbor service node is attached.

Metric An estimated cost, in 200-millisecond increments, to route the VINES packet to the destination service node.

Age (secs)
The current age, in seconds, for the entry. If a router does not receive an update about a service node that is in the routing table at least every 360 seconds (6 minutes), the router removes the entry for that service node from the routing table.

Neighbor Tables

The neighbor table contains information about the neighbor service nodes and client nodes connected to the router. Figure 6 shows a sample neighbor table and descriptions of the fields in this table follow the figure.

```
Nbr Address    Intf   Metric   Age(secs)   H/W Addr RIF
- - - - - - - - - - - - - - - - - - - - - - - - - - - -

30633333:0001  TKR/0     4        30     0000C0095012

0035CC10:8000  Eth/1     2        120    0000C0078221

2 Total Neighbors
```

Figure 6. Sample Neighbor Table

Neighbor Table Field
Description

Nbr Address
The address of the neighbor node. In Figure 6, the address 30633333:0001 is a service node and address 0035CC10:8000 is a client node.

Intf The medium to which the neighbor node is attached.

Metric An estimated cost, in 200-millisecond increments, to route the VINES packet to the neighbor node.

Age (secs)
The current age, in seconds, for the entry. If a router does not receive a routing update from a neighbor at least every 360 seconds (6 minutes), the router removes the entry for that neighbor from the neighbor table and, if the neighbor is a service node, from the routing table.

H/W Addr
The node's LAN address if the neighbor is connected to a LAN. If the Frame Relay protocol is running, the H/W Addr is the Data Link Connection Identifier (DLCI). For X.25 interfaces, the H/W Addr is the X.25 address of the neighbor.

RIF Routing Information Field. A sequence of segment and bridge numbers, in hexadecimal, which indicate a path through the network between two stations. RIF is required for source routing.

RTP Implementation

RTP entities issue the following packets:

- *RTP request packets.* Requests to the service nodes to obtain the current network topology. On initialization, an X.25 interface generates routing request packets every 90 seconds to each X.25 destination on the X.25 interface. When the X.25 interface receives a routing response packet, three full routing database updates, spaced 90 seconds apart, are sent to the services nodes that sent the

routing response packets. Once the X.25 interface receives routing response packets from all of the X.25 destination nodes, routing requests are no longer sent to those X.25 addresses.

- *RTP update packets.* Packets sent by client nodes to the service nodes to notify the service nodes of their existence. RTP update packets are also sent by the service nodes to notify other nodes of their existence and to advertise their routing databases.
- *RTP response packets.* Packets service nodes send in response to RTP request packets.
- *RTP redirect packets.* Informs the nodes of the best paths between them for routing packets.

Unless connected by a permanent circuit, every client and service node broadcasts an RTP update every 90 seconds. This notifies the neighbors of the node's existence and its type (service or client node) and, in the case of service nodes, advertises their routing databases. When a router receives an update packet from a service node, RTP extracts the VINES IP address and looks in the routing table for an existing entry on that service node. If it exists, RTP updates the entry and resets the entry's timer. If an entry does not exist, RTP creates one and initializes the timer for that entry.

Internet Control Protocol (ICP)

ICP generates network information messages on two types of packets destined for the local router:

- *Destination unreachable packet.* Indicates a packet could not reach its destination and was returned to its source. The router then issues an ELS message and flushes the packet.
- *Delay metric packet.* A request packet from a source node for the routing metric from the destination service node to the destination client node.

VINES Address Resolution Protocol (VINES ARP)

The VINES ARP protocol assigns unique VINES IP addresses to the client nodes. VINES ARP includes the following packet types:

- *Query request packet.* Packets the client nodes broadcast on initialization.
- *Query response packet.* The service node's response to a query request packet.
- *Assignment request packet.* The client node's response to a query response packet.
- *Assignment response packet.* Includes the network and subnet addresses the service node assigned to a client node.

To assign a VINES IP address to a client node, VINES ARP implements the following algorithm:

1. The client node broadcasts a query request packet.
2. Service nodes respond with a query response packet containing the destination MAC address of the client node and a broadcast VINES IP address.
3. The client node issues an assignment request packet to a service node that responded with a query response packet.
4. The service node responds with an assignment response packet that contains the VINES network and subnetwork addresses.

Each client node maintains a timer that has a default setting of two seconds. The timer starts when a client node transmits a query request or assignment request packet. The client node stops and resets the timer when it receives a query response packet. When a timeout period exceeds two seconds, the client node initializes, broadcasts a query request packet, and resets the timer. Table 11 summarizes the states the service and client nodes enter during VINES ARP implementation.

Table 11. Client and Service Node VINES ARP States

Client Node States	
Initialization	The client node is initializing.
Query	The client node is transmitting a query request packet.
Request	The client node received a query response packet from a service node and is transmitting an assignment request packet to the service node it heard from.
Assigned	The client node received an assignment response packet containing the VINES network and subnetwork addresses.
Service Node States	
Initialization	The VINES ARP protocol is initializing.
Listen	The service node is waiting for query request packets from the client nodes.
Service	The service node received a query request packet and sent a query response packet.
Assignment	The service node issues an assignment response packet containing the VINES network and subnetwork addresses.

Basic Configuration Procedures

The steps to initially configure each router that sends and receives VINES packets are as follow:

1. Assign a unique 32-bit hexadecimal address to each router in the VINES network. Using the **set network-address** *hex #* command, enter a network address from 30900000 to 3097FFFF. The network address for Banyan servers is the 32-bit hexadecimal serial number of the service node. This number is automatically read from the node server key.
2. Globally enable the VINES protocol using the **enable VINES** command.
3. Enable the interface cards that are to transmit and receive the VINES packets using the **enable interface** *interface#* command.

For configuration changes to take effect you must restart the router. Enter **reload** after the OPCON prompt (*) and answer **yes** to the following prompt:

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

To view the configuration, enter the **list** command after the `VINES config>` prompt.

Running Banyan VINES on the Bridging Router

Banyan VINES servers must have this Banyan option to communicate with other servers or routers:

Server-to-server LAN.

Using VINES

To communicate across X.25 WANs, VINES servers directly connected to the WAN need these two options:

Server-to-server WAN

X.25 support on the server (hardware and software).

Running Banyan VINES over WAN Links

When you set up a PPP, Frame Relay, or X.25 link for use with VINES, you must set the HDLC speed of the link, even if you set the clocking to external.

If you set the HDLC speed to zero, VINES assumes that the speed is 56 Kbps. Do not set the speed to a value that is faster than the line.

Chapter 9. Configuring and Monitoring VINES

This chapter describes the VINES configuring and monitoring commands and includes the following sections:

Accessing the VINES Configuration Environment

To access the VINES configuration environment, enter the following command at the `Config>` prompt:

```
Config> protocol vin
VINES Protocol user configuration
VINES Config>
```

VINES Configuration Commands

This section summarizes and then explains the VINES configuration commands. Enter these commands at the `VINES config>` prompt.

Table 12. VINES 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 xxi.
Add	Adds an X.25 address translation.
Delete	Deletes an X.25 address translation.
Disable	Disables the VINES protocol on all interfaces or a single interface and disables checksumming.
Enable	Enables the VINES protocol on all interfaces or a single interface and enables checksumming.
List	Displays the current VINES configuration.
Set	Assigns the network addresses to routers in the VINES network and sets the maximum number of physical neighbor client and service nodes.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxii.

Add

Adds an X.25 address translation.

Syntax:

add interface ...

Specifies the interface number.

remote-X.25-addr
Can include up to 15 digits. If the virtual circuit connection has been configured as PVC, the VINES *remote-X.25-addr* must match the PVC address configured at the X.25 prompt. If the addresses do not match, the system defaults to a switched virtual circuit (SVC).

handle
user-configurable name that uniquely identifies each remote server.

Example: `add interface 0 4508907898 test`

Delete

Deletes an X.25 address translation.

Syntax:

delete interface ...

Specifies the interface number.

remote-X.25-addr
Can include up to 15 digits. If the specified interface has not been configured using the VINES **add interface** command, the terminal displays the message `That X.25 address has not been configured.`

Example: `delete interface 1 4799999999 compress`

Disable

Use the **disable** command to disable the VINES protocol on all interfaces or a single interface, or to disable checksumming.

Syntax:

disable checksumming ...

interface ...

vines

checksumming *interface#*
Disables checksumming on packets that the specified interface generates, broadcast packets excluded. For all interfaces, the default is checksumming disabled.

Example: `disable checksumming 0`

interface *interface#*
Disables the VINES protocol on the specified interface.

Example: `disable interface 1`

vines Disables the VINES protocol on all interfaces.

Example: `disable vines`

Enable

Use the **enable** command to enable the VINES protocol on all interfaces or a single interface, or to enable checksumming.

Syntax:

enable checksumming ...

interface ...

vines

checksumming *interface#*
Enables checksumming on packets that the specified interface generates.

Example: `enable checksumming 0`

interface *interface#*
Enables the VINES protocol on the specified interface.

Example: `enable interface 1`

vines Globally enables the VINES protocol. If you receive an error message after entering this command, contact your customer service representative. The VINES software may not be in your software load.

Example: `enable vines`

List

Use the **list** command to display the current VINES configuration.

Syntax:

list

Example: `list`

```
VINES:  enabled/disabled
VINES network number (hex):
Maximum Number of Routing Table Entries:
Maximum Number of Neighbor Service Nodes:
Maximum Number of Neighbor Client Nodes:

List of interfaces configured for VINES:

intf 0        (checksumming enabled/disabled)
intf 1        (checksumming enabled/disabled)
intf 2        (checksumming enabled/disabled)

VINES X.25 Configuration

Interface     Remote X.25 Address        Remote Handle
    0            4508907898              test

VINES config>
```

VINES Indicates whether VINES is globally enabled or disabled.

VINES network number (hex)
A configurable 32-bit hexadecimal address for routers in the VINES network.

Maximum Number of Routing Table entries
A configured value specifying the maximum number of entries allowed in the VINES routing table.

Maximum Number of Neighbor Service Nodes
A configured value specifying the maximum number of neighbor service nodes connected to the router.

Maximum Number of Neighbor Client Nodes
A configured value specifying the maximum number of client nodes connected to the router.

List of interfaces configured for VINES
Displays the interfaces that have VINES enabled and whether checksumming is enabled or disabled.

VINES X.25 Configuration

This information represents the following:

Interface
The interface that is configured for X.25.

Remote X.25 Address
The DTE address of the remote server.

Remote Handle
A user-configurable name that uniquely identifies the remote server.

Set

Use the **set** command to assign network addresses to routers in the VINES network and to specify the maximum number of client and service nodes.

Syntax:

set client-node-neighbors ...
network-address ...
routing-table-size ...
service-node-neighbors ...

client-node-neighbors #
Specifies the maximum number of client nodes on your network. **Client-node-neighbors** includes all of the nodes on each network directly connected through the router. The range is 1 to 65535, and the default is 25.

Note: It is recommended that you set this number significantly higher than the number of nodes in your network. This will enable your network to continue functioning without reconfiguring and restarting the routers when additional nodes are added. The increase in this number depends on the size of your network and the amount of anticipated growth. As a rule, set **client-node-neighbors** 25 % higher than the actual number of client stations on LANs that are local to the router.

Example: `set client-node-neighbors 20`

network-address *hex#*
Assigns a network address to each router in the VINES network. *Hex#* is a 32-bit hexadecimal value from 30900000 to 3097FFFF.

Example: `set network-address 30922222`

routing-table-size *#*
Specifies the maximum number of service nodes and routers in the VINES network. The range is 1 to 65535, and the default is 300.

Note: Make sure that the number you specify is large enough to accommodate additional VINES servers and 8210s as your network grows.

Example: `set routing-table-size 250`

service-node-neighbors *#*
Specifies the maximum number of physical neighbor service nodes. This

number includes VINES servers and 8210s that are the first point-of-contact after crossing a WAN. The range is 1 to 65535, and the default is 50.

Example: `set service-node-neighbors 100`

Accessing the VINES Monitoring Environment

To access the VINES monitoring environment,

```
* t 5
```

Then, enter the following command at the **+** prompt:

```
+ protocol vin
VINES>
```

VINES Monitoring Commands

This section describes the VINES monitoring commands. Enter these commands at the VINES> prompt.

Table 13. VINES 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 xxi.
Counters	Displays routing errors and the number of times the VINES input queue was full when packets were received from the specified interface.
Dump	Displays the current contents of the VINES routing and neighbor tables.
Route	Displays an entry from the VINES routing table.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxii.

Counters

Use the **counters** command to display routing errors and the number of times the VINES input queue was full when packets were received from the specified interface.

Syntax:

counters

Example: `counters`

```
  Routing Errors
Count           Type
-----           ----
  2          Net Unreachable
  3          Hop Count Expired
  3          Routing Update from Orphan Client
  0          Routing Redirect Received
  0          Routing Response Received

  VINES Input Packet Overflows
   Net      Count
   ---      -----
  Eth/0      5
  Eth/1      1
```

Net Unreachable
The number of times the router received a packet destined for a node that was not found in the routing table.

Hop Count Expired
The number of times the router discarded a packet because its hop count expired.

Routing Update from Orphan Client
The number of times the router received an update packet from a client node whose service node does not exist. A routing update from an orphan client can occur when the router boots and hears from the client node first rather than the service node, or when a client's service node is down and an entry has been removed from the routing table database.

Routing Redirect Received
The number of times the router received redirect packets from the service nodes.

Routing Response Received
The number of times response packets were generated as a result of request packets initiated by the router.

VINES input packet overflows
The number of times the VINES forwarder input queue was full when packets were received from the specified interface. The packets are subsequently discarded.

Dump

Use the **dump** command to display the contents of the VINES routing and neighbor tables.

Syntax:

dump neighbor-tables
routing-tables

neighbor-tables
Displays information about each neighbor service and client node connected to the router.

Example: `dump neighbor-tables`

```
   Nbr Address    Intf     Metric  Age(secs)   H/W Addr    RIF
 ------------------------------------------------------------
  30622222:0001  TKR/0     4           30     0000C00     95012
  0035CC10:8000  Eth/0     2          120     0000C00     78221

   2 Total Neighbors
```

Nbr Address
The address of the neighbor node. In the above example, address 30622222:0001 is a service node and address 0035CC10:8000 is a client node.

Intf The medium to which the neighbor node is attached.

Metric An estimated cost, in 200-milliseconds, to route the VINES packet to the neighbor node.

Age (secs)
The current age, in seconds, for the entry. If a router does not receive a routing update from a neighbor at least every 360

seconds (6 minutes), the router removes the entry for that neighbor from the neighbor table and, if the neighbor is a service node, from the routing table.

H/W Addr
The node's LAN address if the neighbor is connected to a LAN. If the Frame Relay protocol is running, the H/W Addr is the Data Link Connection Identifier (DLCI). For X.25 interfaces, the H/W Addr is the X.25 address of the neighbor.

RIF Routing Information Field. A sequence of segment and bridge numbers, in hexadecimal, which indicate a path through the network between two stations. RIF is required for source routing.

routing-tables
Displays information about each service node known by the router.

Example: `dump routing-table`

```
Net Address  Next Hop Nbr Addr   Nbr Intf  Metric   Age (secs)
-----------  -----------------   --------  ------   ----------
S  30622222   30622222:0001      Eth/0        20         30
H  0027AA21   0027AA21:0001      Eth/1        2          120
P  0034CC11   0034CC11:0001      X.25/0       45         0

3 Total Routes

S ==> Entry is suspended, H ==> Entry is Holdown, P ==> Entry
is permanent
```

Net Address
The Net Address is a unique, configurable 32-bit hexadecimal value from 30900000 to 3097FFFF. This range of numbers is assigned to IBM by Banyan. It is very important that no two routers on a network are assigned the same Net Address. The Net Address for a Banyan service node is the 32-bit hexadecimal serial number of the service node. An S, H, or P preceding the Net Address field indicates the following:

S: The service node is in suspended state and is advertised, for 90 seconds, as being down. After 90 seconds, the router removes the entry for this service node from the routing table.

H: The service node is in hold-down state and is advertised, for 2 minutes, as being down. After 2 minutes, the router advertises the service node as operational. If a service node is in suspended state and it receives an RTP packet, the service node enters the hold-down state.

P: After initialization, the X.25 interface enters permanent state for 4 and 1/2 minutes. After 4 and 1/2 minutes, the neighbor enters the permanent state and its age stays at 0 while in this state. If the X.25 interface goes down, the entry is removed from the routing table.

Next Hop Nbr Addr
The address of the neighbor service node that is the next hop on the least-cost path to the network.

Nbr Intf
The medium to which the next hop neighbor service node is attached.

Metric An estimated cost, in 200-milliseconds, to route the VINES packet to the destination service node.

Age (secs)
The current age, in seconds, for the entry. If a router does not receive a routing update about a service node that is in the routing table at least every 360 seconds (6 minutes), the router removes the entry for that service node from the routing table.

Route

Use the **route** command to view an entry from the routing table.

Syntax:

route given address

given address
The network address of the service node.

Example: `route 30622222`

```
Net Address  Next Hop Nbr Addr   Nbr Intf  Metric   Age (secs)
-----------  -----------------   --------  ------   ----------
30622222      30622222:0001       Eth/0       2       30
```

Chapter 10. APPN

This chapter describes APPN and includes the following sections:

Note: All references to token-ring and Ethernet apply emulated LANs.

What is APPN?

Advanced Peer-to-Peer networking (APPN) extends the SNA architecture by enabling Type 2.1 (T2.1) nodes to communicate directly without requiring the services of a SNA host computer.

Peer-to-Peer Communications

T2.1 nodes can activate connections with other T2.1 nodes and establish LU-LU sessions with other nodes. The relationship between a pair of T2.1 nodes is referred to as a *peer relationship* because either side can initiate communication.

Prior to APPN, a T2.1 node could communicate directly with another T2.1 node, but required the services of a centralized SNA host to locate its partner and any associated resources. All routes between the two nodes were predefined. APPN enhanced the T2.1 node function by:

- Requiring network resources to be defined only at the node where they are located
- Distributing information about these resources throughout the network as needed
- Dynamically generating routes between nodes using current information about the network's topology and the desired class of service

APPN Node Types

The APPN architecture allows four types of nodes in a network:

- APPN network nodes
- APPN end nodes
- Low-entry networking (LEN) end nodes
- PU 2.0 nodes supported by DLUR

The router can be configured as an APPN network node that supports connections with all four node types. The router cannot function as an end node for APPN.

APPN Network Node

An APPN network node provides directory and routing services for all resources (LUs) in its domain. A network node's domain consists of:

- Local resources owned by the node

- A control point (CP), which manages the node's resources
- Resources owned by APPN end nodes and LEN end nodes that use the services of the network node

APPN network nodes also:

- Exchange information about the topology of the network. This information is exchanged each time network nodes establish a connection or when there is a change in the topology of the network (such as when a network node is deactivated, brought on line, or when a link is congested or fails). When a network node receives a topology update, it broadcasts this information to other active and network nodes with which it has CP-CP sessions.
- Act as intermediate nodes, receiving session data from one adjacent node and passing that data on to the next adjacent node along the route.

As a network node, the router can act as a server to attached APPN end nodes and LEN end nodes and provide functions that include:

Directory services
: The network node, communicating with other network nodes, can locate a resource in the network on behalf of an APPN end node. The network node also maintains a local directory of APPN and LEN end node resources that it can search on behalf of an attached APPN end node, attached LEN end node, or other network nodes.

Topology and Routing services
: At the request of an APPN end node, the network node dynamically determines the route from an origin logical unit (LU) to a destination LU in the network. The network node also maintains information on other network nodes and the routes to those nodes. The route is based on the current topology of the network.

Management services
: The network node can pass *alert* conditions to a designated focal point to allow centralized problem management. The network node is responsible for processing alert conditions for all the resources in its domain. "Managing a Network Node" on page 108 describes this process.

APPN End Nodes

An APPN end node provides limited directory, routing, and management services for logical units (LUs) associated with the node. An APPN end node selects a network node to be its network node server. If the network node agrees to act as the APPN end node's server, the end node can register its local resources with the network node. This enables the network node server to intercept and pass along search requests for resources located on the APPN end node.

The APPN end node and its network node server communicate by establishing CP-CP sessions. An APPN end node may be connected to a number of network nodes, but only one of these nodes acts as the APPN end node's server at any one time.

The APPN end node forwards all requests for unknown resources to the network node server. The network node server, in turn, uses its search facilities to locate the requested resource and calculate a route from the APPN end node to the resource.

LEN Nodes

A LEN node is a T2.1 node without APPN extensions. A LEN node can establish peer connections with other LEN nodes, APPN end nodes, and APPN network nodes, as long as all of the required destination LUs are registered with the LEN node. A LEN node can also serve as a gateway between an APPN network and a SNA subarea network.

Because a LEN node cannot establish CP-CP sessions with an APPN network node server, it cannot register its resources with the server or request that the server search for a resource and dynamically calculate a route to that resource. A LEN node may indirectly use the directory and routing services of a network node by pre-defining remote LUs (owned by nonadjacent nodes) as being located on an APPN network node, although the actual location may be anywhere in the network. When the LEN node needs to initiate a session with the remote LU, it sends a session activation request (BIND) for the LU to the network node. In this case, the network node acts as the LEN node's network node server, locating the requested resource, calculating a route, and forwarding the BIND to its correct destination.

When configuring the router network node, you can specify the names of LUs that are associated with an attached LEN end node. These LU names reside in the router network node's local directory. If the router network node receives a request to search for one of these LEN end node resources, it will be able to find the LU in its local directory and return a positive response to the node originating the search. To reduce the number of LU names you need to specify for an attached LEN end node, the router supports the use of generic LU names, which allow a wildcard character to represent a portion of an LU name.

