Access Integration Services

Protocol Configuration and Monitoring Reference Volume 2
Version 3.4

SC30-3991-02

Access Integration Services

IBM

Protocol Configuration and Monitoring Reference Volume 2 Version 3.4

SC30-3991-02

Note

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

Third Edition (October 1999)

This edition applies to Version 3 Release 4 of the IBM Access Integration Services 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
U.S.A.

If you prefer, you may use the IBM support Web site to submit comments. To do this, click *Overall Site Feedback* at URL:

http://www.networking.ibm.com

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

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

Advanced Peer-to-Peer Networking
APPN
eNetwork
IBM
OS/2
SecureWay
VTAM

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

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

NetView is a trademark of Tivoli Systems, Inc. in the United States or other countries or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Preface

This manual belongs to the product library described in “Library Overview” on page xxiv and describes a group of protocols supported by the 2212. A specific 2212 might not support all of the features and functions described in these manuals. If a feature or function is device-specific, that restriction is indicated in the relevant manual.

This manual refers to the 2212 as either “the router” or “the device.” The examples in the library represent the configuration of a 2212, but the actual output you see may vary. Use the examples as a guideline to what you might see while configuring your device.

Who Should Read This Manual

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

Getting Additional Information

Changes may be made to the documentation after the books are printed. If additional information is available or if changes are required after the books have been printed, the changes will be in a file (named README) on the CD-ROM. You can view the file with an ASCII text editor.

About the Software

IBM Access Integration Services is the software that supports the IBM 2212 (licensed program number 5639-F73). This software has these components:

- The base code, which consists of:
  - The code that provides the routing, bridging, data link switching, and SNMP agent functions for the device.
  - The router user interface, which allows you to configure, monitor, and use the Access Integration Services base code installed on the device. The router user interface is accessed locally through an ASCII terminal or emulator attached to the service port, or remotely through a Telnet session or modem-attached device.

  The base code is installed at the factory on the 2212.
- The Configuration Program for IBM Access Integration Services (referred to in this book as the *Configuration Program*) is a graphical user interface that enables you to configure the device from a stand-alone workstation. The Configuration Program includes error checking and online help information.

  The Configuration Program is not pre-loaded at the factory; it is shipped separately from the device as part of the software order.

  You can also obtain the Configuration Program for IBM Access Integration Services from the IBM Networking Technical Support home page. See *Configuration Program User’s Guide for Nways Multiprotocol and Access Services,*, GC30-3830, for the server address and directories.

Conventions Used in This Manual

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

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

   ```
   reload
   ```

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

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

   Choose one of the keywords as a value for the parameter.
3. 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.
6. Names of keyboard keys that you press are indicated like this: **Enter**
7. Variables (that is, names used to represent data that you define) are denoted by italics. For example:

   File Name: *filename.ext*

Library Overview

Information updates and corrections: To keep you informed of engineering changes, clarifications, and fixes that were implemented after the books were printed, refer to the IBM 2212 home pages at:

`http://www.networking.ibm.com/2212/2212prod.html`

The following list shows the books in the IBM 2212 library, arranged according to tasks.

Planning

GA27-4215

IBM 2212 Introduction and Planning Guide

This book is shipped with the IBM 2212. It explains how to prepare for installation and perform an initial configuration.

Installation

GA27-4216
: *IBM 2212 Access Utility Installation and Initial Configuration Guide*

  This booklet is shipped with the IBM 2212. It explains how to install the IBM 2212 and verify its installation.

GX27-4048
: *2212 Hardware Configuration Quick Reference*

  This reference card is used for entering and saving hardware configuration information used to determine the correct state of an IBM 2212.

Diagnostics and Maintenance

GY27-0362
: *IBM 2212 Access Utility Service and Maintenance Manual*

  This book is shipped with the IBM 2212. It provides instructions for diagnosing problems with and repairing the IBM 2212.

Operations and Network Management

The following list shows the books that support the Access Integration Services program.

SC30-3988
: *Software User's Guide*

  This book explains how to:

  - Configure, monitor, and use the Access Integration Services software.
  - Use the Access Integration Services command-line router user interface to configure and monitor the network interfaces and link-layer protocols shipped with the IBM 2212.

SC30-3989
: *Using and Configuring Features*

SC30-3990
: *Protocol Configuration and Monitoring Reference Volume 1*

SC30-3991
: *Protocol Configuration and Monitoring Reference Volume 2*

  These books describe how to access and use the Access Integration Services command-line user interface to configure and monitor the routing protocol software shipped with the product.

  They include information about each of the protocols that the devices support.

SC30-3682
: *Event Logging System Messages Guide*

  This book contains a listing of the error codes that can occur, along with descriptions and recommended actions to correct the errors.

Configuration

GC30-3830
: *Configuration Program User's Guide for Nways Multiprotocol and Access Services*

This book discusses how to use the Configuration Program.

Safety

SD21-0030

Caution: Safety Information—Read This First

This book, shipped with the IBM 2212, provides translations of caution and danger notices applicable to the installation and maintenance of a IBM 2212.

Marketing

The following IBM Web page provides product information:

`http://www.networking.ibm.com/2212/2212prod.html`

Summary of Changes for the IBM 2212 Software Library

The