PU 2.0 Nodes

A PU 2.0 node is a type T2.0 node containing dependent LUs. PU 2.0 nodes are supported by the Dependent LU Requestor (DLUR) function which is implemented by an APPN end node or network node. PU 2.0 nodes require the services of a system services control point, which is made available through the DLUR-enabled APPN node. Note that APPN nodes can contain dependent LUs supported by the DLUR function. However, the router does not contain dependent LUs.

What APPN Functions Are Implemented on the Router?

The router implements the APPN Release 2 base architecture functions as defined in the Systems Network Architecture APPN Reference. The APPN network node functions implemented by the router are summarized in Table 14. Notes on specific functions follow the table. For a description of the APPN management services supported by the router, see "Managing a Network Node" on page 108.

APPN uses LU 6.2 protocols to provide peer connectivity between CP-CP session partners. The router network node implements the LU 6.2 protocols required for CP-CP sessions and those used in sessions between a network node CP and its network management focal point. The router implementation of APPN does not provide an application program interface to support user-written LU 6.2 programs.

Table 14. Implementation of APPN Network Node Functions

APPN Function	Yes	No	Notes
Session services and supporting functions			
Multiple CP-CP sessions	X		

Table 14. Implementation of APPN Network Node Functions (continued)

APPN Function	Yes	No	Notes
Mode name to class of service (COS) mapping	X		1
Limited resource link stations	X		2
BIND segmentation and reassembly	X		3
Session-level security	X		4
Intermediate session routing			
Intermediate session routing	X		
Routing of dependent LU sessions	X		
Fixed and adaptive session-level pacing	X		
RU segmentation and reassembly	X		5
Directory services			
Broadcast searches	X		
Directed searches	X		
Directory caching	X		
Safe storage of directory services cache		X	6
Central directory server		X	7
Central directory client	X		7
Registration of APPN EN LUs with network node server	X		
Definition of LEN node LUs on network node server	X		
Use of wild cards to define attached LEN node resources	X		
Accept multiple “resource found” conditions	X		
Network node server for DLUR EN - Option set 1116	X		
Topology and routing services			
Topology exchange	X		
Periodic topology broadcasts	X		8
Topology database maintenance	X		9
Topology awareness of CP-CP sessions	X		
Randomized route computation	X		10
Cached routing trees	X		11
Safe storage of topology database		X	
Garbage Collection Enhancements	X		
Connectivity			
Connection network definition	X		12
Multiple transmission groups	X		
Parallel transmission groups	X		
Management services			
Multiple domain support (MDS)	X		
Explicit focal point	X		
Implicit focal point	X		
Held alerts	X		
SSCP-PU sessions with focal points		X	
SNA/MS problem diagnosis data in alerts	X		

Notes:

1. New mode names can be defined on the router using the Command Line interface. These new mode names can be mapped to existing Class of Service (COS) definition names or to new COS definitions, which may be defined using the Configuration tool.
2. Limited resource link stations are supported for:
   - connection network links

- ATM SVC.

3. When the router activates a TG to an adjacent node, it negotiates with that node the maximum message size that can be sent across the TG. If a BIND message is larger than the negotiated message size, the router segments the BIND. Segmentation only occurs if the adjacent node is capable of reassembling the BIND. The router supports BIND reassembly.
4. A session level security feature can be enabled for connections between the router network node and an adjacent node. Both partners in the connection require a matching hexadecimal key that enables each node to verify its partner before the connection is established.
5. When routing session data to an adjacent node, the router segments a request/response unit (RU) if the message unit exceeds the maximum message size that can be sent across the transmission group. If the router receives a segmented RU, the node reassembles it.
6. After successfully locating a resource in the APPN network, the router stores or *caches* this information in its local directory database for future use. However, the router does not save these cached directory entries to a permanent storage medium, such as a disk, to provide for recovery if the node fails.
7. The router cannot be used as a central directory server for an APPN network. The router is capable of using a central directory server, however, to obtain directory information about the location of a resource in the network.
8. To prevent other network nodes from discarding information about the router from their topology databases, the router creates a topology database update (TDU) about itself and its locally-owned transmission groups every 5 days and broadcasts this TDU to network nodes.
9. An interval timer is associated with every resource entry in the router's network topology database. If the router does not receive any information about a resource within 15 days, it discards the entry for that resource from the database.
10. If there is more than one least-weight route from an origin LU to a destination LU for a given class of service, the router randomly selects one of these routes for the session. This practice helps distribute the flow of traffic in the network.
11. The router maintains a copy of the network topology database. The database identifies the available routes to other network nodes for a particular class of service. When the router needs to calculate a route to a network node or to an end node adjacent to that network node, it uses information in the topology database to generate a routing tree for that network node. The routing tree identifies the optimal routes to the network node for the class of service required.

    When the router generates a new routing tree, it stores that tree in a cache. When the router receives a service request, it checks this cache first to see if a route has been computed. Use of the cache reduces the number of route calculations required. When the router receives topology information that invalidates a routing tree, it discards the tree. The router recalculates the tree as needed and caches the new tree.
12. The router can be defined as a member of a connection network on Ethernet ports, Token-Ring ports, Enterprise Extender Support for HPR over IP, and ATM ports.

APPN Network Node Optional Features

In addition to the base APPN Architecture functions, the router also implements the following option set towers and new functions:

087 Garbage Collection Enhancements

1002 Adjacent Link Station name

1007 Parallel TGs

1012 LU name = CP name

1016 Extended Border Node

1061 Prerequisites for SS Extensions for NNS Support

1063 SS Extensions NNS Support

1067 Dependent LU Requester

1071 Generalized ODAI Usage

1101 Preloaded Directory Cache

1107 Central Resource Registration (of LUs)

1116 Network Node Server support for DLUS-Served LU registration

1119 Report Branch Topology to a Manager

1120 Branch Awareness

1121 Branch Extender

1200 Tree Caching and TG Caching

1201 Permanent Storage Medium

1400 High-Performance Routing (HPR)

1401 Rapid Transport Protocol (RTP)

1402 Control Flows over RTP

1405 HPR Border Node

Node performance tuning

Node service traces

Accounting and node statistics collection

High-Performance Routing

HPR is an enhancement to APPN architecture that provides better performance over high speed, low error rate links using existing hardware. HPR replaces the normal APPN intermediate session routing (ISR) with a Network Control Layer (NCL) containing a new type of source routing function called automatic network routing (ANR). The complete HPR route is contained in the ANR packet allowing intermediate routing nodes to route the packets with less processing overhead and storage.

HPR also eliminates the error recovery and flow control (session-level pacing) procedures for each link between nodes and moves the error recovery and flow/congestion control procedures to the end-points of an HPR connection. A transport layer using a new error recovery procedure called Rapid Transport

Protocol (RTP) is used by the endpoints of the HPR connection. HPR intermediate nodes have no session or RTP connection awareness. This new transport layer features:

- Selective retransmission error recovery procedure
- Segmentation and reassembly
- Adaptive Rate-Based (ARB) flow and congestion control mechanism that meters data onto a route that allows efficient utilization of network resources while minimizing congestion. ARB uses a preventative rather than reactive approach to flow and congestion control.
- Non-disruptive Path Switch (NDPS) function that automatically reroutes traffic around node or link failures without disrupting end user sessions.
- Detection of Forward Explicit Congestion Notification (FECN) bit set, allowing RTP's adaptive rate-based flow and congestion control algorithm to adjust the data send rate. This algorithm prevents traffic bursts and congestion, maintaining a high level of throughput.

The router implements both ANR routing and Rapid Transport Protocol. Therefore, the router can function both as an intermediate routing HPR node and as an HPR connection endpoint node.

Interoperability

HPR uses APPN network control functions including class of service (COS)-based least-weight route calculation and transmission priority. HPR interoperates seamlessly with APPN ISR:

- The network automatically adapts to the presence of HPR-capable nodes and HPR-enabled links.
- An APPN network can have any mix of ISR and HPR links, although the greatest benefit of HPR is realized when the network has three or more HPR-enabled nodes with two or more HPR-capable links back-to-back. This allows the middle HPR node to be an HPR intermediate node and use only ANR routing, allowing session data to be routed through the middle node using only NCL.
- A given session route can be made up of a combination of ISR and HPR links.
- HPR uses the same TG and node characteristics for least-weight route calculation as APPN ISR. No special consideration is given to HPR capable nodes or links other than their potentially improved characteristics (such as higher effective capacity if a higher speed link).

Traffic types

APPN ISR uses the IEEE 802.2 LLC Type 2 protocol for token-ring and Ethernet. APPN HPR, which is supported on token-ring and Ethernet, does not use LLC Type 2 protocol, but does use some functions of an APPN link station for XID and inactivity timeout. A single APPN link station is therefore used for ISR or HPR. Different mechanisms are used to distinguish between ISR and HPR traffic depending upon the DLC type.

Each protocol that uses a port must have a unique SAP address. A unique SAP address identifies the APPN link station for HPR traffic (Local HPR SAP address parameter). If ISR traffic is destined for a link station, then a different SAP address (Local APPN SAP address parameter) must be used. The ISR traffic uses LLC Type 2 LAN frames. The HPR traffic is handled in similar fashion to LLC Type 1 LAN frames and must have a different SAP address.

The default SAP address for HPR traffic is X'C8'. If X'C8' has already been used by another protocol on a port, the default must be overridden.

Note: There is only one APPN link station even though APPN ISR and HPR traffic use different SAP addresses.

Dependent LU Requester (DLUR)

The DLUR option extends the support of T2.0 or T2.1 devices containing dependent LUs to APPN nodes. The DLUR function on an APPN network node or an APPN end node works in conjunction with a dependent LU server (DLUS) in a mixed APPN/subarea network. The DLUS function may reside in some other part of the mixed network from the DLUR.

The dependent LU flows (SSCP-PU and SSCP-LU) are encapsulated over an LU 6.2 (CP-SVR) pipe established between the DLUR APPN node and the DLUS SSCP. The CP-SVR pipe is made up of a pair of LU 6.2 sessions using a new CPSVRMGR mode between the DLUR and the DLUS. This pipe brings the SSCP function (in the DLUS) to the DLUR APPN node where it can be made available to attached T2.0/T2.1 nodes containing dependent LUs.

The dependent LU will appear to be located within the domain of the serving SSCP. Session initiation flows will be emulated from the DLUS, but session bind and data paths will be calculated directly between the dependent LU and its session partner. This path may or may not traverse the serving DLUS node.

Set the adjacent node type parameter to **PU 2.0 Node** when defining a link station to a T2.0 adjacent node containing dependent LUs. Set the adjacent node type parameter to **APPN end node** or **LEN end node** when defining a link station to a T2.1 adjacent node containing dependent LUs.

Functions Supported

The APPN DLUR option includes the following functions:

- Support for downstream T2.0 nodes containing dependent LUs that respond with XID type 0 and XID type 1.
- Support for downstream T2.1 nodes containing dependent LUs that respond with XID type 3.
- Support for dependent LUs that is equivalent to the support provided by the Subarea environment for:
  - Activating PUs and their LUs
  - Locate and be located by other LUs in an APPN or subarea network
  - Determine LU's characteristics
  - Allow terminal operators to logon to applications both in APPN and subarea networks
  - SSCP takeover
  - Uninterrupted LU-LU sessions, if the supporting DLUS (SSCP) fails
  - SLU init, PLU init, and Third-party init

Restrictions

The DLUR option, as implemented on the router network node, has the following functional restrictions:

- Only secondary LUs (SLUs) can be supported by the DLUR function. An LU supported by DLUR cannot function as a primary LU (PLU). Therefore, the downstream physical unit (DSPU) should be configured as secondary.
- Because only SLUs are supported, Network Routing Facility (NRF) and Network Terminal Option (NTO) are not supported.
- Extended recovery facility (XRF) and XRF/CRYPTO are not supported.
- DLUR and DLUS must be in the same APPN topology network, but they can be in different subnets. The CPSVRMGR session cannot pass through a subarea network. If the Border Node (either the same netid or different netid) is used, the DLUR can reside in a different (sub-)network than DLUS.

VTAM Considerations for DLUR

The following are example VTAM Switched Major Node definitions for DLUR. You should note that PATH statements are necessary only if VTAM is initiating the connection to the DSPU.

You should refer to *VTAM Resource Definition Reference* SC31-6427, for details of the DLC parameter statements for the Switched Major Node definitions.

```
DABDLURX VBUILD TYPE=SWNET,MAXGRP=400,MAXNO=400,MAXDLUR=20
*********************************************************************
*IN THE DLCADDR, THE 'SUBFIELD_ID' = CV SUBFIELD OF THE CV91          *
* MINUS 0X90.                                                        *
*FOR EXAMPLE, THE CV94 SUBFIELD IS CODED ON DLCADDR=(4,X,...          *
*********************************************************************
*********************************************************************
* Following are PU Statements for 2.0 and for 2.1
*********************************************************************
*********************************************************************
* 2.0 PU STATEMENT
*********************************************************************
*PU20RT   PU   ADDR=05,PUTYPE=2,MAXPATH=8,ANS=CONT,USSTAB=AUSSTAB,
*              ISTATUS=ACTIVE,MAXDATA=521,IRETRY=YES,MAXOUT=7,
*              PASSLIM=5,IDBLK=017,IDNUM=00035,MODETAB=AMODETAB
*              LOGAPPL=ECHO71,DLOGMOD=M23278I
*********************************************************************
* Path statements are not required if the DSPU is initiating the
* connection to VTAM
*********************************************************************
*PU20LU1  LU    LOCADDR=2
*PU20LU2  LU    LOCADDR=3
*PU20LU3  LU    LOCADDR=4
*********************************************************************
* 2.1 PU STATEMENT
*********************************************************************
*PU21RT   PU   ADDR=06,PUTYPE=2,CPNAME=PU21RT,ANS=CONT,MAXPATH=8,
*              ISTATUS=ACTIVE,USSTAB=AUSSTAB,MODETAB=AMODETAB
*              LOGAPPL=ECHO71,DLOGMOD=M23278I
*********************************************************************
*********************************************************************
* There is no difference in the path statement definitions
* between a PU 2.0 and a PU 2.1
*
* Path statements are required if VTAM is initiating the connection
* to the DSPU.
*
*********************************************************************
```

```
*********************************************************************
*********************************************************************
* LU statements
*********************************************************************
*********************************************************************
*PU21LU1  LU    LOCADDR=2
```

```
*PU21LU2  LU    LOCADDR=3
*PU21LU3  LU    LOCADDR=4
************************************************************************
```

Notes:

1 The difference between PU statement coding is:

– For 2.0 definitions, the PU statement has IDBLK=...,IDNUM=....

– For 2.1 definitions, the PU statement has CPNAME=....

2 Port name in ASCII defined on the router and used by DSPU

3 SAP of DSPU (noncanonical, except for Ethernet)

6 MAC address of the DSPU (noncanonical, except for Ethernet MAC address, which is canonical)

7 DLSw appears to VTAM like a token ring DLC

11 LU coding

APPN Connection Network

When nodes are attached to a shared-access transport facility (SATF), any-to-any connectivity is possible. This any-to-any connectivity allows direct connections between any two nodes, eliminating routing through intermediate network nodes and the corresponding data traversing the SATF multiple times. To achieve this direct connectivity, however, TGs must be defined on each node for all the other possible partners.

Defining connections between all possible pairs of nodes attached to the SATF results in a large number of definitions (increasing on the order of the square of the number of nodes involved) and also a large number of topology database updates (TDUs) flowing in the APPN network. To alleviate these problems, APPN allows nodes to become members of a connection network to represent their attachment to an SATF. Session traffic between two nodes that have been defined as members of a connection network can be routed directly, without passing through a network node (achieves direct connectivity). To become a member of a connection network, an APPN node's port must be ″attached″ to a Connection Network by defining a connection network interface. When the port is defined, a Connection Network TG is created by the APPN component to identify the direct connection from the port to the SATF (i.e. the connection network). This TG is not a conventional TG as in the case of defined link stations, but rather represents the connection to the Connection Network in the topology database.

Note: TGs for end nodes are not contained in the network topology database, but are contained in the node's local topology database. TDUs do not flow through the network when a connection is established through a Connection Network or when an end node is made a member of a Connection Network.

Because the connectivity is represented by a TG from a given node to a Connection Network, normal topology and routing services (TRS) can be used for the network node server to calculate the direct path between any two nodes attached to the SATF (with TGs to the same Connection Network). DLC signaling information is returned from the destination node during the normal locate process to enable the origin node to establish a connection directly to the destination node.

Therefore, to achieve direct connectivity on an SATF, instead of each node on the SATF being defined (or connected) to each other, each node is connected to a Connection Network. The Connection Network is often visualized as a virtual node

on the SATF to which all other nodes are attached. This model is frequently used and, in fact, the term Virtual Routing Node (VRN) is often interchanged with the term Connection Network.

When a connection network is defined, it is named. This name then becomes the CP name of the VRN and must follow all the requirements of any CP name. See Table 36 on page 192 for a list of these requirements.

Restrictions

- The same connection network (VRN) can be defined on only one LAN. The same VRN can be defined on multiple ports having the same characteristics to the same LAN however.
- There is only one connection network TG from a given port to a given connection network's VRN.
- Because the VRN is not a real node, CP-CP sessions cannot be established with or through a VRN.
- When a connection network is defined on the router network node, a fully qualified name is specified for the *connection network name* parameter. Only connection networks with the same network ID as the router network node may be defined. The network ID of the VRN is then the same as the network ID of the router network node.

Branch Extender

The Branch Extender (BrNN) function is designed to optimize the connection of a branch office to an APPN WAN backbone network. The BrNN isolates all the end nodes on one or more branch office LANs from the backbone WAN. The domain of a BrNN may contain only end nodes and cascaded BrNNs. The domain of a BrNN does not contain network nodes or nodes with DLUR.

When configuring a BrNN, configure link stations to the backbone to be uplinks. This causes the BrNN to appear as a conventional end node to the backbone. From the perspective of the backbone, all resources in the domain of the BrNN appear to be owned by the BrNN, hiding the topology of the BrNN's domain from the backbone and reducing the number of broadcast locates in the backbone.

A BrNN presents a conventional network node interface over downlinks. End nodes in the domain of the BrNN register their resources with the BrNN and use the BrNN as a conventional network node server.

A BrNN accomplishes:

- Reduction of the number of network nodes in a large APPN network.
- Hidden branch office topology from the WAN.
- Direct, peer-to-peer communication between defined branches connected to the same connection network.
- Reduces CP-CP session traffic on the WAN link.

The following are limitations of Branch Extender:

- Network nodes are allowed to connect only over links that a BrNN defines as uplinks.
- Only end nodes or cascaded BrNNs may be attached to a BrNN downlink. Border nodes acting as end nodes and DLUR nodes may not be attached to a BrNN downlink.

- A node cannot connect to a Branch Extender over an uplink and a downlink at the same time.
- A BrNN can have CP-CP sessions with only one network node at a time.

Branch Extender vs. Extended Border Node

Both Branch Extender and Extended Border Nodes serve to minimize network topology. The choice of which to use depends upon the network.

A **branch extender** is the appropriate choice when you have a single network with one or more groups of end nodes where each group of end nodes typically needs to communicate with other end nodes in that group, and only occasionally need to interact with the backbone network.

None of the devices downstream from the branch extender may be network nodes, DLUR, VTAM, or VTAM end nodes.

With the branch extender in place the backbone network's view of the branch extender is as a giant end node with all the downstream LUs being owned by this giant end node. The backbone has no knowledge of the topology downstream from the branch extender, thus reducing the overhead of topology exchanges. Conversely, the branch extender's network node server, which is part of the backbone, will have knowledge of all the LUs owned by the branch extender if the branch extender is configured to register resources. This serves to reduce the number and size of broadcast searches and topology updates.

An **extended border node** is the appropriate choice when you have multiple networks you want to tie together, or when you have a large network you want to subdivide without restriction on what node types are allowed in the subdivided pieces. There is no concept of upstream or downstream and you can have additional extended border nodes, network nodes, end nodes, DLUR, VTAM, or VTAM end nodes located anywhere in your network. Unlike the branch extender, an extended border node cannot register resources with another network.

Managing a Network Node

The router network node can act as an APPN entry point that forwards APPN-related alerts to an APPN focal point. APPN focal points may be defined explicitly or implicitly.

You can use SNMP to access these IETF standardized MIBs:

- APPC (RFC 2051)
- APPN (RFC 2155)
- HPR (RFC 2238)
- DLUR (RFC 2232)

You can also use SNMP to access these enterprise-specific MIBs:

- IBM APPN Memory
- IBM Accounting
- IBM HPR NCL
- IBM HPR Route Test
- IBM Branch Extender Node
- IBM Extended Border Node (EBN)

Entry Point Capabilities for APPN-related Alerts

The router network node can serve as an APPN entry point for alerts related to the APPN protocol. As an entry point, the router is responsible for forwarding APPN and LU 6.2 generic alerts about itself and the resources in its domain to a *focal point* for centralized processing. A focal point is an entry point that provides centralized management and control for other entry points for one or more network management categories.

Note: If a focal point is not available to receive an alert from the device, the alert is held (stored) by the device.

Entry points that communicate with a focal point make up that focal point's *sphere of control*. If a focal point explicitly defines the entry points in its sphere of control and initiates communication with those entry points, it is an *explicit focal point*. If a focal point is designated by its entry points, which initiate communication with the focal point, the focal point is an *implicit focal point*. The focal point for the router can be either an explicit or implicit focal point.

Routers configured as branch extender nodes have additional flexibility. As with conventional network nodes, the focal point can directly establish an explicit relationship with the branch extender node. Also as with conventional network nodes, you can configure one or more implicit focal points at the branch extender node.

Unlike conventional network nodes, branch extender nodes can alternatively learn of the focal point from its network node server. When the network node server establishes a relationship with the focal point, either explicitly or implicitly, it will notify all its served end nodes, including served branch extender nodes, of the focal point name.

If the session between the router entry point and its primary focal point fails, the router can initiate a session with a designated backup focal point. Before initiating a session with a backup focal point, the router entry point makes an attempt to reestablish communication with its primary focal point if the router has been assigned session re-establishment responsibility. If that attempt fails, the router switches to the backup focal point.

Note: The router will attempt to establish a session with the backup focal point, or will attempt to re-establish the session with the primary focal point, only if the router has an alert to send.

After switching to a backup focal point, the router will periodically attempt to re-establish its session with the primary focal point. The interval between attempts is doubled each time an attempt fails until a maximum interval of one day is reached. From that point on, the attempt is performed daily.

Notes:

1. If the focal point is explicit and the explicit focal point retains the re-establishment responsibility for itself, this retry mechanism is disabled.
2. If the focal point is explicit and assigns re-establishment responsibility to the router, the router will attempt to reestablish communication until the next restart of APPN in the router.

The router entry point communicates with the focal point through an LU 6.2 session. Multiple-domain support (MDS) is the mechanism that controls the transport of

management services requests and data between these nodes. The router network node does *not* support SSCP-PU sessions with focal points.

Management processes within the router's control point are handled by its control point management services (CPMS) component. The CPMS component within the router network node collects unsolicited problem management data from resources within the router's domain and forwards this data to the appropriate focal point.

Supported Message Units

The router network node uses the following message units for sending and receiving management services data, including alert messages from domain ENs:

Message unit
Description

CP-MSU
Control point management services unit. This message unit is generated by CPMS and contains alert information forwarded by the router entry point. CPMS passes CP-MSU message units to MDS.

MDS-MU
Multiple-domain support message unit. This message unit is generated by MDS. It encapsulates the CP-MSU for transport between nodes.

SNMP Capabilities for APPN MIBs

An operator or application at an SNMP network management station can query objects in the APPN MIBs (using the SNMP **get** and **get_next** commands) to retrieve APPN status information and node statistics. A subset of APPN MIB objects can be modified using the SNMP **set** command. The APPN MIBs can be accessed only using SNMP.

Topology Database Garbage Collection

Information flows between APPN NNs to inform the NNs about network resources. Each NN keeps a topology database consisting of the names and characteristics of those resources. When a resource is eliminated from the network, it can also be deleted from each NN topology database. When a NN detects that a resource in its topology database is obsolete, the node will broadcast information stating that the resource should be garbage-collected. If NNs receiving this information support Enhanced Garbage Collection, they should delete that resource from their topology database. The record is not actually garbage-collected until the next garbage collection cycle. A NN examines each resource in its topology database once a day.

Configurable Held Alert Queue

The configurable held alert queue function allows you to configure the size of the held alert queue. If a focal point is not available, the held alert queue saves APPN alerts. When a focal point becomes available, the held alerts are sent. If more alerts arrive than can be held, the oldest alerts are discarded.

Note: If you configure a large value for the **Held Alert Queue Size**, the extra memory should be accounted for. You can do this by letting the tuning algorithm automatically calculate the **Maximum Shared Memory** value. See "APPN Node Tuning" on page 119 for additional information about the node tuning algorithm.

Implicit Focal Point

A focal point is a node with centralized management responsibility. The managing node can contact the managed node (router) and establish a management session. The managing node is then an explicit focal point. When the name of the managing node is configured at the router and the router can initiate a management session, the managing node is an implicit focal point. You can configure a single, primary implicit focal point with up to eight backup implicit focal points, where each focal point is a fully qualified network name. The router will attempt to contact each focal point in order until a successful management session is established.

If the management session is with a backup implicit focal point, the device will periodically attempt to reestablish its session with the primary implicit focal point. The interval between attempts is doubled each time an attempt fails until a maximum interval of one day is reached. From that point on, the attempt is performed daily.

Note: If an explicit focal point initiates a management session with a device, it will cause a session with an implicit focal point to terminate.

Enterprise Extender Support for HPR over IP

Enterprise Extender support for HPR over IP allows HPR/APPN applications to run over an IP backbone network and still take advantage of APPN Class of Service. HPR over IP encapsulates HPR data into a UDP/IP packet for delivery over the IP network.

Supported DLCs

Table 15 shows the DLC ports supported by the device over APPN:

Table 15. Port Types Supported for APPN Routing

Port Type	Standard	HPR	ISR	DLUR*
DLSw (remote only) ***		No	Yes	Yes
LANE	Forum compliant	Yes	Yes	Yes
ATM		Yes	No	Yes
FDDI		Yes	Yes	Yes
HPR over IP		Yes	No	Yes
100Mbps TR	802.5	Yes	Yes	Yes

Notes:

1. * This column refers to the port providing the connection to the downstream PU (DSPU).

Router Configuration Process

This section describes the router configuration process and includes details about parameters.

Configuration Changes That Require the APPN Function to Restart

- Network ID of the network node
- Control point name of the network node
- XID number (of network node) for subarea connection
- Adjacent node type (of link station)
- Any parameters under the following options:
  - High-Performance Routing (HPR) at the node level
  - Dependent LU Requester (DLUR) at the node level
  - Connection network
  - Class of service
  - Node tuning
  - Node management
  - Focal points
  - Mode name mappings

Configuration Requirements for APPN

APPN routing is configured on the individual adapters supporting the DLC desired. To use APPN routing, at least one of the following DLCs must be configured and enabled:

- Token-ring emulated LAN ports
- Ethernet emulated LAN ports

The `talk 6` code required to configure APPN or TN3270 resides on the corresponding DLL, and that DLL is not loaded unless you have enabled the corresponding function. If you use the Configuration Program to configure the device, this will be taken care of automatically. If you use `talk 6` commands to configure the device, you must issue one or both of the following commands and then reboot prior to being able to invoke the `talk 6` APPN or TN3270 commands:

- `Config>` **load add package appn**
- `Config>` **load add package tn3270**

Configuring the Router as an APPN Network Node

You can configure the router as an APPN network node in one of three ways, depending on the level of connectivity you desire with other nodes.

- Minimum configuration
- Initiate connections configuration
- Controlling connections configuration

Minimum Configuration

This group of APPN configuration steps:

- Allows the network node to accept any request it receives from another node to establish a connection.
- Restricts the network node from initiating connections with other nodes.

If you choose the minimum configuration steps, adjacent nodes must define connections to the router network node to ensure connectivity. Because APPN nodes can initiate CP-CP sessions with the router network node, these nodes do

not need to be defined in the router's configuration. In general, when configuring APPN on the router, you can simplify the task considerably by allowing the router network node to accept connection requests from any node. Configuring the network node in this manner eliminates the need to define information about adjacent nodes, except in the following cases:

- The adjacent node is a LEN end node. LEN end nodes do not support CP-CP sessions, so information about such nodes and their LU resources must be configured on the router network node.
- You want the router network node to be able to initiate a CP-CP session with an adjacent APPN node.

In these cases, you must specify information about the adjacent node when enabling APPN routing on the specific port you are using to connect to the adjacent node, and should follow the configuration steps described in "Initiate Connections Configuration".

Use the following procedure for minimum configuration steps:

1. If you are configuring APPN using a DLSw port:
   a. Enable bridging on the node
   b. Enable DLSw on the node
   c. Define the DLSw port with a locally administered MAC address for DLSw.
2. Enable APPN routing on the port.

   Note: Since *Service Any* is enabled by default, the node accepts any request for a connection that it receives from another node.
3. Enable the APPN Network Node.
4. Configure the following parameters:
   - Network ID
   - Control point name
5. Define the XID number for subarea connections parameter for the APPN network node (optional).
6. Accept all other defaults.
7. Optionally do the following:
   - Modify High-Performance Routing parameters
   - Configure Dependent LU Requester
   - Define connection networks
   - Define new COS names or mode name mappings
   - Tune the performance of this node
   - Perform node service trace diagnostics
   - Collect statistics for this network node

Notes:

1. APPN routing must be defined and enabled on the specific ports you configure the router network node to use.
2. Bridging and DLSw must still be enabled on the specific adapter ports you desire the device network node to use.

Initiate Connections Configuration

This group of APPN configuration steps:

- Allows the network node to accept any request it receives from another node to establish a connection.
- Enables the network node to initiate connections with other nodes that you specify, including LEN end nodes.

Because APPN nodes can initiate CP-CP sessions with the router network node, these nodes do not need to be defined in the router's configuration, except in the following cases:

- The adjacent node is a LEN end node. LEN end nodes do not support CP-CP sessions, so information about such nodes and their LU resources must be configured on the router network node.
- You want the router network node to be able to initiate a CP-CP session with an adjacent APPN node.

If neither of these cases apply to your configuration, you should follow the configuration steps described in "Minimum Configuration" on page 112.

Use the following procedure for initiate connections configuration :

1. If you are configuring APPN using a DLSw port:
   a. Enable bridging on the node
   b. Enable DLSw on the node
   c. Define the DLSw port with a locally administered MAC address for DLSw.
2. Select the ports over which to initiate connections to adjacent nodes. The following are the DLC port types supported by APPN:
   - DLSw
   - Emulated token-ring LAN port
   - Emulated Ethernet LAN port
   - FDDI
3. Enable APPN routing on APPN ports with the *enable APPN routing on this port* parameter.

   Note: Since *Service Any* is enabled by default, the node accepts any request for a connection that it receives from another node.
4. Define APPN link stations on the selected DLC ports for the adjacent nodes to which this network node may initiate a connection.

   Note: Link stations do not have to be defined on every port, only those over which you want to initiate connections to adjacent nodes.
5. Enable the APPN network node.
6. Configure the following parameters for the APPN network node:
   - Network ID
   - Control point name
7. Define the XID number for subarea connections parameter for the APPN network node (optional).
8. Accept all other defaults
9. Optionally do the following:
   - Modify High-Performance Routing parameters
   - Configure Dependent LU Requester
   - Define connection networks

- Define new COS names or mode name mappings
- Tune the performance of this node
- Perform node service trace diagnostics
- Collect statistics for this network node

Controlling Connections Configuration

This group of APPN configuration steps:

- Allows the network node to accept requests only from nodes that you specify.
- Enables the network node to initiate connections with other nodes that you specify, including LEN end nodes.

This configuration provides a higher level of security because you explicitly define which APPN nodes may communicate with this router network node. A connection request from an adjacent node will be accepted only if its fully qualified CP name parameter has been configured on this network node. This group of configuration steps optionally enables you to have a secure link with each adjacent node by configuring the session level security feature for each link.

Use the following procedure for the controlling connections configuration:

1. Select ports over which you desire to establish connections to adjacent nodes from the following DLC port types supported by APPN:
   - Emulated token-ring LAN port
   - Emulated Ethernet LAN port
   - IP
2. Define ports selected as direct APPN ports with the following parameters:
   - Enable *APPN routing* on this port
   - Disable the *service any port* parameter
3. If you are configuring APPN using a DLSw port:
   - Enable bridging on the node
   - Enable DLSw on the node.
   - Define the DLSw ports with the following parameter:
     - Define a locally administered MAC address for DLSw
     - Disable the *Service any* node parameter
4. Enable APPN routing on the port.
5. Define APPN link stations on the selected DLC ports for the adjacent nodes:
   - that may initiate a connection to this network node.
   - which you desire this router network node to initiate a connection.

   Specify the following link station parameters:
   - Fully Qualified CP name of adjacent node (required)
   - Any required addressing parameters for adjacent node
   - And optionally:

     CP-CP Session Level Security

     Security Encryption Key
6. Enable the APPN network node.
7. Configure the following parameters for the APPN network node:
   - Network ID
   - Control point name

8. Define the XID number for subarea connections parameter for the APPN network node (optional):
9. Accept all other defaults.
10. (Optional) Configure the following router network node options:
    - Modify High-Performance Routing parameters
    - Configure Dependent LU Requester
    - Define connection networks
    - Define new COS names or mode name mappings
    - Tune the performance of this node
    - Perform node service trace diagnostics
    - Collect statistics for this network node

Configuring Branch Extender

To configure Branch Extender, set the following configuration parameters as appropriate for your network.

1. Use the **set node** command to:
    a. Answer 1 for Branch Extender to the *Enable Branch Extender or Border Node* question. If you answer 0, none of the following Branch Extender questions will appear.
    b. Answer yes or no to the *Permit search for unregistered LUs* question depending on whether or not you want to allow searches from the backbone for LUs that were not registered with the network node server.
    c. Your answer to the *Branch uplink* question will determine the default for the analogous link level question.
2. Use the **add link** command to:
    a. Answer yes to the *Branch uplink* question if you want the router to appear as an end node on this link. An end node is for links to network nodes in the backbone. Note that this question doesn't appear and is forced to yes if you have defined the adjacent link station to be a network node on one of the earlier configuration prompts. Answer no if you want the router to appear as a network node on this link. A network node is for links to end nodes
    b. The *Is uplink to another Branch Extender node* question is asked only if this link has been defined as a limited resource and has also been defined as a Branch Extender uplink. Answer yes if the adjacent node is another Branch Extender.
    c. The *Preferred network node server* question is asked only if the adjacent node is a network node and CP-CP sessions are supported on this link. Since you can only have a single preferred network node server you won't be prompted for this question once it has been set to yes on any link.

High-Performance Routing

See "Configuration Requirements for APPN" on page 112 for information about configuring the protocols that support APPN and HPR routing on the router. In the case of HPR parameters such as retry and path switch timers, the configuration is done at the node level and is not specified on individual adapters.

DLUR

See Table 15 on page 111 for a list of ports that support DLUR.

Configuring Focal Points

Focal points can be explicit or implicit. Explicit focal points are configured at the focal point itself. No configuration at the router is required.

Implicit focal points on the other hand are configured at the router. You configure them with the command **add focal_point**. Add the primary implicit focal point first. If you add another focal point, it is known as the first backup implicit focal point. If you add yet another, it is known as the second backup implicit focal point. Up to eight backup implicit focal points may be added for a total of 9.

To delete a focal point use the command **delete focal_point**. You will be prompted for the name of the focal point to delete. When the name is deleted, the remaining focal points retain their relative position with each other. Subsequent focal points will be added at the end of the list.

There is no way to insert a focal point in the middle of the list. You must delete them one at a time and then re-enter the entire list.

Configuring Held Alert Queue Size

To configure the size of the held alert queue enter the command **set management** and answer the ***Held Alert Queue Size*** question. The queue defaults to a size of 10 alerts, and valid values are from 0 through 255 alerts.

As you increase the size of the held alert queue, additional memory is needed. If you set it to a high value, you may want to adjust the ″Maximum Shared Memory″ value. See“APPN Node Tuning” on page 119 for additional information.

Defining Transmission Group (TG) Characteristics

When you configure APPN on the router, you can specify the Transmission Group (TG) characteristics for the link station that defines a connection between the router network node and an adjacent node. These characteristics, such as the security of a link or its effective capacity, are used by APPN when calculating an optimum or least-weight route between nodes in the APPN network.

APPN on the router uses a set of default TG characteristics for each port (or DLSw port). These defaults, defined by the *default TG characteristics* parameter apply to all the TGs for link stations defined on a port unless they are overridden for a particular link station by the *modify TG characteristics* parameter.

These default TG characteristics are also used for dynamic link stations established when an adjacent node requests a connection with the router network node, but does not have a predefined link station definition on the router network node. The *Service any node* parameter must be enabled.

You can change the following parameters using the router **talk 6>** interface as well as the Configuration Program:

time cost

byte cost
user-defined TG characteristics 1 - 3
effective capacity
propagation delay
security

Calculating APPN Routes Using TG Characteristics

The APPN route calculation function uses a COS definition for TGs which is a table containing rows of TG characteristic ranges. Each row defines a given range for each of the eight TG characteristics and the corresponding TG weight for that row. APPN starts at the top of the table and continues down the table until all eight of the TG characteristic parameter values fit within the ranges given for that row. APPN then assigns the weight of that row as the TG weight for that link. There is also a COS definition for nodes that calculates a node's weight. The route calculation function continues until it has found the path with the least combined weight of TGs and nodes. This is the least weight route.

As an example of how TG characteristics are used to influence the selection of a route through an APPN network node, suppose that a route from network node router A to network node router D can pass through either network node router B or router C. In this example, router A defines connections to both router B and router C. However, the connection from router A to router B is a 64-Kbps link, while the connection from router A to router C is a slower-speed 19.2-Kbps link.

To ensure that the higher-speed connection from router A to router B is viewed as the more desirable path for routing APPN interactive traffic, the effective capacity TG characteristic for the link station associated with this path would be modified. In this case, the default value for effective capacity is X'38', which correctly represents a link speed of approximately 19.2-Kbps. However, the effective capacity would be changed to X'45' to properly represent the 64-Kbps link. Since the effective capacity for the TG from router A to router B is now X'45', this path is assigned a lower weight in the COS file for interactive traffic. Consequently, the connection from router A to router B is represented as more desirable than the connection from router A to router C.

You can also change the TG characteristics if you purposefully want to favor certain TGs for route selection. In addition to the five architected TG characteristics, there are also three user-defined TG characteristics. You may define these user-defined TG characteristics in order to bias the route selection calculation in favor of certain paths.

Note: For DLSw ports the TG characteristics that you define effect only the selection of routes between APPN nodes over these DLSw ports. These characteristics have no direct effect on any intermediate routing performed by DLSw on APPN's behalf.

COS Options

You can use a template to create new user-defined COS names and associated definitions for TGs and nodes which can be used with new mode names or mapped to existing mode names.

In addition you can create new mode names that can be mapped to existing COS names.

Each COS definition file is identified by a COS name and contains an associated transmission priority and a table of ranges of acceptable TG and node characteristics that APPN compares against actual TG and node characteristics to determine weights for TGs and nodes from which APPN calculates the least weight route for the session. Using the Configuration Program you can:

- View a COS definition file:
  - View the transmission priority
  - View a list of node row references along with their corresponding weights
  - View a list of TG row references along with their corresponding weights
- Select standard or ATM COS tables as templates to define a new user-defined COS definition file with a new COS name:
  - Import an IBM-defined COS definition file to use as a template
  - Import a previously exported user-defined COS definition file to use as a template
- Define the minimum and maximum ranges for the user-defined TG characteristics within an IBM-defined COS definition.

  Note: In an IBM-defined COS definition you can edit only the user-defined TG characteristic ranges.

Using Configuration Program or **talk 6** you can:

- Use standard COS tables or the Enhanced COS tables (for ATM).
- Define a new mode name and its mapping to a COS name.
- Change a mode name to COS name mapping:
  - Re-map an IBM-defined mode name to a different COS name.
  - Re-map a previously specified user-defined mode name to a different COS name.

Refer to the discussion of Topology and Routing Services in the *SNA APPN Architecture Reference*, SC30–3422, for a description of standard and ATM COS tables.

APPN Node Tuning

The performance of the router APPN network node can be tuned in two ways:

- By manually setting the values of the *maximum shared memory*, *percent of APPN shared memory to be used for buffers*, and the *maximum cached directory entries* tuning parameters using the **talk 6** option of the command line interface.
- By selecting values for the *maximum number of ISR sessions*, *maximum number of adjacent nodes* and other parameters shown in Table 21 on page 143, and having the tuning algorithm automatically calculate the *maximum shared memory* and *maximum cached directory entries* tuning parameter values.

  Use the IBM 8210 Multiprotocol Switched Services Server Configuration Program to invoke the tuning algorithm.

The *maximum shared memory* parameter affects the amount of storage available to the APPN network node for network operations. For example, you can allow APPN to have a 4K RU size by setting *maximum shared memory* to at least 1 Megabyte

and setting *percent of APPN shared memory used for buffers* to a sufficiently large value to allow at least 1 Megabyte of memory to be available to the buffer manager.

The *maximum cached directory entries* parameter affects the amount of directory information that will be stored or cached to reduce the time it takes to locate a resource in the network.

In general, tuning the APPN network node involves a trade-off between node performance and storage usage. The better the performance, the more storage required.

Tuning Notes

1. The tuning parameter settings should reflect anticipated growth in your network.
2. If you define connection networks within your APPN network and you anticipate that most end nodes will initiate LU-LU sessions with other end nodes on the same connection network, you should set the *maximum number ISR sessions* parameter to a smaller value (1). Using connection networks in this manner reduces the shared memory requirements for the router network node because most LU-LU sessions will not flow through the APPN component in the router.
3. Because the *maximum shared memory* parameter affects storage allocation within the router, you should use care when explicitly defining this parameter. Use the defaults as a guide when increasing or reducing maximum shared memory manually.

Node Service (Traces)

The APPN Node Service (Traces) option allows you to start any APPN trace through **talk 6** or the Configuration Program. The traces are activated when the configuration file is applied to the router. The traces will continue to be active until they are stopped when a new configuration that stops the traces is applied to the router.

Note: Running traces on the router can affect its performance. Traces should be started only when needed for node service and should be stopped as soon as the required amount of trace information is gathered.

The APPN traces are grouped into the following 5 categories:

- Node-level traces specify traces concerning the overall APPN network node.
- Inter-process signals traces specify component-level traces concerning signals between APPN components.
- Module entry and exit traces specify component-level traces concerning the entry and exit of APPN modules.
- General traces specify component-level traces concerning the APPN components.
- Miscellaneous traces specify trace information about DLC transmissions and receptions.

APPN Trace Enhancements

The following are enhancements to the APPN traces:

- You can now enable/disable all trace flags through `talk 6` using the *Turn all trace flags off* question asked under the **set trace** command or by using the Configuration Program. See 167 for more information.

- You can now filter the data link control transmissions and receptions trace data by either message type or by specifying the maximum length of data per packet to trace. See Table 27 on page 165 for information.

Accounting and Node Statistics

Intermediate sessions are LU-LU sessions that pass through the APPN network node, but whose endpoints (origin and destination) lie outside of the network node. Information about intermediate sessions is generated by the ISR component in the network node and falls into two categories:

- Intermediate session names and counters
- Route selection control vector (RSCV) data for intermediate sessions

Enabling the *collect intermediate session information* parameter instructs the router to collect session names and counters for all active intermediate sessions. Enabling the *save RSCV information for intermediate sessions* parameter instructs the router to collect RSCV data for active intermediate sessions. The RSCV data is useful for monitoring session routes. In both cases, you can retrieve the data on active sessions by issuing SNMP **get** and **get-next** commands for variables in the APPN Management Information Base (MIB).

The *collect intermediate session information* function defaults to being disabled. You can enable it using the Configuration Program or using the **set management** `talk 6` command. Once enabled, you can control it, including disabling and re-enabling, using SNMP **set** commands to the APPN accounting MIB.

Note: This function can use a significant amount of APPN memory. You should configure APPN with the needed memory before you enable the collection of ISR information.

For accounting purposes, you can maintain records of intermediate sessions passing through the network node. The data records can be created and stored in router memory. SNMP must be used to retrieve data from accounting records stored in the router's local memory.

Notes:

1. You can enable collection of active intermediate session data (session counters and session characteristics) in SNMP MIB variables explicitly or implicitly.

   To enable collection explicitly, set the *collect intermediate session information* parameter to yes.

   To enable collection implicitly, set *create intermediate session records* to yes. This setting will override the setting of *collect intermediate session information*.
2. Configuration changes to the APPN accounting parameters made using the **talk 6** interface will not take effect until the router or the APPN function on the router is restarted. You can make changes interactively, however, by issuing SNMP **set** commands to modify the APPN MIB variables associated with the configuration parameters. Refer to the *Multiprotocol Switched Services (MSS) Interface Configuration and Software User's Guide* for a list of these MIB variables.
3. Data on intermediate session RSCVs is obtained by examining the BIND request used to activate a session between two LUs. RSCV data is not collected for sessions that have already been established because the BIND information for those sessions is not available.

4. Intermediate session data is not collected for HPR sessions since intermediate sessions are not part of HPR. If the router contains an ISR/HPR boundary, intermediate session data is collected when it flows across that boundary.

DLUR Retry Algorithm

If communication between DLUR and DLUS is broken, the following algorithm is used to reestablish communication:

If *Perform retries to restore disrupted pipe* is No:

- If DLUR receives a non-disruptive UNBIND (sense code of X'08A0 000A'), DLUR waits indefinitely for a DLUS to reestablish the broken pipe.
- If the pipe fails for any other reason than a non-disruptive UNBIND, DLUR attempts to reach the primary DLUS once. If this is unsuccessful, DLUR attempts to reach the backup DLUS. If DLUR is unable to reach the backup DLUS, it waits indefinitely for a DLUS to reestablish the broken pipe.

If *Perform retries to restore disrupted pipe* is Yes, DLUR will attempt to reestablish the pipe based on the following configuration parameters:

- Delay before initiating retries
- Perform short retries to restore disrupted pipe
- Short retry timer
- Short retry count
- Perform long retries to restore disrupted pipe
- Long retry timer

There are two cases that determine the retry algorithm:

- For the case of receiving a non-disruptive UNBIND:
  1. Wait for the amount of time specified by the *Delay before initiating retries* parameter. This delay allows time for an SSCP takeover, where the pipe would be reestablished by a new DLUS without action on the DLUR's part.
  2. Attempt to reach the primary DLUS.
  3. If unsuccessful, attempt to reach the backup DLUS.
  4. If the attempt to reach the backup DLUS is unsuccessful, DLUR will retry as described in steps 5 - 7 as long as the DSPU is requesting ACTPU.
  5. Wait for the amount of time specified by the *Long retry timer*.

     Note: If *Perform long retries to restore disrupted pipe* is No, no further retries will be attempted.
  6. Attempt to reach the primary DLUS.
  7. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS.

  Example:

  – Assume the following parameter values:
    - *Delay before initiating retries* = 120 sec
    - *Perform short retries to restore disrupted pipe* = yes
    - *Short retry timer* = 60 sec
    - *Short retry count* = 2
    - *Perform long retries to restore disrupted pipe* = yes

- *Long retry timer* = 300 sec

– Pipe activation fails.
– Wait 120 seconds (the value of *Delay before initiating retries*).
– Retry the primary DLUS and, if this fails, retry the backup DLUS.
– If retry fails, wait 300 seconds (the value of *Long retry timer*), retry the primary DLUS,and if this retry fails, retry the backup DLUS.
– If retries fail, continue to retry the primary and backup DLUS, waiting 300 seconds between retry sequences, for as long as the DSPU is requesting ACTPU.

- For all other cases of pipe failure, DLUR will try the primary DLUS and then the backup DLUS immediately. If this fails, DLUR will:
  1. Wait for the amount of time specified by the minimum of the *short retry timer* and the *Delay before initiating retries* parameters.
  2. Attempt to reach the primary DLUS.
  3. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS
  4. If pipe activation continues to fail, DLUR will retry as described in steps 1 - 3 for the number of times specified in the *short retry count*.

     If the *short retry count* is exhausted, DLUR will retry as defined in steps 5 - 7 as long as the DSPU is requesting ACTPU.
  5. Wait for the amount of time specified by the *Long retry timer*

     Note: If *Perform long retries to restore disrupted pipe* is No, no further retries will be attempted.
  6. Attempt to reach the primary DLUS.
  7. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS.

  Example:

  – Assume the following parameter values:
    - *Delay before initiating retries* = 120 sec
    - *Perform short retries to restore disrupted pipe* = yes
    - *Short retry timer* = 60 sec
    - *Short retry count* = 2
    - *Perform long retries to restore disrupted pipe* = yes
    - *Long retry timer* = 300 sec
  – Pipe activation fails.
  – Retry the primary and backup DLUS immediately.
  – If this retry fails, wait 60 seconds (the value of *Short retry timer*).
  – Retry the primary DLUS. If this retry fails, retry the backup DLUS. This is attempt #1 of the *Short retry count*.
  – If this fails, wait 60 seconds (the value of *Short retry timer*).
  – Retry the primary DLUS, and then the backup DLUS. This is attempt #2 *Short retry count*. *Short retry count* is now exhausted.
  – If the retry still fails, wait 300 seconds (the value of *Long retry timer*). Then retry the primary DLUS. If this retry attempt fails, retry the backup DLUS.
  – As long as the retry fails, continue to retry the primary and the backup DLUS, waiting 300 seconds between retry sequences, for as long as the DSPU is requesting ACTPU.

APPN Implementation on the Router Using DLSw

The router also supports APPN over DLSw for connectivity to nodes through a remote DLSw partner. An example is shown in Figure 7. This support allows customers with DLSw configurations to migrate their networks to 8210.

Note: It is recommended to use APPN over direct DLCs when available instead of APPN over DLSw.

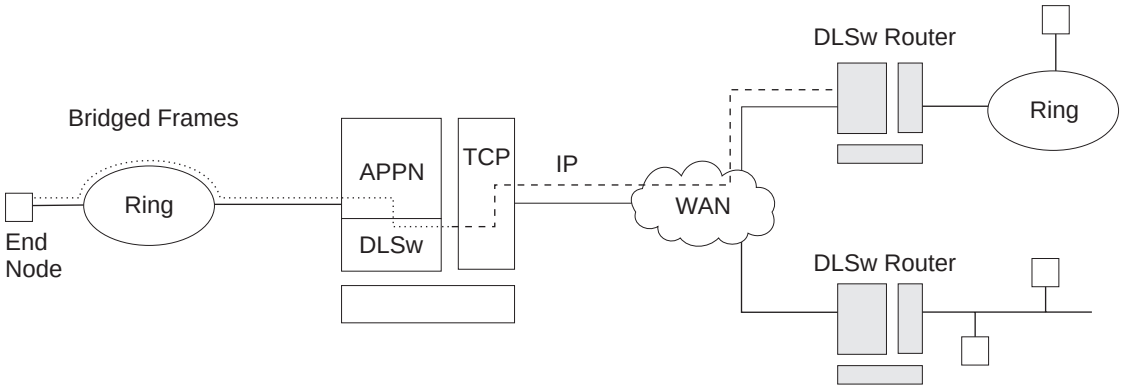

Figure 7. Data Flow in an APPN Configuration Using DLSw Port

APPN configuration restrictions using DLSw:

- Connectivity through remote DLSw partners only
- Only 1 DLSw port per router
- Use of a locally administered MAC address
- HPR is not supported on DLSw ports
- DLSw ports cannot be members of connection networks
- Parallel TGs are not supported on DLSw ports

See “Configuring the Router as an APPN Network Node” on page 112 to configure APPN using DLSw.

How APPN Uses DLSw ports to Transport Data

When APPN is configured on the router to use Data Link Switching (DLSw) port, DLSw is used to provide a connection-oriented interface (802.2 LLC type 2) between the APPN component in the router and APPN nodes and LEN end nodes attached to a remote DLSw partner.

When configuring a DLSw port for APPN on the router, you assign the network node a unique MAC and SAP address pair that enables it to communicate with DLSw. The MAC address for the network node is locally administered and must not correspond to any physical MAC address in the DLSw network.

Port Level Parameter Lists

Use the following tables to configure APPN ports:

- “Port Configuration” on page 171
- “Port Definition” on page 179

Link Level Parameter Lists

Use the following tables to configure APPN link stations:

LU Parameter List

Use the following table to configure an LU:

Node Level Parameter Lists

Use the following tables to configure an APPN node:

APPN Configuration Notes

The following examples show special parameters to consider when configuring various features to transport APPN traffic.

Note: These examples show sample output. The output you see may not appear exactly like the output shown here.

Note: In some configuration examples, the results of a **talk 6 list** command may show more configuration than is actually presented in the sample. However, the sample will show all of the configuration that is unique.

Configuring APPN Over ATM

The following sample configures APPN over ATM.

Notes:

1. When PVCs are configured, the link station must be defined on both APPN nodes wanting to use the PVC. The link station must be defined with **Activate link automatically**= yes.
2. When parallel TGs over ATM are configured, the adjacent node name and TG number must be defined in both nodes for each link station.

```
add po
APPN Port
Link Type:  (E)THERNET, (T)OKEN RING,
 (D)LSw,(A)TM, (IP) [ ]?atm 1
Interface number(Default 0): [0]?6
Port name (Max 8 characters) [ATM006]?

WARNING!! You are changing an existing record.
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Maximum BTU size (768-2048) [2048]?
        Maximum number of link stations (1-976) [512]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local ATM Address (hex) [99998888777766]?
        Local SAP address (04-EC) [4]?
        Enable Incoming Calls (Y)es (N)o [N]?
        ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        Shareable Connection Network Traffic (Y)es (N)o [N]?
        Shareable Other Protocol Traffic (Y)es (N)o [N]?
        Broadband Bearer Class: 0 = CLASS_A, 1 = CLASS_C, 2 = CLASS_X [2]?
        Best Effort Indicator (Y)es (N)o [N]?
        Forward Traffic Peak Cell Rate (1-16777215) [131750]?
        Forward Traffic Sustained Cell Rate (1-16777215) [131750]?
        Forward Traffic Tagging (Y)es (N)o [Y]?
        Forward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
         3 = CLASS_3, 4 = CLASS_4 [0]?
        Backward Traffic Peak Cell Rate (1-16777215) [460800]?
        Backward Traffic Sustained Cell Rate (1-16777215) [39168]?
        Backward Traffic Tagging (Y)es (N)o [Y]?
        Backward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
         3 = CLASS_3, 4 = CLASS_4 [0]?
        Call out anonymously (Y)es (N)o [N]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [1]?
        Limited resource timer for HPR(1-2160000 seconds) [180]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.


nada205 APPN config>add li atm006 2
APPN Station
Station name (Max 8 characters) [ ]? tograya
WARNING!! You are changing an existing record.
        Limited resource: (Y)es (N)o [N]?
        Activate link automatically (Y)es (N)o [Y]?
        Virtual Channel Type (0 = PVC , 1 = SVC) [0]? 3
        Destination ATM Address  [39999999999999000099990101031689022594l1]?
        VPI (0-255) [0]?
        VCI (0-65535) [70]? 34
        ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        Shareable Connection Network Traffic (Y)es (N)o [N]?
        Shareable Other Protocol Traffic (Y)es (N)o [N]?
        Remote SAP(04-EC) [4]?
        Adjacent node type: 0 = APPN network node,
```

```
        1 = APPN end node or Unknown node type,
        2 = LEN end node [0]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [1]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.



nada205 APPN config>add link atm006
APPN Station
Station name (Max 8 characters) [ ]?tograya
WARNING!! You are changing an existing record.
        Limited resource: (Y)es (N)o [N]?
        Activate link automatically (Y)es (N)o [Y]?
        Virtual Channel Type (0 = PVC , 1 = SVC) [0]? 1
        Destination ATM Address  [39999999999999900009999010103168902259411]?
        Broadband Bearer Class: 0 = CLASS_A, 1 = CLASS_C, 2 = CLASS_X [2]?
        Best Effort Indicator (Y)es (N)o [N]?
        Forward Traffic Peak Cell Rate (1-16777215) [30000]?
        Forward Traffic Sustained Cell Rate (1-16777215) [20000]?
        Forward Traffic Tagging (Y)es (N)o [Y]?
        Forward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
         3 = CLASS_3, 4 = CLASS_4 [0]?
        Backward Traffic Peak Cell Rate (1-16777215) [30000]?
        Backward Traffic Sustained Cell Rate (1-16777215) [20000]?
        Backward Traffic Tagging (Y)es (N)o [Y]?
        Backward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
         3 = CLASS_3, 4 = CLASS_4 [0]?
        Call out anonymously (Y)es (N)o [N]?
        ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        Shareable Connection Network Traffic (Y)es (N)o [N]?
        Shareable Other Protocol Traffic (Y)es (N)o [N]?
        Remote SAP(04-EC) [4]?
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type,
        2 = LEN end node [0]?
        TG Number (0-20) [0]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [1]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.


nada205 APPN config>
```

Notes:

1. Define an APPN port with link type ATM
2. Define an APPN link station
3. Define a PVC
4. Define an SVC

Configuring Enterprise Extender Support for HPR Over IP

```
t 6
Q45 Config>p appn
APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (I)P  [ ]? ip
Port name (Max 8 characters) [IP255]?
```

```
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o [Y]?
Maximum BTU size (768-2048) [768]?
UDP port number for XID exchange (1024-65535) [11000]?
UDP port number for low priority traffic (1024-65535) [11004]?
UDP port number for medium priority traffic (1024-65535) [11003]?
UDP port number for high priority traffic (1024-65535) [11002]?
UDP port number for network priority traffic (1024-65535) [11001]?
IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
Local SAP address (04-EC) [4]?
LDLC Retry Count(1-255) [3]?
LDLC Timer Period(1-255 seconds) [15]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
****3.3.3.3 is the router's internal IP address
APPN config>add link
APPN Station
Port name for the link station [ ]? ip255
Station name (Max 8 characters) [ ]? tonn
Activate link automatically (Y)es (N)o [Y]?
IP address of adjacent node  [0.0.0.0]? 3.3.3.3
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type  [0]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Remote SAP(04-EC) [4]?
IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
LDLC Retry Count(1-255) [3]?
LDLC Timer Period(1-255 seconds) [15]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>
```

Configuring Connection Networks over HPR over IP

```
t 6
Config>p appn
APPN config>add connection network
Fully-qualified connection network name (netID.CNname) [ ]? supernet.cn1
Port Type: (E)thernet, (T)okenRing, (FR), (A)TM, (FD)DI, (I)P [ ]? ip
Limited resource timer for HPR (1-2160000 seconds) [180]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>add additional port
APPN Connection Networks Port Interface
Fully-qualified connection network name (CPname.CNname) [ ]? supernet.cn1
Port name [ ]? "en000"
Write this record? [Y]?
The record has been written.
```

Chapter 11. Configuring and Monitoring APPN

This chapter describes the APPN configuration and monitoring commands. It includes the following sections:

- "APPN Configuration Command Summary"
- "APPN Configuration Command Detail" on page 130

Accessing the APPN Configuration Process

Use the following procedure to access the APPN *configuration* process.

1. At the * prompt, enter **talk 6**. The `Config>` prompt is displayed.
   (If this prompt is not displayed, press **Return** again.)
2. Enter **protocol appn**. The `APPN Config>` prompt is displayed.
3. Enter an APPN configuration command.

APPN Configuration Command Summary

Table 16. APPN Configuration Command Summary

Command	Function	See page:
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page xxi.	
Enable/Disable	Enables/disables the following:	130
	APPN	
	Dependent LU Requestor	
	Port *port name*	
Set	Sets the following:	
	Node	131
	Traces	148
	HPR	135
	DLUR	139
	Management	167
	Tuning	143
Add	Adds or updates the following:	
	Port *port name*	171
	Link-station *link station name*	192
	LU-Name *LU name*	213
	Connection-network *connection network name*	214
	Additional-port-to-connection-network	225
	Mode	223
	Focal_point	226
	local-pu	226

Table 16. APPN Configuration Command Summary (continued)

Command	Function	See page:
Delete	Deletes the following: • Port *port name* • Link-station *link station name* • LU-Name *LU name* • Connection-network *connection network name* • Connection networks port interface (CN PORTIF) *CN name* • Mode *mode name* • Focal_point • local-pu	227
List	Lists the following from configuration memory: • All • Node • Traces • Management • HPR • DLUR • Port *port name* • Link-station *link name* • LU-Name *LU name* • Mode *mode name* • Connection-network *connection network name* • Focal_point	228
Activate_new_config	Reads the configuration into non-volatile configuration memory.	228
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxii.	

Note: APPN will respond to a dynamic **reset** command at the interface level.

APPN Configuration Command Detail

Enable/Disable

Use the **enable/disable** command to enable (or disable):

Syntax:

enable appn

[or disable] dlur

port *port name*

Set

Use the **set** command to set:

Syntax:

set node

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 17. Configuration Parameter List - APPN Routing

Parameter Information
Parameter Enable APPN **Valid Values** Yes, No **Default Value** Yes **Description** This parameter enables or disables the router as an APPN network node. This parameter enables both APPN and HPR routing capability for this network node which consists of defining the Network ID and CP name for this node. APPN, however, must be enabled on the particular ports on which you desire to support APPN routing. Additionally, support for HPR must be enabled on the particular APPN ports desired and must be supported by the particular link stations on those ports. **Note:** HPR only supported on LAN.
Parameter Network ID (required) **Valid Values** A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** A network identifier for an existing network, of which this router network node is to become a member, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new network IDs. **Default Value** None **Description** This parameter specifies the name of the APPN network to which this network node belongs. The network ID must be the same for all network nodes in the APPN network. Attached APPN end nodes and LEN end nodes can have different network IDs.

Table 17. Configuration Parameter List - APPN Routing (continued)

Parameter Information
Parameter Control point name (required) **Valid Values** A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing CP name that this node would be acquiring, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names. **Default** None **Description** This parameter specifies the name of the CP for this APPN network node. The CP is responsible for managing the APPN network node and its resources. The CP name is the logical name of the APPN network node in the network. The CP name must be unique within the APPN network identified by the Network ID parameter.
Parameter Enable Branch Extender **Valid Values** Yes or No **Default** No **Description** This parameter specifies whether the Branch Extender function will be enabled on this node. If *yes* is specified, the Branch Extender function will be enabled on this node. If *no* is specified, additional questions related to Branch Extender will not be asked during Node, Port, and Link Station definitions.
Parameter Permit search for unregistered LUs **Valid Values** Yes or No **Default** No **Description** This parameter specifies whether this node (when acting as an End Node) can be searched for LUs even if the LUs were not registered with the network node server of the Branch Extender. If *yes* is specified, this node can be searched for LUs.

Table 17. Configuration Parameter List - APPN Routing (continued)

Parameter Information
Parameter Route addition resistance **Valid Values** 0 to 255 **Default Value** 128 **Description** This parameter indicates the desirability of routing through this node. This parameter is used in the class of service based route calculation. Lower values indicate higher levels of desirability.
Parameter XID number for subarea connection (see table notes) **Valid Values** A string of 5 hexadecimal digits **Default** X'00000' **Description** This parameter specifies a unique ID number (identifier) for the network node. The XID number is combined with an ID block number (which identifies a specific IBM product) to form an XID node identification. Node identifications are exchanged between adjacent nodes when the nodes are establishing a connection. The router network node automatically appends an ID block number to this parameter during the XID exchange to create an XID node identification. The ID number you assign to this node must be unique within the APPN network identified by Network ID parameter. Contact your network administrator to verify that the ID number is unique.
Note: Node identifications are normally exchanged between T2.1 nodes during CP-CP session establishment. If the network node is communicating with the IBM Virtual Telecommunications Access Method (VTAM) product through a T2.1 LEN node and the LEN node has a CP name defined for it, the XID number parameter is not required. If the adjacent LEN node is not a T2.1 node or does not have an explicitly defined CP name, the XID number parameter must be specified to establish a connection with the LEN node. VTAM versions prior to Version 3 Release 2 do not allow CP names to be defined for LEN nodes.

Table 17. Configuration Parameter List - APPN Routing (continued)

Parameter Information
Parameter Use enhanced BATCH COS **Valid Values** Yes or No **Default** Yes **Description** This parameter specifies whether to use the enhanced COS tables. The enhanced tables assign reasonable weights to ATM TGs based on cost, speed, and delay. For ATM, the order of preference is: • Campus Best Effort (SVC or PVC)/Reserved PVC (WAN or Campus) • Campus Reserved SVC • WAN Best Effort (SVC or PVC) • WAN Reserved SVC
Parameter Use enhanced BATCHSC COS **Valid Values** Yes or No **Default** Yes **Description** This parameter specifies whether to use the enhanced COS tables. The enhanced tables assign reasonable weights to ATM TGs based on cost, speed, and delay. For ATM, the order of preference is: • Campus Best Effort (SVC or PVC)/Reserved PVC (WAN or Campus) • Campus Reserved SVC • WAN Best Effort (SVC or PVC) • WAN Reserved SVC
Parameter Use enhanced INTER COS **Valid Values** Yes or No **Default** Yes **Description** This parameter specifies whether to use the enhanced COS tables. The enhanced tables assign reasonable weights to ATM TGs based on cost, speed, and delay. For ATM, the order of preference is: • Campus Reserved (SVC or PVC) • Campus Best Effort (SVC or PVC)/WAN reserved PVC • WAN Reserved SVC • WAN Best Effort (SVC or PVC)

Table 17. Configuration Parameter List - APPN Routing (continued)

Parameter Information
Parameter Use enhanced INTERSC COS **Valid Values** Yes or No **Default** Yes **Description** This parameter specifies whether to use the enhanced COS tables. The enhanced tables assign reasonable weights to ATM TGs based on cost, speed, and delay. For ATM, the order of preference is: • Campus Reserved (SVC or PVC) • Campus Best Effort (SVC or PVC)/WAN reserved PVC • WAN Reserved SVC • WAN Best Effort (SVC or PVC)

Syntax:

set high-performance routing

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 18. Configuration Parameter List - High-Performance Routing (HPR)

Parameter Information
Parameter Maximum sessions for HPR connections **Valid Values** 1 to 65535 **Default Value** 100 **Description** This parameter specifies the maximum number of sessions allowed on an HPR connection. An HPR connection is defined by the class of service (COS), the physical path (TGs), and the network connection end points. This parameter is applicable only when the router is the initiator of the BIND. If the number of sessions exceeds the specified value for this parameter, HPR will allocate another HPR (RTP) connection.

Table 19. Configuration Parameter List - HPR Timer and Retry Options

Parameter Information
Low transmission priority traffic

Table 19. Configuration Parameter List - HPR Timer and Retry Options (continued)

Parameter Information
Parameter RTP inactivity timer **Valid Values** 1 to 3600 seconds **Default Value** 180 seconds **Description** This parameter specifies RTP's inactivity interval for HPR connections that carry traffic with *low* transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection.
Parameter Maximum RTP retries **Valid Values** 0 to 10 **Default Value** 6 **Description** This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with low transmission priority.
Parameter Path switch timer **Valid Values** 0 to 7200 seconds **Default Value** 180 seconds **Description** This parameter specifies the maximum amount of time that a path switch may be attempted on an HPR connection carrying traffic with low transmission priority. A value of zero indicates that the path switch function is to be disabled, and a path switch will not be performed.
Medium transmission priority traffic
Parameter RTP inactivity timer **Valid Values** 1 to 3600 seconds **Default Value** 180 seconds **Description** This parameter specifies RTP's inactivity interval for HPR connections that carry traffic with *medium* transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection.

Table 19. Configuration Parameter List - HPR Timer and Retry Options (continued)

Parameter Information
Parameter Maximum RTP retries **Valid Values** 0 to 10 **Default Value** 6 **Description** This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with medium transmission priority.
Parameter Path switch timer **Valid Values** 0 to 7200 seconds **Default Value** 180 seconds **Description** This parameter specifies the maximum amount of time that a path switch may be attempted on an HPR connection carrying traffic with medium transmission priority. A value of zero indicates that the path switch function is to be disabled, and a path switch will not be performed.
High transmission priority traffic
Parameter RTP inactivity timer **Valid Values** 1 to 3600 seconds **Default Value** 180 seconds **Description** This parameter specifies RTP's inactivity interval for HPR connections that carry traffic with *high* transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection.
Parameter Maximum RTP retries **Valid Values** 0 to 10 **Default Value** 6 **Description** This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with high transmission priority.

Table 19. Configuration Parameter List - HPR Timer and Retry Options (continued)

Parameter Information
Parameter Path switch timer **Valid Values** 0 to 7200 seconds **Default Value** 180 seconds **Description** This parameter specifies the maximum amount of time that a path switch may be attempted on an HPR connection carrying traffic with high transmission priority. A value of zero indicates that the path switch function is to be disabled, and a path switch will not be performed.
Network transmission priority traffic
Parameter RTP inactivity timer **Valid Values** 1 to 3600 seconds **Default Value** 180 seconds **Description** This parameter specifies RTP's inactivity interval for HPR connections that carry traffic with *network* transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection.
Parameter Maximum RTP retries **Valid Values** 0 to 10 **Default Value** 6 **Description** This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with network transmission priority.
Parameter Path switch timer **Valid Values** 0 to 7200 seconds **Default Value** 180 seconds **Description** This parameter specifies the maximum amount of time that a path switch may be attempted on an HPR connection carrying traffic with network transmission priority. A value of zero indicates that the path switch function is to be disabled, and a path switch will not be performed.

Syntax:

set dlur

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 20. Configuration Parameter List - Dependent LU Requester

Parameter Information
Parameter Enable dependent LU requester (DLUR) on this network node **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether a dependent LU requester is to be functionally enabled on this node.
Parameter Default fully-qualified CP name of primary DLUS (required when DLUR is enabled) **Valid Values** A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a CP name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully-qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names. **Default Value** None **Description** This parameter specifies the fully-qualified control point (CP) name of the dependent LU server (DLUS) that is used by default. The default primary server may be overridden on a link station basis. The default server is used for incoming requests from downstream PUs when a primary DLUS has not been specified for the associated link station.

Table 20. Configuration Parameter List - Dependent LU Requester (continued)

Parameter Information
Parameter Default fully-qualified CP name of backup dependent LU server (DLUS) **Valid Values** A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a CP name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully-qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names. **Default Value** Null **Description** This parameter specifies the fully-qualified CP name of the dependent LU server (DLUS) that is used as the default backup. A backup is not required, and the null value (representing no entry) indicates the absence of a default backup server. The default backup server may be overridden on a link station basis.
Parameter Perform retries to restore disrupted pipe **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether DLUR will attempt to reestablish the pipe to a DLUS after a pipe failure. If DLUR receives a non-disruptive UNBIND and this parameter is No, DLUR waits indefinitely for a DLUS to reestablish the broken pipe. If the pipe fails for any other reason and this parameter is No, DLUR attempts to reach the primary DLUS once. If this is unsuccessful, DLUR attempts to reach the backup DLUS. If this attempt also fails, DLUR waits indefinitely for a DLUS to reestablish the pipe. See “DLUR Retry Algorithm” on page 122 for a description of the retry algorithm.

Table 20. Configuration Parameter List - Dependent LU Requester (continued)

Parameter Information
Parameter Delay before initiating retries **Valid Values** 0 to 2 756 000 seconds **Default Value** 120 seconds **Description** This parameter specifies an amount of time for two different cases when the pipe between the DLUR and its DLUS is broken. • For the case of receiving a non-disruptive UNBIND: This parameter specifies the amount of time the DLUR must wait before attempting to reach the primary DLUS. A value of 0 indicates immediate retry by the DLUR. • For all other cases of pipe failure: The DLUR will try the primary DLUS and then the backup DLUS immediately. If this fails, DLUR will wait for the amount of time specified by the minimum of the *short retry timer* and this parameter before attempting to reach the primary DLUS. See “DLUR Retry Algorithm” on page 122 for a complete description of the retry algorithm.
Parameter Perform short retries to restore disrupted pipe **Valid Values** Yes, No **Default Value** If *Perform retries to restore disrupted pipes* is Yes, then the default value is Yes. Otherwise, the default is No. **Description** See “DLUR Retry Algorithm” on page 122 for a complete description of the retry algorithm.
Parameter Short retry timer **Valid Values** 0 to 2 756 000 seconds **Default Value** 120 seconds **Description** In all cases of pipe failure other than non-disruptive UNBIND, the minimum of *Delay before initiating retries* and this parameter specifies the amount of time DLUR will wait before attempting to reach the primary DLUS after an attempt to establish this connection has failed. See “DLUR Retry Algorithm” on page 122 for a complete description of the retry algorithm.

Table 20. Configuration Parameter List - Dependent LU Requester (continued)

Parameter Information
Parameter Short retry count **Valid Values** 0 to 65 535 **Default Value** 5 **Description** In all cases of pipe failure other than non-disruptive UNBIND, this parameter specifies the number of times the DLUR will attempt to perform short retries to reach the DLUS after an attempt to establish this connection has failed. See “DLUR Retry Algorithm” on page 122 for a complete description of the retry algorithm.
Parameter Perform long retries to restore disrupted pipe **Valid Values** Yes, No **Default Value** If *Perform retries to restore disrupted pipes* is Yes, then the default value is Yes. Otherwise, the default is No **Description** See “DLUR Retry Algorithm” on page 122 for a complete description of the retry algorithm.
Parameter Long retry timer **Valid Values** 0 to 2 756 000 seconds **Default Value** 300 seconds **Description** This parameter specifies the time DLUR will wait when performing long retries. See “DLUR Retry Algorithm” on page 122 for a complete description of the retry algorithm.

Syntax:

set tuning

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Note: You will have to re-boot in order for the changes you specify to take place.

Table 21. Configuration Parameter List - APPN Node Tuning

Parameter Information
Parameter Maximum number of adjacent nodes **Valid Values** 1 to 2 800 **Default** 100 **Description** This parameter is an estimate of the maximum number of nodes that you expect to be logically adjacent to this router network node at any one time. This parameter is used along with the *Maximum number of ISR sessions* parameter by the automatic tuning algorithm to calculate the values for the *Maximum shared memory* and *Maximum cached directory entries* tuning parameters. This parameter is configurable using the Configuration Program only.
Parameter Maximum number of network nodes sharing the same APPN network id **Valid Values** 10 to 8 000 **Default** 50 **Description** This parameter is an estimate of the maximum number of nodes that you expect in the subnetwork (that is, in the topology known by this node). This parameter is configurable using the Configuration Program only.
Parameter Maximum number of TGs connecting network nodes with the same APPN network id **Valid Values** 9 to 64 000 **Default** 3 times the value of the *maximum number of network nodes in the subnetwork*. **Description** This parameter is an estimate of the maximum number of TGs connecting network nodes in the subnetwork (that is, in the topology known by this node). This parameter is configurable using the Configuration Program only.

Table 21. Configuration Parameter List - APPN Node Tuning (continued)

Parameter Information
Parameter Maximum number of ISR sessions **Valid Values** 10 to 7 500 **Default Value** 200 **Description** This parameter specifies an estimate of the maximum number of intermediate session routing sessions (ISR) expected to be supported by this router network node at any one time. This parameter is used in conjunction with the Maximum number of adjacent nodes parameter by the automatic tuning algorithm to calculate the values for the Maximum shared memory and Maximum cached directory entries tuning parameters. This parameter is configurable using the Configuration Program only.
Parameter Percent of adjacent nodes with CP-CP sessions using HPR **Valid Values** 0 to 100% **Default Value** 0 (none) **Description** This parameter specifies an estimate of the maximum number of adjacent EN and NN, with CP-CP sessions using option set 1402 (Control Flows over RTP option set). This parameter is configurable using the Configuration Program only.
Parameter Maximum percent of ISR sessions using HPR data connections **Valid Values** 0 to 100 percent **Default** 0 percent **Description** This parameter specifies the largest percentage of ISR sessions that use ISR to HPR mappings. This parameter is configurable using the Configuration Program only.

Table 21. Configuration Parameter List - APPN Node Tuning (continued)

Parameter Information
Parameter Percent adjacent nodes that function as DLUR PU nodes **Valid Values** 0 to 100 percent **Default** 0 percent **Description** This parameter specifies the largest percentage of adjacent nodes allowed to function as adjacent DLUR PU nodes. This parameter is configurable using the Configuration Program only.
Parameter Maximum percent ISR sessions used by DLUR LUs **Valid Values** 0 to 100 percent **Default** 0 percent **Description** This parameter specifies the largest percentage of ISR sessions used by DLUR LUs. This parameter is configurable using the Configuration Program only.
Parameter Maximum number of ISR accounting memory buffers **Valid Values** 0 or 1 **Default Value** 0 (default is 1 if ISR session accounting is enabled) **Description** This parameter specifies a maximum number of buffers to be reserved for ISR session accounting. This parameter is configurable using the Configuration Program only.
Parameter Maximum memory records per ISR accounting buffer **Valid Values** 0 to 2000 **Default Value** 100 **Description** This parameter specifies a maximum number of memory records per ISR accounting buffer. This parameter is configurable using the Configuration Program only.

Table 21. Configuration Parameter List - APPN Node Tuning (continued)

Parameter Information
Parameter Override tuning algorithm **Valid Values** Yes, No **Default Value** No **Description** When enabled, this parameter overrides the tuning calculations generated by the Command Line and enables you to specify explicit values for the Maximum shared memory parameter and the Maximum cached directory entries parameter. This parameter is configurable using the Configuration Program only.
Parameter Number of local-pus for TN3270E support **Valid Values** **Default Value** **Description** This parameter specifies the number of local PUs that are available for TN3270 support. This parameter is configurable using the Configuration Program only.
Parameter Total number of LUs for TN3270E **Valid Values** **Default Value** **Description** This parameter specifies the total number of LUs available for TN3270E support. This parameter is configurable using the Configuration Program only.

Table 21. Configuration Parameter List - APPN Node Tuning (continued)

Parameter Information
Parameter Maximum shared memory **Valid Values** 1280 - 100 000 KB **Default Value** 5 108 KB **Description** This parameter specifies the amount of shared memory within the router that is allocated to the APPN network node. APPN uses its shared memory allocation to perform network operations and to maintain required tables and directories. You can allow APPN to have a 4K RU size by setting *percent of APPN shared memory used for buffers* to a sufficiently large value to allow at least 1 Megabyte of memory to be available to the buffer manager. This parameter is configurable using the Configuration Program and from **talk 6**
Parameter Percent of APPN shared memory to be used for buffers **Valid Values** 10 to 50 **Default** 10% or 512 Kilobytes, whichever is larger. **Description** This parameter specifies the amount of shared memory that APPN will use for buffers. You can allow APPN to have a 4K RU size by setting *maximum shared memory* to at least 1 Megabyte and setting *percent of APPN shared memory used for buffers* to a sufficiently large value to allow at least 1 Megabyte of memory to be available to the buffer manager. This parameter is configurable using the Configuration Program and from **talk 6**
Parameter Maximum cached directory entries **Valid Values** 0 to 65 535 **Default** 4000 **Description** This parameter specifies the number of directory entries to be stored or cached by the router network node. If a directory entry for a node is cached, the router does not need to broadcast a search request to locate the node. This reduces the time it takes to initiate sessions with the node. This parameter is configurable using the Configuration Program and from **talk 6**

Syntax:

set traces

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 22. Configuration Parameter List - Trace Setup Questions

Parameter Information
Parameter Turn all trace flags off **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables trace flags.
Parameter Edit Node-Level Traces **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. See Table 23 on page 149 for the set of questions you will be asked if this option is enabled.
Parameter Edit Interprocess Signals **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. See Table 24 on page 154 for the set of questions you will be asked if this option is enabled.
Parameter Edit Module Entry and Exit **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. See Table 25 on page 158 for the set of questions you will be asked if this option is enabled.

Table 22. Configuration Parameter List - Trace Setup Questions (continued)

Parameter Information
Parameter Edit General **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. See Table 26 on page 160 for the set of questions you will be asked if this option is enabled.

Table 23. Configuration Parameter List - Node Level Traces

Parameter Information
Parameter Process management **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the management of processes within the APPN network node, including the creation and termination of processes, processes entering a wait state, and the posting of processes.
Parameter Process to process communication **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about messages exchanged between processes in the APPN network node, including the queuing and receipt of such messages.

Table 23. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
Parameter Locking **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about locks that were obtained and released on processes in the APPN network node.
Parameter Miscellaneous tower activities **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about miscellaneous activities within the APPN network node.
Parameter I/O to and from the system **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the flow of messages entering and exiting the APPN network node.
Parameter Storage management **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about any shared memory that was obtained and released by the APPN network node.

Table 23. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
Parameter Queue data type management **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls in the APPN network node that manage general purpose queues.
Parameter Table data type management **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls in the APPN network node that manage general purpose tables, including calls to add table entries and calls to query tables for specific entries.
Parameter Buffer management **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about buffers in the APPN network node that were obtained and released.
Parameter Configuration control **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the activities of the configuration control component of the APPN network node. The configuration control component manages information about node resources.

Table 23. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
Parameter Timer service **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about requests for timer service from the APPN network node.
Parameter Service provider management **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the definition and enabling or disabling of services within the APPN network node.
Parameter Inter-process message segmenting **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the buffer transfer and freeing of chained messages within the APPN network node.
Parameter Control of processes outside scope of this tower **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the definition and activation of processes external to this APPN network node, such as when the node operator facility (NOF) defines the external process configuration control.

Table 23. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
Parameter Monitoring existence of processes, services, towers **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about requests that start or stop the monitoring of processes or services within the APPN network node.
Parameter Distributed environment control **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about requests within the APPN network node that define subsystems and create environments.
Parameter Process to service dialogs **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this trace option causes the router trace facility to gather data about all calls within the APPN network node that open, close, or send data on a dialog.
Parameter AVL Tree Support **Valid Values** Yes, No **Default** No **Description** This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls that manage AVL trees.

Table 24. Configuration Parameter List - Inter-process Signals Traces

Parameter Information
Parameter Address space manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the address space manager component.
Parameter Attach manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the attach manager component.
Parameter Configuration services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the configuration services component.
Parameter Dependent LU requester **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the dependent LU requester component.

Table 24. Configuration Parameter List - Inter-process Signals Traces (continued)

Parameter Information
Parameter Directory services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the directory services component.
Parameter Half Session **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the half session component.
Parameter HPR Path Control **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the HPR path control component.
Parameter LUA RUI **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the LUA RUI component.

Table 24. Configuration Parameter List - Inter-process Signals Traces (continued)

Parameter Information
Parameter Management Services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the management services component.
Parameter Node Operator Facility **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the node operator facility component.
Parameter Path Control **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the path control component.
Parameter Presentation Services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the presentation services component.

Table 24. Configuration Parameter List - Inter-process Signals Traces (continued)

Parameter Information
Parameter Resource manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the resource manager component.
Parameter Session connector manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the session connector manager component.
Parameter Session connector **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the session connector component.
Parameter Session manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the session manager component.

Table 24. Configuration Parameter List - Inter-process Signals Traces (continued)

Parameter Information
Parameter Session services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the session services component.
Parameter Topology and routing services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about inter-process signals from the topology and routing services component.

Table 25. Configuration Parameter List - Module Entry and Exit Traces

Parameter Information
Parameter Attach manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the attach manager component.
Parameter Half session **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the half session component.

Table 25. Configuration Parameter List - Module Entry and Exit Traces (continued)

Parameter Information
Parameter LUA RUI **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the LUA RUI component.
Parameter Node operator facility **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the node operator facility component.
Parameter Presentation services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the presentation services component.
Parameter Rapid transport protocol **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the rapid transport control component.

Table 25. Configuration Parameter List - Module Entry and Exit Traces (continued)

Parameter Information
Parameter Resource manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the resource manager component.
Parameter Session manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the session manager component.

Table 26. Configuration Parameter List - General Component Level Traces

Parameter Information
Parameter Accounting services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the accounting services component.
Parameter Address space manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the address space manager component.

Table 26. Configuration Parameter List - General Component Level Traces (continued)

Parameter Information
Parameter Architected transaction programs **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the architected transaction programs component.
Parameter Configuration services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the configuration services component.
Parameter Dependent LU requester **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the dependent LU requester component.
Parameter Directory services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the directory services component.

Table 26. Configuration Parameter List - General Component Level Traces (continued)

Parameter Information
Parameter HPR path control **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the HPR path control component.
Parameter LUA RUI **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the LUA RUI component.
Parameter Management services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the management services component.
Parameter Node operator facility **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the node operator facility component.

Table 26. Configuration Parameter List - General Component Level Traces (continued)

Parameter Information
Parameter Path control **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the path control component.
Parameter Problem determination services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the problem determination component.
Parameter Rapid transport protocol **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the rapid transport control component.
Parameter Session connector manager **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the session connector manager component.

Table 26. Configuration Parameter List - General Component Level Traces (continued)

Parameter Information
Parameter Session connector **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the session connector component.
Parameter Session services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the session services component.
Parameter SNMP subagent **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the SNMP subagent component.
Parameter TN3270E Server **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the TN3270E Server component.

Table 26. Configuration Parameter List - General Component Level Traces (continued)

Parameter Information
Parameter Topology and routing services **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the topology and routing services component.

Table 27. Configuration Parameter List - Miscellaneous Traces

Parameter Information
Parameter Data link control transmissions and receptions **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace all XIDs and PIUs transmitted and received by the APPN node.
Parameter Filter the Data **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will filter the trace data according to the way you answer the following questions.
Parameter Truncate the data **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will truncate the trace data. You will be asked to specify the *length to trace*

Table 27. Configuration Parameter List - Miscellaneous Traces (continued)

Parameter Information
Parameter Length to trace **Valid Values** 1 - 3600 **Default Value** 100 **Description** This parameter specifies the number of bytes of trace data to accumulate.
Parameter Trace Locates **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace locates.
Parameter Trace TDUs **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace topology data updates.
Parameter Trace route setups **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace route setups.
Parameter Trace CP Capabilities **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace CP Capabilities.

Table 27. Configuration Parameter List - Miscellaneous Traces (continued)

Parameter Information
Parameter Trace Session Control **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace session control traffic.
Parameter Trace XIDs **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace XIDs.

Syntax:

set management

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 28. Configuration Parameter List - APPN Node Management

Parameter Information
Parameter Collect intermediate session information **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether the APPN node should collect data on intermediate sessions passing through this node (session counters and session characteristics). The data is captured in SNMP MIB variables for APPN.

Table 28. Configuration Parameter List - APPN Node Management (continued)

Parameter Information
Parameter Save RSCV information for intermediate sessions **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether the APPN node should save the Route Selection control vector (RSCV) for an intermediate session. The data is captured in an associated SNMP MIB variable for APPN. The session RSCV is carried in the BIND request used to activate a session between two LUs. It describes the optimum route through an APPN network for a particular LU-LU session. The session RSCV contains the CP names and TG associated with each pair of adjacent nodes along a route from an origin node to a destination node.
Parameter Create intermediate session records **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables the creation of data records for intermediate sessions passing through this node. The records contain information about session counters and session characteristics. RSCV information is also included in the data records if the Save RSCV information for intermediate sessions parameter is enabled. If this parameter is set to yes, the setting of *collect intermediate session information* is overridden.
Parameter Record creation threshold **Valid Values** 0 to 4 294 967, in 1 KB increments **Default Value** 0 **Description** This parameter specifies a byte threshold for creating intermediate session records. When session data exceeds the value in this byte counter by an even multiple, a record is created.

Table 28. Configuration Parameter List - APPN Node Management (continued)

Parameter Information
Parameter Held alert queue size **Valid Values** 0 — 255 **Default Value** 10 **Description** This parameter sets the size of the configurable held alert queue. This queue is used to save APPN alerts prior to sending them to a focal point. If the queue overflows, the oldest alerts are discarded.

Table 29. Configuration Parameter List - APPN ISR Recording Media

Parameter Information
Memory Parameters
Parameter Memory (see table notes) **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables the collection of intermediate session data in the router's local memory.
Parameter Maximum memory buffers **Valid Values** 0 to 1 **Default Value** 1 **Description** This parameter specifies the number of buffers to be allocated in the router's local memory for storing intermediate session records.
Parameter Maximum memory records per buffer **Valid Values** 0 to 2000 **Default Value** 100 **Description** This parameter specifies the maximum number of intermediate session records that may be stored in the memory buffer on the router.

Table 29. Configuration Parameter List - APPN ISR Recording Media (continued)

Parameter Information
Parameter Memory buffers full **Valid Values** Stop recording (0), Wrap (1) **Default Value** Stop recording (0) **Description** This parameter specifies the action to take when the memory buffer allocated to store intermediate session records becomes full. Select **Stop recording** to instruct the router to discard any new intermediate session records. Select **Wrap** to allow new records to overwrite existing records in the buffer. The oldest records in the buffer are overwritten first.
Parameter Memory record format **Valid Values** ASCII (0), Binary (1) **Default Value** ASCII (0) **Description** This parameter specifies the format in which intermediate session records are to be stored in the router's local memory.
Parameter Time between database updates **Valid Values** 60 — 1440 minutes **Default Value** 60 **Description** This parameter sets the time in minutes between topology database updates.
Note: • When you enable the collection of intermediate session records, the data associated with the records also is collected, by default, in SNMP • MIB variables for APPN. The MIB variables are updated, in this case, whether or not the Collect intermediate session information parameter (in Table 28 on page 167) has been enabled. • Intermediate session data can be stored in router memory.

Add

Use the **add** command to add or update:

Syntax:

add port

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 30. Configuration Parameter List - Port Configuration

Parameter Information
Parameter Link type **Valid Values** Ethernet (E) Token ring (T) ATM (A) DLSw (D) FDDI IP **Default Value** None **Description** This parameter specifies the type of link associated with this port.
Parameter Interface number **Valid Values** 0 to 65533 **Default Value** 0 **Description** This parameter defines the physical interface number of the hardware interface to which this device is attached.

Table 30. Configuration Parameter List - Port Configuration (continued)

Parameter Information
Parameter Port name **Valid Values** A string of 1 to 8 characters, where the first character is alphabetic and the 2nd through 8th characters are alphanumeric. **Default Value** A unique unqualified name that is automatically generated. The name will consist of: • TR (token-ring) • EN (Ethernet) • DLS (DLSw) • IP255 • ATM • FDD (FDDI) • IP followed by the interface number. You can change the port name to a name of your choice. **Description** This parameter specifies the name representing this port.
Parameter Enable APPN routing on this port **Valid Values** Yes, No **Default Value** Yes **Description** This parameter specifies whether APPN routing is to be enabled on this port.

Table 30. Configuration Parameter List - Port Configuration (continued)

Parameter Information
Parameter Service any node **Valid Values** Yes No **Default Value** Yes **Description** This parameter specifies how the router network node responds to a request from another node to establish a connection over this port. When this parameter is enabled, the network node accepts any request it receives from another node to establish a connection. When this parameter is disabled, the network node accepts connection requests only from nodes that you explicitly define (via link station definitions). This option provides an added level of security for the router network node. **Note:** When you disable this parameter, a connection request from an adjacent node will be accepted only if the node's fully-qualified CP name parameter has been configured for a link station defined on this port. When this parameter is enabled (the default), you may still want this network node to be able to initiate connections with specific nodes over this port.
Parameter High-performance routing (HPR) supported **Valid Values** Yes, No **Default Value** Disabled for all other port types (Cannot be changed). **Description** This parameter indicates whether link stations on this port will support HPR. This value may be overridden on the link station definition.

Table 31. Configuration Parameter List - Port Configuration for ATM

Parameter Information
Parameter Local ATM Address **Valid Values** Any 14-hexadecimal character string **Default Value** None **Description** This parameter specifies the 7-byte string that comprises the user part of the local ATM address. The user part is the 6-byte ESI and the 1-byte selector field. This user-part must be unique with respect to the network part of the ATM address, which is retrieved from the ATM adapter. The selector must be unique for each protocol type.

Table 31. Configuration Parameter List - Port Configuration for ATM (continued)

Parameter Information
Parameter Enable incoming calls **Valid Values** Yes or No **Default Value** Yes **Description** This parameter determines whether calls will be rejected at the ATM level.
Parameter ATM Network Type **Valid Values** Campus or Widearea **Default Value** Campus **Description** This parameter specifies the network type used for default values for connection networks and other link stations defined on this port.
Parameter Shareable connection network traffic **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether connection network traffic can be routed on the ATM VC set up for a link station on this port.
Parameter Shareable other protocol traffic **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether other higher level protocol traffic can be routed on the ATM VC set up for a link station on this port.

Table 31. Configuration Parameter List - Port Configuration for ATM (continued)

Parameter Information
Parameter Broadband Bearer Class **Valid Values** Class_A, Class_C, Class_X **Default Value** Class_X **Description** This parameter specifies the bearer class requested from the ATM network. The classes are defined: **Class A** Constant bit rate (CBR) with end-to-end timing requirements **Class C** Variable bit rate (VBR) with no end-to-end timing requirements **Class X** Service allowing user-defined traffic type and timing requirements
Parameter Best Effort Indicator **Valid Values** Yes, No **Default Value** No **Description** This parameter indicates if a throughput guarantee is required on this SVC. If the value of this parameter is *yes*, then VCCs associated with this interface will be allocated based upon the available bandwidth.
Note: The following parameters are forward traffic parameters.
Parameter Forward Traffic Peak Cell Rate **Valid Values** 1 - 85% of line speed **Default Value** Port's Default Effective Capacity/48 **Description** This parameter indicates an upper bound on the cell transmission rate.

Table 31. Configuration Parameter List - Port Configuration for ATM (continued)

Parameter Information
Parameter Forward Traffic Sustained Cell Rate **Valid Values** 1 - 85% of line speed **Default Value** Port's Default Effective Capacity/48 **Description** This parameter indicates an upper bound on the average cell transmission rate. You cannot specify this parameter if you are using a Best Effort connection.
Parameter Forward Traffic Tagging **Valid Values** Yes, No **Default Value** Yes **Description** This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network. You cannot specify this parameter if you are using a Best Effort connection.
Parameter Forward QoS **Valid Values** CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where **CLASS_0** The unspecified class. The network does not specify any QoS. **CLASS_1** Performance is comparable to current digital private line performance. **CLASS_2** Intended for packetized video and audio in teleconferencing and multimedia applications. **CLASS_3** Intended for interoperation of connection-oriented protocols, such as Frame Relay. **CLASS_4** Intended for interoperation of connectionless protocols, such as IP. **Default Value** CLASS_0 **Description** This parameter indicates which class of service is provided to an ATM virtual connection. This parameter is always CLASS_0 for a Best Effort connection.
Note: The following parameters are backward traffic parameters.

Table 31. Configuration Parameter List - Port Configuration for ATM (continued)

Parameter Information
Parameter Backward Traffic Peak Cell Rate **Valid Values** 1 - 85% of line speed **Default Value** Port's Default Effective Capacity/48 **Description** This parameter indicates an upper bound on the cell transmission rate.
Parameter Backward Traffic Sustained Cell Rate **Valid Values** 1 - 85% of line speed **Default Value** Port's Default Effective Capacity/48 **Description** This parameter indicates an upper bound on the average cell transmission rate. You cannot specify this parameter for a Best Effort connection.
Parameter Backward Traffic Tagging **Valid Values** Yes, No **Default Value** Yes, unless Best Effort connection **Description** This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network. You cannot specify this parameter for a Best Effort connection.

Table 31. Configuration Parameter List - Port Configuration for ATM (continued)

Parameter Information
Parameter Backward QoS **Valid Values** CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where **CLASS_0** The unspecified class. The network does not specify any QoS. **CLASS_1** Performance is comparable to current digital private line performance. **CLASS_2** Intended for packetized video and audio in teleconferencing and multimedia applications. **CLASS_3** Intended for interoperation of connection-oriented protocols, such as Frame Relay. **CLASS_4** Intended for interoperation of connectionless protocols, such as IP. **Default Value** CLASS_0 **Description** This parameter indicates which class of service is provided to an ATM virtual connection. You cannot specify this parameter for a Best Effort connection.
Parameter LDLC retry count **Valid Values** 1 — 255 **Default Value** 3 **Description** This parameter is used in conjunction with the LDLC timer period to provide reliable delivery of XIDs. The retry count is initialized when a command or request is first transmitted over the link. If the LDLC timer period expires before a response is received, the command or request is retransmitted, the retry count is decremented, and the LDLC timer period is restarted. If the timer expires with the retry count at 0, the link is assumed to be inoperative.
Parameter LDLC Timer Period **Valid Values** 1 — 255 seconds **Default Value** For ATM:1 second For IP: 15 seconds **Description** This parameter specifies the timer period used with the **LDLC retry count**.

Table 32. Configuration Parameter List - Port Definition

Parameter Information
Parameter Maximum BTU size **Valid Values** 768 to 1496 bytes for Ethernet 768 to 17745 bytes for token-ring 768 to 17745 bytes for FDDI 768 to 4096 bytes for ATM **Default Value** 1289 bytes for Ethernet 2048 bytes for token-ring 2048 bytes for FDDI 2048 for ATM 1469 bytes for IP **Description** This parameter specifies the number of bytes in the largest basic transmission unit (BTU) that can be processed (transmitted or received) by a link station defined on this port. **Note:** If a negotiable BIND with an RU size greater than 2048 is received, the device will normally choose a maximum RU size of 2048. If a non-negotiable BIND with an RU size greater than 2048 is received, the device will support the larger RU size up to a maximum size of 4096.
Parameter Maximum number of link stations **Valid Values** 1 to 976 **Default Value** 512 for all ports **Description** This parameter specifies the maximum number of link stations that will be allowed to use this port. This parameter allows the resources for the APPN node and this port to be constrained.

Table 32. Configuration Parameter List - Port Definition (continued)

Parameter Information
Parameter Percent of link stations reserved for incoming calls **Valid Values** 0 to 100 The sum of the percent of link stations reserved for incoming calls and the percent of link stations reserved for outgoing calls cannot exceed 100%. **Default Value** 0 **Description** This parameter specifies the percentage of the maximum number of link stations that will be reserved for incoming calls. Link stations that are not reserved for incoming or outgoing calls are available for either purpose on a demand basis.
Parameter Percent of link stations reserved for outgoing calls **Valid Values** 0 to 100 The sum of the percent of link stations reserved for incoming calls and the percent of link stations reserved for outgoing calls cannot exceed 100%. **Default Value** 0 **Description** This parameter specifies the percentage of the maximum number of link stations that will be reserved for outgoing calls. Fractions resulting from the computation are truncated. Link stations that are not reserved for incoming or outgoing calls are available for either purpose on a demand basis.
Parameter UDP port number for XID exchange **Valid Values** 1024 to 65535 **Default Value** 11000 **Description** This parameter specifies the UDP port number to be used for XID exchange and is used during IP port definition. This port number must be the same as the one defined on other devices in the network.

Table 32. Configuration Parameter List - Port Definition (continued)

Parameter Information
Parameter UDP port number for network priority traffic **Valid Values** 1024 to 65535 **Default Value** 11001 **Description** This parameter specifies the UDP port number to be used for network priority traffic.
Parameter UDP port number for high priority traffic **Valid Values** 1024 to 65535 **Default Value** 11002 **Description** This parameter specifies the UDP port number to be used for high priority traffic.
Parameter UDP port number for medium priority traffic **Valid Values** 1024 to 65535 **Default Value** 11003 **Description** This parameter specifies the UDP port number to be used for medium priority traffic.
Parameter UDP port number for low priority traffic **Valid Values** 1024 to 65535 **Default Value** 11004 **Description** This parameter specifies the UDP port number to be used for low priority traffic.
Parameter IP network type **Valid Values** Campus or Widearea **Default Value** Widearea **Description** This parameter specifies the IP network type.

Table 32. Configuration Parameter List - Port Definition (continued)

Parameter Information
Parameter Local APPN SAP address **Valid Values** Multiples of four in the hexadecimal range X'04' to X'EC' **Default Value** X'04' **Description** This parameter specifies the local SAP address to be used for communicating with APPN link stations defined on this port.
Parameter Local HPR SAP address **Valid Values** Multiples of four in the hexadecimal range X'04' to X'EC' **Default Value** X'C8' **Description** This parameter indicates the local service access point to be used for communicating with HPR link stations defined on this port.
Parameter Branch uplink **Valid Values** Yes or No **Default Value** No **Description** This parameter indicates whether the default for link stations using this port will be uplink or downlink. If *yes* is specified, link stations using this port will default **Branch uplink** to *yes*. **Notes:** 1. This question is asked only if the node-level parameter **Enabled Branch Extender** is *yes*. 2. If **Branch uplink** is yes, the Branch Extender will present its end node appearance to this link station. Otherwise, the Branch Extender will present its network node appearance. 3. Typically, **Branch uplink** is yes for WAN-attached network nodes and is no for LAN-attached end nodes.

Table 33. Configuration Parameter List - Port Default TG Characteristics

Parameter Information	
Parameter	Cost per connect time
Valid Values	0 to 255
Default Value	For ATM SVCs: **Campus ATM best effort** 0 **Campus ATM reserved** 64 **WAN ATM best effort** 0 **WAN ATM reserved** 128 For ATM PVCs: **Campus ATM best effort** 0 **Campus ATM reserved** 0 **WAN ATM best effort** 0 **WAN ATM reserved** 0 For IP: 0 for Campus and WAN For all other: 0
Description	This parameter specifies the cost per connect time TG characteristic for all link stations on this port. The cost per connect time TG characteristic expresses the relative cost of maintaining a connection over the associated TG. The units are user-defined and are typically based on the applicable tariffs of the transmission facility being used. The assigned values should reflect the actual expense of maintaining a connection over the TG relative to all other TGs in the network. A value of zero means that connections over the TG may be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.

Table 33. Configuration Parameter List - Port Default TG Characteristics (continued)

Parameter Information
Parameter Cost per byte **Valid Values** 0 to 255 **Default Value** For ATM SVCs and ATM PVCs: **Campus ATM best effort** 0 **Campus ATM reserved** 0 **WAN ATM best effort** 128 **WAN ATM reserved** 0 For IP: 0 for Campus and WAN For all other: 0 **Description** This parameter specifies the cost per byte TG characteristic for all link stations defined on this port. The cost per byte TG characteristic expresses the relative cost of transmitting a byte over the associated TG. The units are user-defined and the assigned value should reflect the actual expenses incurred for transmitting over the TG relative to all other TGs in the network. A value of zero means that bytes may be transmitted over the TG at no additional cost. Higher values represent higher costs.

Table 33. Configuration Parameter List - Port Default TG Characteristics (continued)

Parameter Information
Parameter Security **Valid Values** **Nonsecure** all else (for example, satellite-connected, or located in a nonsecure country). **Public switched network** secure in the sense that route is not predetermined **Underground cable** located in secure country (as determined by the network administrator) **Secure conduit** Not guarded, (for example, pressurized pipe) **Guarded conduit** protected against physical tapping **Encrypted** link-level encryption is provided **Guarded radiation** guarded conduit containing the transmission medium; protected against physical and radiation tapping **Default Value** For ATM SVCs and ATM PVCs: **Campus ATM best effort** Nonsecure **Campus ATM reserved** Nonsecure **WAN ATM best effort** Public switched network **WAN ATM reserved** Public switched network For IP: **Campus** Nonsecure **WAN** Public switched network For all other: Nonsecure **Description** This parameter specifies the security TG characteristic for all link stations defined on this port. The security TG characteristic indicates the level of security protection associated with the TG. If security attributes other than the architecturally-defined ones are needed, one of the user-defined TG characteristics may be used to specify additional values.

Table 33. Configuration Parameter List - Port Default TG Characteristics (continued)

Parameter Information
Parameter Propagation delay **Valid Values** **Minimum LAN** less than 480 microseconds **Telephone** between .48 and 49.152 milliseconds **Packet switched** between 49.152 and 245.76 milliseconds **Satellite** greater than 245.76 milliseconds maximum **Default Value** For LAN: **For token-ring and Ethernet/802.3 ports** LAN **For frame-relay ports** Packet switched **For all other ports** Telephone For ATM SVCs and ATM PVCs: **Campus ATM best effort** Telephone **Campus ATM reserved** Minimum LAN **WAN ATM best effort** Packet switched **WAN ATM reserved** Telephone For IP: **Campus** Telephone **WAN** Packet switched **Description** This parameter specifies the propagation delay TG characteristic for all link stations defined on this port. The propagation delay TG characteristic specifies the approximate range for the length of time that it takes for a signal to propagate from one end of the TG to the other.

Table 33. Configuration Parameter List - Port Default TG Characteristics (continued)

Parameter Information
Parameter Effective capacity **Valid Values** 2 hexadecimal digits in the range X'00' to X'FF' **Default Value** token-ring ports: dependent upon minimum data rate specified. • X'75' when minimum is 4 Mbps • X'85' when minimum is 16 Mbps • DLSw:X'75' (4 Mbps) • FDDI: X'9A' Ethernet/802.3 ports: • X'80' for 10 Mbps For ATM SVCs (155 Mbps) and ATM SVCs (155Mbps): Campus ATM best effort: X'9F' Campus ATM reserved: X'9F' WAN ATM best effort: X'9F' WAN ATM reserved: X'9F' For IP: Campus: X'75' WAN: X'43' **Description** This parameter specifies the effective capacity TG characteristic for all associated connections (TGs) on this port. This parameter specifies the maximum bit transmission rate for both physical links and logical links. Note that the effective capacity for a logical link may be less than the physical link speed. The rate is represented in COS files as a floating-point number encoded in a single byte with units of 300 bps. The effective capacity is encoded as a single-byte representation. The values X'00' and X'FF' are special cases used to denote minimum and maximum capacities. The range of the encoding is very large; however, only 256 values in the range may be specified. This parameter provides the default value for the Effective capacity parameter on the Modify TG Characteristics Command Line option. The Modify TG Characteristics Command Line option enables you to override the .* default values assigned to TG characteristics on the individual link stations you define.

Table 33. Configuration Parameter List - Port Default TG Characteristics (continued)

Parameter Information
Parameter First user-defined TG characteristic **Valid Values** 0 to 255 **Default Value** 128 **Description** This parameter specifies the first user-defined TG characteristic for all link stations defined on this port. The first user-defined TG characteristic specifies the first of three additional characteristics that users can define to describe the TGs in a network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs.
Parameter Second user-defined TG characteristic **Valid Values** 0 to 255 **Default Value** 128 **Description** This parameter specifies the second user-defined TG characteristic for all link stations defined on this port. The second user-defined TG characteristic specifies the second of three additional characteristics that users can define to describe the TGs in a network.
Parameter Third user-defined TG characteristic **Valid Values** 0 to 255 **Default Value** 128 **Description** This parameter specifies the third user-defined TG characteristic for all link stations defined on this port. The third user-defined TG characteristic specifies the third of three additional characteristics that users can define to describe the TGs in a network.

Table 34. Configuration Parameter List - Port default LLC Characteristics

Parameter Information
Parameter Remote APPN SAP **Valid Values** Multiples of four in the hexadecimal range of X'04' to X'EC' **Default Value** X'04' **Description** This parameter specifies the SAP associated with an adjacent node's APPN link station.
Parameter Maximum number of outstanding I-format LPDUs (TW) **Valid Values** 1 to 127 **Default Value** 26 **Description** This parameter specifies the LLC maximum number of outstanding I-format LPDUs (TW) for all link stations on this port. The maximum number of outstanding I-format LPDUs defines the transmit Command Line option (TW) which is the maximum number of sequentially numbered I-format LPDUs that the link station may have unacknowledged at any given time.
Parameter Receive window size **Valid Values** 1 to 127 **Default Value** 26 **Description** This parameter specifies the LLC receive Command Line option size (RW) for all link stations on this port. The RW parameter specifies the maximum number of unacknowledged sequentially numbered I-format LPDUs that the link station can receive from the remote link station. RW is advertised in SNA XID frames and IEEE 802.2 XID frames. The XID receiver should set its effective TW to a value less than or equal to the value of the received RW to avoid overruns.

Table 34. Configuration Parameter List - Port default LLC Characteristics (continued)

Parameter Information
Parameter Inactivity timer (Ti) **Valid Values** 1 to 254 seconds **Default Value** 30 seconds **Description** This parameter specifies the LLC inactivity timer (Ti) for all link stations on this port. An LLC link station uses Ti to detect an inoperative condition in either the remote link station or in the transmission media. If an LPDU is not received in the time interval specified by Ti, an S-format command LPDU with the poll bit set is transmitted to solicit remote link station status. Recovery is then based on the reply timer (T1).
Parameter Reply timer (T1) **Valid Values** 1 to 254 half-seconds **Default Value** 2 half-seconds **Description** This parameter specifies the LLC reply timer (T1) for all link stations on this port. An LLC link station uses T1 to detect a failure to receive a required acknowledgment or response from the remote link station. When T1 expires, the link station sends an S-format command link layer protocol data unit (LPDU) with the poll bit set to solicit remote link station status or any U-format command LPDUs that have not been responded to. The duration of T1 should take into account any delays introduced by underlying layers.
Parameter Maximum number of retransmissions (N2) **Valid Values** 1 to 254 **Default Value** 8 **Description** This parameter specifies the maximum number of retransmissions (N2) for all link stations on this port. The N2 parameter specifies the maximum number of times an LPDU will be retransmitted following expiration of the reply timer (T1).

Table 34. Configuration Parameter List - Port default LLC Characteristics (continued)

Parameter Information
Parameter Receive acknowledgment timer (T2) **Valid Values** 1 to 254 half-seconds **Default Value** 1 half-second **Description** This parameter specifies the LLC receiver acknowledgment timer (T2) for all link stations on this port. The T2 parameter may be used with the N3 counter to reduce acknowledgment traffic. A link station uses T2 to delay the sending of an acknowledgment for a received I-format LPDU. T2 is started when an I-format LPDU is received, and reset when an acknowledgment is sent in an I-format or S-format LPDU. If T2 expires, the link station must send an acknowledgment as soon as possible. The value of T2 must be less than that of T1, to ensure that the remote link station will receive the delayed acknowledgment before its T1 expires.
Parameter Acknowledgments needed to increment working window **Valid Values** 0 to 127 **Default Value** 1 **Description** When the working window (Ww) is not equal to the Maximum Transmit Window Size (Tw), this parameter is the number of transmitted I-format LPDUs that must be acknowledged before the working window can be incremented (by 1). When congestion is detected, by the loss of I-format LPDUs, Ww is set to 1.

Table 35. Configuration Parameter List - HPR Override Defaults

Parameter Information
Parameter Inactivity timer override for HPR (HPR Ti) **Valid Values** 1 to 254 seconds **Default Value** 2 seconds **Description** This parameter specifies the LLC inactivity timer (HPR Ti) that is to be used for all link stations on this port supporting HPR when the HPR supported parameter is enabled on this port. This default overrides the value of the default LLC inactivity timer (Ti) parameter specified on the default LLC characteristics parameter.

Table 35. Configuration Parameter List - HPR Override Defaults (continued)

Parameter Information
Parameter Reply timer override for HPR (HPR T1) **Valid Values** 1 to 254 half-seconds **Default Value** 2 half-seconds **Description** This parameter specifies the LLC reply timer (HPR T1) that is to be used for all link stations on this port supporting HPR when the HPR supported parameter is enabled on this port. This default overrides the value of the default LLC reply timer (T1) parameter specified on the default LLC characteristics parameter.
Parameter Maximum number of retransmissions for HPR (HPR N2) **Valid Values** 1 to 254 **Default Value** 3 **Description** This parameter specifies the LLC maximum number of retransmissions (HPR N2) that is to be used for all link stations on this port supporting HPR when the HPR supported parameter is enabled on this port. This default overrides the value of the default LLC maximum number of retransmissions (N2) parameter specified on the default LLC Characteristics parameter.

Syntax:

add link-station

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 36. Configuration Parameter List - Link Station - Detail

Parameter Information
Parameter Does link support APPN function **Valid Values** Yes or No **Default Value** Yes **Description** This parameter specifies whether this link station will support APPN function. If the answer is *no*, questions concerning CP-CP sessions, security, encryption, CP name, adjacent node type, branch extender, and extended border node will not be asked and all of these functions will be disabled. Also, HPR will be disabled and no HPR questions will be asked.

Table 36. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter Link station name (required) **Valid Values** A string of 1 to 8 characters : • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Default Value** None **Description** This parameter specifies the name of a link station that represents the TG (link) between the router network node and the adjacent node. The link station name must be unique within this network node.
Parameter Port name **Valid Values** A unique unqualified name that is automatically generated. The name will consist of: • TR (token-ring) • EN (Ethernet) • DLS (DLSw) • PPP (point-to-point) • IP • FDD (FDDI) followed by the interface number. **Default Value** The name of the port that this link station is defined on. **Description** This parameter specifies the name representing the port this link station is defined on. The port must already have been configured for APPN.

Table 36. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter MAC address of adjacent node (required) **Valid Values** Token-ring 12 hexadecimal digits in the range X'000000000001' to X'7FFFFFFFFFFF' Ethernet/802.3 ports: 12 hexadecimal digits in the form *X'xyxxxxxxxxxx'* where: *x* is any hexadecimal digit *y* is a hexadecimal digit in the set {0, 2, 4, 6, 8, A, C, E} DLSw ports: • 12 hexadecimal digits in the range X'000000000001' to X'7FFFFFFFFFFF' **Default Value** None **Description** This parameter specifies the medium access control (MAC) layer address of the adjacent node. Different formats are used for token-ring and Ethernet/802.3. Token-ring and DLSw ports: The MAC address is specified in noncanonical form. In the noncanonical address format, the bit within each octet that is to be transmitted first is represented as the most significant bit. Ethernet/802.3 ports: The MAC address is specified in canonical form. In the canonical address format, the bit within each octet that is to be transmitted first is represented as the least significant bit.
Parameter IP address of adjacent node **Valid Values** Any valid IP address **Default Value** none **Description** Each link on the HPR/IP port must have a unique destination IP address.

Table 36. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter Adjacent node type **Valid Values** APPN network node, APPN end node, LEN end node **Default Value** APPN network node **Description** This parameter identifies whether the adjacent node is an APPN node, a low-entry networking (LEN) end node. When *APPN end node* is selected and *Limited resource* is No, APPN changes the adjacent node type internally to *learn* and will work with any node type. When *APPN end node* is selected and *Limited resource* is Yes, the adjacent node type is unchanged. When you select *LEN end node*, the fully-qualified control point name parameter is a required parameter. If this network node is communicating with the IBM Virtual Telecommunications Access Method (VTAM) product through the LEN node, and the LEN node is not a T2.1 node or does not have an explicitly defined control point (CP) name, then the router network node's XID number for the Subarea connection parameter also must be specified to establish a connection. **Note:** *LEN end node* is not a valid node type for HPR/IP interface.

Table 36. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter fully-qualified CP name of adjacent node **Valid Values** A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a control point name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully-qualified CP name, using the special characters @, $, and from the character set A, continues to be supported; however, these characters should not be used for new CP names. **Default Value** None **Description** This parameter specifies the fully-qualified CP name of the adjacent node. For the cases where this parameter is not required, the adjacent node's CP name may be learned dynamically during XID exchange; however, if a CP name is specified, it must match the adjacent node's definition for the link to be successfully activated. **Note:** This parameter is required when any of the following occur: • The *Service any node* parameter is set to Disable. • The *Adjacent node type* parameter is set to LEN end node. • The *CP-CP session level security* parameter is set to Enable. • The link is a limited resource.
Parameter Activate link automatically If limited resource, then this parameter is set to No and is not configurable. **Valid Values** Yes, No **Default Value** Yes **Description** When this parameter is enabled, the router network node automatically activates the link to the adjacent node and initiates a connection.

Table 36. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter Allow CP-CP sessions on this link **Valid Values** Yes, No **Default Value** Yes, if adjacent node type is APPN network node or APPN end node. No for all other adjacent node types **Description** This parameter specifies whether sessions between control points are to be activated over this link station. This parameter allows control of CP-CP session establishment between adjacent network nodes so that the overhead associated with topology database updates (TDUs) may be constrained. **Note:** Every APPN network node must have at least one CP-CP session established to another APPN network node in order to maintain the minimum connectivity necessary to update the topology database. In addition, more than minimum connectivity could be desired to eliminate single points of failure and to improve network dynamics.
Parameter CP-CP session level security **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether session level security is enforced for CP-CP sessions established over this link station. When session level security is enabled, encrypted data is exchanged and compared during the BIND flows (which includes the BIND, the BIND response, and an FMH-12 Security RU). To successfully establish a CP-CP session with session level security enabled, both partners must be configured with the same encryption key. Currently, session level security support is limited to the basic LU-LU verification protocol.
Parameter Encryption key **Valid Values** Up to 16 hexadecimal digits. If fewer than 16 digits are specified, the value is padded on the right with zeros. **Default Value** None **Description** This parameter is used to encrypt data exchanged during BIND flows. Both partners must be configured with the same key to establish a CP-CP session.

Table 36. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter Use enhanced session security (If security is enabled) **Valid Values** Yes, No **Default Value** No
Parameter High-performance routing (HPR) supported **Valid Values** Yes, No **Default Value** APPN network node, APPN end node or LEN end node: the value specified in the default HPR supported parameter for this port All other adjacent node types: No **Description** This parameter indicates whether this link station supports HPR. The user should disable HPR support if the underlying link is unreliable. An HPR connection will not be established unless both link stations advertise HPR support during XID exchange.
Parameter Branch Uplink **Valid Values** Yes or No **Default Value** The value specified for **Branch Uplink** on the port. **Description** This parameter indicates whether this link will be a Branch uplink (to WAN) or Branch downlink (to LAN). This question is asked only if **Enabled Branch Extender** has been set to *yes* and if this link station is not a network node. If **Enabled Branch Extender** has been set to *yes* and this link station is a network node, then **Branch Uplink** defaults to *yes*
Parameter Is uplink to another Branch Extender node **Valid Values** Yes or No **Default Value** No **Description** This parameter indicates whether or not the adjacent node has the Branch Extender function enabled. This question is asked only if **Branch Extender** is enabled on this node, this is an uplink, and the uplink is a limited resource.

Table 36. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter Preferred Network Node Server **Valid Values** Yes or No **Default Value** No **Description** This parameter indicates whether this uplink is to a network node server that is to be used as the network node server for the node supporting Branch Extender function and acting as an end node. If *yes* is specified, this uplink will be used as the network node server for this node. This question will be asked only if: • **Enabled Branch Extender** is *yes,* • This station is a network node, • **Branch Uplink** is *yes*, and • CP-CP sessions are supported on this link.
Parameter TG Number **Valid Values** 0 - 20 **Default Value** 0 **Description** This parameter specifies the TG number for the ATM VC.

Table 37. Configuration Parameter List - Station Configuration for ATM

Parameter Information
Parameter Virtual Channel Type **Valid Values** SVC, PVC **Default Value** SVC **Description** This parameter identifies the ATM channel type as switched virtual circuit (SVC) or permanent virtual circuit (PVC).
Note: The following parameters are common for SVCs and PVCs.

Table 37. Configuration Parameter List - Station Configuration for ATM (continued)

Parameter Information
Parameter Destination ATM Address **Valid Values** A 40- hexadecimal character string **Default Value** None **Description** This parameter specifies the 20–byte string that comprises the entire destination ATM address.
Parameter ATM network type **Valid Values** Campus, Widearea **Default Value** Campus **Description** This parameter specifies the ATM network type.
Parameter Shareable connection network traffic **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether connection network traffic can be routed on the ATM VC set up this TG.
Parameter Shareable other protocol traffic **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether other higher level protocol traffic can be routed on the ATM VC set up for this TG.

Table 37. Configuration Parameter List - Station Configuration for ATM (continued)

Parameter Information
Parameter LDLC retry count **Valid Values** 1 — 255 **Default Value** 3 **Description** This parameter is used in conjunction with the LDLC timer period to provide reliable delivery of XIDs. The retry count is initialized when a command or request is first transmitted over the link. If the LDLC timer period expires before a response is received, the command or request is retransmitted, the retry count is decremented, and the LDLC timer period is restarted. If the timer expires with the retry count at 0, the link is assumed to be inoperative.
Parameter LDLC Timer Period **Valid Values** 1 — 255 seconds **Default Value** For ATM: 1 second For IP: 15 seconds **Description** This parameter specifies the timer period used with the **LDLC retry count**.
Parameter VPI **Valid Values** 0 — 255 **Default Value** 0 **Description** This parameter identifies the VPI of the PVC at the interface.
Parameter VCI **Valid Values** 0 —65535 **Default Value** 0 **Description** This parameter identifies the VCI of the PVC at the interface.

Table 37. Configuration Parameter List - Station Configuration for ATM (continued)

Parameter Information
Parameter Broadband Bearer Class **Valid Values** Class_A, Class_C, Class_X **Default Value** Class_X **Description** This parameter specifies the bearer class requested from the ATM network. The classes are defined: **Class A** Constant bit rate (CBR) with end-to-end timing requirements **Class C** Variable bit rate (VBR) with no end-to-end timing requirements **Class X** Service allowing user-defined traffic type and timing requirements
Parameter Best Effort Indicator **Valid Values** Yes, No **Default Value** No **Description** This parameter indicates if a throughput guarantee is required on this SVC. If the value of this parameter is *yes*, then VCCs associated with this interface will be allocated based upon the available bandwidth.
Note: The following parameters are forward traffic parameters.
Parameter Forward Peak Cell Rate **Valid Values** 85% of line speed **Default Value** Port's Default Effective Capacity/48 **Description** This parameter indicates an upper bound on the cell transmission rate.

Table 37. Configuration Parameter List - Station Configuration for ATM (continued)

Parameter Information
Parameter Forward Sustained Cell Rate **Valid Values** 1 - 85% of line speed **Default Value** Port's Default Effective Capacity/48 **Description** This parameter indicates an upper bound on the average cell transmission rate. You cannot specify this parameter for Best Effort connections.
Parameter Forward Tagging **Valid Values** Yes, No **Default Value** Yes **Description** This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network. You cannot specify this parameter for Best Effort connections.
Parameter QoS **Valid Values** CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where **CLASS_0** The unspecified class. The network does not specify any QoS. **CLASS_1** Performance is comparable to current digital private line performance. **CLASS_2** Intended for packetized video and audio in teleconferencing and multimedia applications. **CLASS_3** Intended for interoperation of connection-oriented protocols, such as Frame Relay **CLASS_4** Intended for interoperation of connectionless protocols, such as IP. **Default Value** CLASS_0 **Description** This parameter indicates which class of service is provided to an ATM virtual connection. You cannot specify this parameter for Best Effort connections.
Note: The following parameters are backward traffic parameters.

Table 37. Configuration Parameter List - Station Configuration for ATM (continued)

Parameter Information
Parameter Backward Peak Cell Rate **Valid Values** 1 - 85% of line speed **Default Value** Taken from the port definition **Description** This parameter indicates an upper bound on the cell transmission rate.
Parameter Backward Sustained Cell Rate **Valid Values** 1 - 85% of line speed **Default Value** Taken from the port definition **Description** This parameter indicates an upper bound on the average cell transmission rate. You cannot specify this parameter for Best Effort connections.
Parameter Backward Tagging **Valid Values** Yes, No **Default Value** Yes **Description** This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network. You cannot specify this parameter for Best Effort connections.

Table 37. Configuration Parameter List - Station Configuration for ATM (continued)

Parameter Information
Parameter QoS **Valid Values** CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where **CLASS_0** The unspecified class. The network does not specify any QoS. **CLASS_1** Performance is comparable to current digital private line performance. **CLASS_2** Intended for packetized video and audio in teleconferencing and multimedia applications. **CLASS_3** Intended for interoperation of connection-oriented protocols, such as Frame Relay **CLASS_4** Intended for interoperation of connectionless protocols, such as IP. **Default Value** CLASS_0 **Description** This parameter indicates which class of service is provided to an ATM virtual connection. You cannot specify this parameter for Best Effort connections.

Table 38. Configuration Parameter List - Modify TG Characteristics

Parameter Information
Parameter Cost per connect time **Valid Values** 0 to 255 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter expresses the relative cost of maintaining a connection over the associated TG. The units are user-defined and are typically based on the applicable tariffs of the transmission facility being used. The assigned values should reflect the actual expense of maintaining a connection over the TG relative to all other TGs in the network. A value of zero means that connections over the TG may be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.

Table 38. Configuration Parameter List - Modify TG Characteristics (continued)

Parameter Information
Parameter Cost per byte **Valid Values** 0 to 255 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter expresses the relative cost of transmitting a byte over the associated TG. The units are user-defined and the assigned value should reflect the actual expenses incurred for transmitting over the TG relative to all other TGs in the network. A value of zero means that bytes may be transmitted over the TG at no additional cost. Higher values represent higher costs.
Parameter Security **Valid Values** • Nonsecure - all else (for example, satellite-connected, or located in a nonsecure country). • Public switched network - secure in the sense that route is not predetermined. • Underground cable - located in secure country (as determined by the network administrator). • Secure conduit - Not guarded, (for example, pressurized pipe). • Guarded conduit - protected against physical tapping. • Encrypted - link-level encryption is provided. • Guarded radiation - guarded conduit containing the transmission medium; protected against physical and radiation tapping. **Default Value** Default value is taken from the associated port parameter. **Description** This parameter indicates the level of security protection associated with the TG. If security attributes other than the architecturally-defined ones are needed, one of the user-defined TG characteristics may be used to specify additional values.
Parameter Propagation delay **Valid Values** Minimum LAN – less than 480 microseconds Telephone – between .48 and 49.152 milliseconds Packet switched - between 49.152 and 245.76 milliseconds Satellite - greater than 245.76 milliseconds Maximum **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the approximate range for the length of time that it takes for a signal to propagate from one end of the TG to the other.

Table 38. Configuration Parameter List - Modify TG Characteristics (continued)

Parameter Information
Parameter Effective capacity **Valid Values** 2 hexadecimal digits in the range X'00' to X'FF' **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the maximum bit transmission rate for both physical links and logical links. Note that the effective capacity for a logical link may be less than the physical link speed. The effective capacity is encoded as a single-byte representation. The values X'00' and X'FF' are special cases used to denote minimum and maximum capacities. The range of the encoding is very large; however, only 256 values in the range may be specified.
Parameter First user-defined TG characteristic **Valid Values** 0 to 255 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the first of three additional characteristics that users can define to describe the TGs in a network.
Parameter Second user-defined TG characteristic **Valid Values** 0 to 255 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the second of three additional characteristics that users can define to describe the TGs in a network.
Parameter Third user-defined TG characteristic **Valid Values** 0 to 255 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the third of three additional characteristics that users can define to describe the TGs in a network.

Table 39. Configuration Parameter List - Modify Dependent LU Server

Parameter Information
Parameter fully-qualified CP name of primary DLUS **Valid Values** A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a control point name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully-qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names. **Default Value** The value specified in the default fully-qualified CP name of primary dependent LU server parameter. **Description** This parameter specifies the fully-qualified CP name of the dependent LU server (DLUS) that is to be used for incoming requests from the downstream PU associated with this link station.
Parameter fully-qualified CP name for backup DLUS **Valid Values** A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a control point name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully-qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names. **Default Value** The value specified in the default fully-qualified CP name of backup dependent LU server parameter. **Description** This parameter specifies the fully-qualified CP name of the dependent LU server (DLUS) that is to be used as a backup for the downstream PU associated with this link station. This parameter allows the default backup server to be overridden. A backup is not required, and the NULL value indicates the absence of a backup server. Note that NULL can be specified even when a default backup server has been defined (by erasing the default value that appears for this parameter).

Table 40. Configuration Parameter List - Modify LLC Characteristics

Parameter Information
Parameter Remote APPN SAP **Valid Values** Multiples of four in the hexadecimal range of X'04' to X'EC'. **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the Destination SAP (DSAP) address on the destination node to which data will be sent. This DSAP address value will appear in the LLC frame to identify the service access point (SAP) address associated with the adjacent node's APPN link station.
Parameter Maximum number of outstanding I-format LPDUs (TW) **Valid Values** 1 to 127 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the transmit Command Line option which is the maximum number of sequentially numbered I-format LPDUs that the link station may have unacknowledged at any given time.
Parameter Receive window size **Valid Values** 1 to 127 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the maximum number of unacknowledged sequentially numbered I-format LPDUs that the LLC link station can receive from the remote link station. RW is advertised in SNA XID frames and IEEE 802.2 XID frames. The XID receiver should set its effective TW to a value less than or equal to the value of the received RW to avoid overruns.

Table 40. Configuration Parameter List - Modify LLC Characteristics (continued)

Parameter Information
Parameter Inactivity timer (Ti) **Valid Values** 1 to 254 seconds **Default Value** Default value is taken from the associated port parameter. **Description** A link station uses Ti to detect an inoperative condition in either the remote link station or in the transmission media. If an LPDU is not received in the time interval specified by Ti, an S-format command LPDU with the poll bit set is transmitted to solicit remote link station status. Recovery is then based on the reply timer (T1).
Parameter Reply timer (T1) **Valid Values** 1 to 254 half-seconds **Default Value** Default value is taken from the associated port parameter. **Description** A link station uses T1 to detect a failure to receive a required acknowledgment or response from the remote link station. When T1 expires, the link station sends an S-format command link layer protocol data unit (LPDU) with the poll bit set to solicit remote link station status or any U-format command LPDUs that have not been responded to. The duration of T1 should take into account any delays introduced by underlying layers.
Parameter Maximum number of retransmissions (N2) **Valid Values** 1 to 254 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the maximum number of times an LPDU will be retransmitted following the expiration of the reply timer (T1).

Table 40. Configuration Parameter List - Modify LLC Characteristics (continued)

Parameter Information
Parameter Receive acknowledgment timer (T2) **Valid Values** 1 to 254 half-seconds **Default Value** Default value is taken from the associated port parameter. **Description** This parameter may be used in conjunction with the N3 counter to reduce acknowledgment traffic. A link station uses T2 to delay the sending of an acknowledgment for a received I-format LPDU. T2 is started when an I-format LPDU is received, and reset when an acknowledgment is sent in an I-format or S-format LPDU. If T2 expires, the link station must send an acknowledgment as soon as possible. The value of T2 must be less than that of T1, to ensure that the remote link station will receive the delayed acknowledgment before its T1 expires.
Parameter Acknowledgment needed to increment working window **Valid Values** 0 to 127 acknowledgments **Default Value** Default value is taken from the associated port parameter. **Description** When the working window (Ww) is not equal to the Maximum Transmit Window Size (Tw), this parameter is the number of transmitted I-format LPDUs that must be acknowledged before the working window can be incremented (by 1). When congestion is detected, by the lost of I-format LPDUs, Ww is set to 1.

Table 41. Configuration Parameter List - Modify HPR Defaults

Parameter Information
Parameter Inactivity timer override for HPR (HPR Ti) **Valid Values** 1 to 254 seconds **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the HPR override LLC inactivity timer (HPR Ti) that is to be used when HPR is supported by this link station. This parameter overrides the value taken from the default inactivity timer override for the HPR parameter. This parameter supersedes the value of the LLC inactivity timer (Ti) parameter specified on the Modify Logical Link Control (LLC) Characteristics parameter when HPR is supported.

Table 41. Configuration Parameter List - Modify HPR Defaults (continued)

Parameter Information
Parameter Reply timer override for HPR (HPR T1) **Valid Values** 1 to 254 half-seconds **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the HPR override LLC reply timer (HPR T1) that is to be used when HPR is supported by this link station. This parameter overrides the value taken from the default reply timer override for HPR parameter specified on HPR Defaults. This parameter supersedes the value of the LLC reply timer (T1) parameter specified on the Modify Logical Link Control (LLC) Characteristics parameter when HPR is supported.
Parameter Maximum number retransmission (HPR N2) **Valid Values** 1 to 2 160 000 **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the HPR override LLC maximum number of retransmissions (HPR N2) that is to be used when HPR is supported by this link station. This parameter overrides the value taken from the default maximum number of retransmissions for HPR parameter specified on the HPR LLC Override defaults. This parameter supersedes the value of the LLC maximum number of retransmissions (N2) parameter specified on the Modify Logical Link Control (LLC) Characteristics parameter when HPR is supported.

Syntax:

add lu-name

You will be prompted to enter a station name to associate this LU with.

You will be prompted to enter a value for the following parameter. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 42. Configuration Parameter List - LEN End Node LU Name

Parameter Information
Parameter fully-qualified LU name **Valid Values** fully-qualified (explicit) LU name Generic (partially explicit) LU name Wildcard entry A string of up to 17 characters in the form of *netID.LUname*, where: • *netID* is a network ID from 1 to 8 characters • *LUname* is a control point name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully-qualified LU name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new LU names. To reduce the number of fully-qualified LU names you need to specify, you can define a generic LU name using the wildcard character (*) to represent a portion of the LU name (*LUname*). You can also define a wildcard entry by using the wildcard character as the whole LU name. **Default Value** None **Description** This parameter specifies the fully-qualified names of LUs associated with a LEN end node. The specified LU names are registered in the network node's directory services database. If a name is not registered, the network node cannot locate the LU (unless the LU name is the same as the CP name of the LEN end node). You need to specify a fully-qualified LU name, which consists of a network ID and the LU name. The network ID is the name of the network that contains the adjacent LEN end node. The LU name is the name of a logical unit accessible through the adjacent LEN end node.

Syntax:

add connection-network

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 43. Configuration Parameter List - Connection Network - Detail

Parameter Information
Parameter Fully-qualified Connection network name (required for each connection network defined) **Valid Values** A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing connection network of which this node desires to become a member, named using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new connection network names. **Default Value** None **Description** This parameter specifies the fully-qualified name of the connection network being defined on this router network node. Since this name becomes the CP name of the virtual routing node (VRN), the name must be unique among all CP and LU names in the APPN network (same as in the local Control Point Name). All nodes that are members of a given connection network must use the same VRN Name. The fully-qualified VRN Name (CP name of VRN) has the form: *NetworkID.ConnectionNetworkName* where *NetworkID* is this router network node's network identifier.
Parameter Port type (required) **Valid Values** Token-ring, Ethernet, Frame Relay BAN, IP, ATM **Note:** If the **port type** is IP, no **port name** will be specified since there is only one IP port. **Default Value** None **Description** This parameter specifies the type of ports providing connectivity to the SATF for the connection network being defined. A given connection network only supports one type of port with one set of characteristics.

Table 43. Configuration Parameter List - Connection Network - Detail (continued)

Parameter Information
Parameter Port name (required) **Valid Values** Name of port on which APPN routing has been enabled. **Note:** If the **port type** is IP, no **port name** will be specified since there is only one IP port. **Default Value** None **Description** This parameter specifies the name of a port providing connectivity to the shared access transport facility (SATF) for the connection network being defined. All ports defined for a given connection network must be the same type and have the same characteristics. **Note:** For a **port type** of IP, additional ports added to an IP connection network can be any port that IP has been defined to use. At least one additional port besides the IP port must be added for the connection network to be used. Since the IP port is a pseudo port that always comes up when the node is initialized, real ports that IP is defined on (TR, ATM, FR, ...) must be added to the CN. When at least one of these real ports is up, the connection network link is assumed active. When all of these real ports is down, the connection network link is assumed to be inactive.

Table 44. Configuration Parameter List - Connection Network Configuration for ATM

Parameter Information
Parameter Port name (required) **Valid Values** Name of port on which APPN routing has been enabled. **Default Value** None **Description** This parameter specifies the name of a port providing connectivity to the shared access transport facility (SATF) for the connection network being defined. All ports defined for a given connection network must be the same type and have the same characteristics.

Table 44. Configuration Parameter List - Connection Network Configuration for ATM (continued)

Parameter Information
Parameter fully-qualified connection network name **Valid Values** A string of 3 to 17 characters in the form of *netID.CNname*, where: • *netID* is a network ID from 1 to 8 characters • *CNname* is a connection network name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Default Value** None **Description** This parameter specifies the fully-qualified CN name to which this TG is defined.
Parameter Connection network TG number **Valid Values** 1 to 239 **Default Value** None **Description** This parameter specifies the TG number uniquely identifying this connection from the local port to the CN. The CN name and TG number pair must be unique.
Parameter Limited Resource **Valid Values** Yes or No **Default Value** Yes **Description** This parameter indicates if this TG should be brought down when not in use by session traffic.
Parameter Limited Resource Timer **Valid Values** 1 to 2160000 seconds **Default Value** 180 seconds **Description** This parameter indicates the time limit after which this CN TG should be brought down when not in use by session traffic.

Table 44. Configuration Parameter List - Connection Network Configuration for ATM (continued)

Parameter Information
Parameter LDLC retry count **Valid Values** 1 to 255 **Default Value** 3 **Description** This parameter is used in conjunction with the LDLC timer period to provide reliable delivery of XIDs. The retry count is initialized when a command or request is first transmitted over the link. If the LDLC timer period expires before a response is received, the command or request is retransmitted, the retry count is decremented, and the LDLC timer period is restarted. If the timer expires with the retry count at 0, the link is assumed to be inoperative.
Parameter LDLC Timer Period **Valid Values** 1 to 255 seconds **Default Value** For ATM: 1 second For IP: 15 seconds **Description** This parameter specifies the timer period used with the **LDLC retry count**.
Parameter Broadband Bearer Class **Valid Values** Class_A, Class_C, or Class_X **Default Value** Class_X **Description** This parameter specifies the bearer class requested from the ATM network. The classes are defined: **Class A** Constant bit rate (CBR) with end-to-end timing requirements **Class C** Variable bit rate (VBR) with no end-to-end timing requirements **Class X** Service allowing user-defined traffic type and timing requirements

Table 44. Configuration Parameter List - Connection Network Configuration for ATM (continued)

Parameter Information
Parameter Shareable Regular Network traffic **Valid Values** Yes or No **Default Value** Yes, if this is a Best Effort CN. No, otherwise. **Description** This parameter specifies whether traffic on this connection network TG can be routed on an ATM VC set up for a regular TG or another CN TG.
Parameter Shareable other protocol traffic **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether the ATM VC established for this CN TG may be shared with other higher level protocols in the router.
Note: The following parameters are forward traffic parameters.
Parameter Forward Peak Cell Rate **Valid Values** 1 to 85% of line speed **Default Value** Taken from the port definition **Description** This parameter indicates an upper bound on the cell transmission rate.
Parameter Forward Sustained Cell Rate **Valid Values** 1 to 85% of line speed **Default Value** Taken from the port definition **Description** This parameter indicates an upper bound on the average cell transmission rate.

Table 44. Configuration Parameter List - Connection Network Configuration for ATM (continued)

Parameter Information
Parameter Forward Tagging **Valid Values** Yes or No **Default Value** Yes **Description** This parameter indicates that cells that are nonconforming to cell loss priority 0 traffic specification but are conforming to cell loss priority 1 traffic specification are marked and allowed into the ATM network.
Parameter QoS **Valid Values** CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, where **CLASS_0** The unspecified class. The network does not specify any QoS. **CLASS_1** Performance is comparable to current digital private line performance. **CLASS_2** Intended for packetized video and audio in teleconferencing and multimedia applications. **CLASS_3** Intended for interoperation of connection-oriented protocols, such as Frame Relay. **CLASS_4** Intended for interoperation of connectionless protocols, such as IP. **Default Value** CLASS_3 **Description** This parameter indicates which class of service is provided to an ATM virtual connection.

Table 45. Configuration Parameter List - TG Characteristics (Connection Network)

Parameter Information
Parameter Cost per connect time **Valid Values** 0 to 255 **Default Value** 0 **Description** This parameter expresses the relative cost of maintaining a connection over the associated TG. The units are user-defined and are typically based on the applicable tariffs of the transmission facility being used. The assigned values should reflect the actual expense of maintaining a connection over the TG relative to all other TGs in the network. A value of zero means that connections over the TG may be made at no additional cost (as in the case of many non-switched facilities). Higher values represent higher costs.
Parameter Cost per byte **Valid Values** 0 to 255 **Default Value** 0 **Description** This parameter expresses the relative cost of transmitting a byte over the associated TG. The units are user-defined and the assigned value should reflect the actual expenses incurred for transmitting over the TG relative to all other TGs in the network. A value of zero means that bytes may be transmitted over the TG at no additional cost. Higher values represent higher costs.
Parameter Security **Valid Values** Nonsecure – all else (for example, satellite-connected, or located in a nonsecure country). Public switched network – secure in the sense that route is not predetermined. Underground cable – located in secure country (as determined by the network administrator). Secure conduit – not guarded, (for example, pressurized pipe). Guarded conduit – protected against physical tapping. Encrypted – link-level encryption is provided. Guarded radiation – guarded conduit containing the transmission medium; protected against physical and radiation tapping. **Default Value** Nonsecure **Description** This parameter indicates the level of security protection associated with the TG. If security attributes other than the architecturally-defined ones are needed, one of the user-defined TG characteristics may be used to specify additional values.

Table 45. Configuration Parameter List - TG Characteristics (Connection Network) (continued)

Parameter Information
Parameter Propagation delay **Valid Values** • Minimum LAN – less than 480 microseconds • Telephone – between .48 and 49.152 milliseconds • Packet switched – between 49.152 and 245.76 milliseconds • Satellite – greater than 245.76 milliseconds Maximum **Default Value** LAN **Description** This parameter specifies the approximate range for the length of time that it takes for a signal to propagate from one end of the TG to the other.
Parameter Effective capacity **Valid Values** 2 hexadecimal digits in the range X'00' to X'FF' **Default Value** X'75' **Description** This parameter specifies the effective maximum bit transmission rate for this connection network TG. Effective capacity specifies the maximum effective rate for both physical links and logical links. The effective capacity is encoded as a single-byte representation. The values X'00' and X'FF' are special cases used to denote minimum and maximum capacities. The range of the encoding is very large; however, only 256 values in the range may be specified.
Parameter First user-defined characteristic **Valid Values** 0 to 255 **Default Value** 128 **Description** This parameter specifies the first of three additional characteristics that users may define to describe the TGs in the network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs.

Table 45. Configuration Parameter List - TG Characteristics (Connection Network) (continued)

Parameter Information
Parameter Second user-defined characteristic **Valid Values** 0 to 255 **Default Value** 128 **Description** This parameter specifies the second of three additional characteristics that users may define to describe the TGs in the network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs.
Parameter Third user-defined characteristic **Valid Values** 0 to 255 **Default Value** 128 **Description** This parameter specifies the third of three additional characteristics that users may define to describe the TGs in the network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs.

Syntax:

add mode

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 46. Configuration Parameter List - APPN COS - Mode Name to COS Name Mapping - Detail

Parameter Information
Parameter Mode name (required) **Valid Values** A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing mode name for an existing network, of which this router network node is to become a member, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new mode names. **Default Value** None **Description** This parameter specifies the Mode name for the Mode name to COS name mapping being defined. See “COS Options” on page 118 for additional information about Mode name to COS mapping.
Parameter COS name (required) **Valid Values** The name of a previously defined COS definition, selected from the list of COS names defined for this router network node. **Default Value** None **Description** This parameter specifies the COS Name to be associated with the Mode name being defined for this mode name to COS name mapping.

Table 46. Configuration Parameter List - APPN COS - Mode Name to COS Name Mapping - Detail (continued)

Parameter Information
Parameter Session-level pacing Command Line option size **Valid Values** 1 to 63 **Default Value** 7 **Description** This parameter specifies the session-level pacing Command Line option size. This parameter has different definitions depending upon the type of pacing used: • For fixed session-level pacing: – The session-level pacing Command Line option size parameter specifies the receive pacing Command Line option for this node. – The value of this parameter is the suggested receive pacing Command Line option for the adjacent node. • For adaptive session-level pacing: – The session-level pacing Command Line option size parameter specifies a tuning parameter to be used as the minimum size for Isolated Pacing Messages sent by the adjacent nodes.

Syntax:

add additional-port-to-connection-network

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Note: You can have a maximum of 5 ports per connection network definition.

Table 47. Configuration Parameter List - APPN Additional port to Connection Network

Parameter Information
Parameter Connection network name (fully-qualified) (required for each connection network defined) **Valid Values** A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing connection network of which this node desires to become a member, named using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new connection network names. **Default Value** None **Description** This parameter specifies the name of the connection network being defined on this router network node. Since this name becomes the CP name of the virtual routing node (VRN), the name must be unique among all CP and LU names in the APPN network (same as in the local Control Point Name). All nodes that are members of a given connection network must use the same VRN Name. The fully-qualified VRN Name (CP name of VRN) has the form: *NetworkID.ConnectionNetworkName* where *NetworkID* is this router network node's network identifier.
Parameter Port name **Valid Values** A unique unqualified name that is automatically generated by the Command Line. The name will consist of: • TR (token-ring) • EN (Ethernet) **Default Value** Unqualified name generated by the Command Line. **Description** This parameter specifies the name representing this port. When the connection network that the port is being added to is IP, only ports that IP is defined to have an interface on will be permitted to be added to the IP CN. At least one real port that has IP defined must be added to the IP CN for the CN to become active and to be used.

Syntax:

add focal_point

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default

will be shown in square brackets [ ].

Table 48. Configuration Parameter List - APPN Implicit Focal Point

Parameter Information
Parameter focal point **Valid Values** A fully-qualified CP name **Default Value** Blanks **Description** This parameter specifies the fully-qualified CP name representing this focal point. The first focal point added is the primary implicit focal point. Up to 8 additional backup implicit focal points may be added by invoking **Add focal_point** multiple times. If the primary implicit focal point is taken off the focal point list with **Delete focal_point**, the first backup implicit focal point, if there is one, becomes the primary implicit focal point.

Syntax:

add local-pu

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 49. Configuration Parameter List - APPN Local PU

Parameter Information
Parameter Station name **Valid Values** A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Default Value** None **Description** This parameter specifies the name representing the link between the DLUR and the PU.

Table 49. Configuration Parameter List - APPN Local PU (continued)

Parameter Information
Parameter Primary DLUS name **Valid Values** A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Default Value** None **Description** This parameter specifies the name to be used to override the primary DLUS configured for this node.
Parameter Secondary DLUS name **Valid Values** A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Default Value** None **Description** This parameter specifies the name to be used to override the secondary DLUS configured for this node.
Parameter Autoactivate **Valid Values** Yes or No **Default Value** Yes **Description** This parameter specifies whether to activate this link at start-up.

Delete

Use the **delete** command to delete:

Syntax:

delete port *port-name*
link *link-station-name*
lu-name *lu-name*
connection-network *connection-network-name*
additional-port-to-connection-network *cn-port-name*
mode *name*

focal_point *focal-point-name*

local-pu

List

Use the **list** command to list:

Syntax:

list all

node

traces

management

hpr

dlur

port *port name*

link station *link station name*

lu name *lu name*

mode name *mode name*

connection network *connection network name*

focal_point

Activate_new_config

Use the **activate_new_config** command to read the configuration into non-volatile memory.

Syntax:

activate_new_config

Monitoring APPN

This section describes how to monitor APPN. It includes the following sections:

- "Accessing the APPN Monitoring Commands"
- "APPN Monitoring Commands" on page 229

Accessing the APPN Monitoring Commands

Use the following procedure to access the APPN monitoring commands. This process gives you access to an APPN's *monitoring* process.

At the OPCON prompt, enter **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 **Return** again.

Enter **protocol APPN** For example:

```
* talk 5
+
+ protocol APPN
```

APPN Monitoring Commands

This section describes the APPN monitoring commands for monitoring APPN interfaces. Enter the commands at the APPN> prompt.

Table 50. APPN 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 xxi.
Aping	Pings an address
List	Lists: • CP-CP_sessions - displays information on CP-CP sessions. • ISR_sessions - displays information on active ISR transmission groups. • Session_information - If *Save RSCV information for intermediate nodes* is Yes, displays origin CP Name, primary LU Name, and secondary LU Name. • RTP_connections - displays information on RTP connections. • Port_information - displays information on all ports unless a particular interface is requested. • Link_information - displays information on all links unless a particular interface is requested. • Focal_point - displays currently active focal point. • Local-link • Log • Incomplete_locates
Memory	Obtains and displays APPN memory usage information.
Restart	Restarts APPN
Stop	Stops APPN
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxii.

Aping

Syntax:

aping *flags lu_name*

where,

flags Specifies the options for the APING.

-m Mode name

Default Value: #INTER

-t TP name

Default Value: APING

-i Count of sends and receives to issue

Default Value: 1

-x Count of conversations to run

Default Value: 1

-y Count of TPs to run

Default Value: 1

-s Size of packet

Default Value: 100

-q Quiet

-b Background display goes to `talk 2`

lu_name

Specifies the fully-qualified LU name of the target of the APING.

Valid Values: Any valid fully-qualified LU name

Default Value: None

Dump

Use the **Dump** command to create an APPN dump.

Syntax:

dump

You can check the size on the dump server to know when the dump finishes.

The router continues to execute while the dump occurs.

List

Use the **List** command to display information about the APPN configuration. The command lists:

Syntax:

list *name*

Command	Function
List cp	Displays a table of all cp sessions.
List isr	Displays a table of all defined active ISR transmission groups.
List session_info	Displays origin CP Name, primary LU Name and secondary LU Name if *Save RSCV information for intermediate sessions* is Yes.
List rtp	Displays a table of all RTP connections.
List port	Displays a summary table of all ports.
List port *port name*	Displays detailed information about the requested port.
List link	Displays a summary table of all links.

List link *station name*
Displays detailed information about the requested link station.

List focal Displays currently active focal point, if there is one.

List local_link_information
Displays information about local links.

log Displays the last 20 log entries.

incomplete_locates
Displays information on locates waiting for replies.

Memory

Use the **Memory** command to display APPN memory usage information.

Syntax:

memory

Restart

Use the **Restart** command to restart APPN after it has been stopped.

Syntax:

restart

Stop

Use the **Stop** command to cause APPN to stop.

Syntax:

stop

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 LANE Shortcuts Interface

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

A

B

C

D

E

F

H

I

J

L

M

N

O

P

R

S

T

V

Readers' Comments — We'd Like to Hear from You

Nways Multiprotocol Switched Services
Configuring Protocols and Features
Volume 2

Publication No. SC30-3994-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

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

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
SC30-3994-00

IBM®

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

SC30-3994-00

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC30-3994-00

Spine information:

Nways Multiprotocol Switched Services

MSS Configuring Protocols Vol. 2

SC30-3994-00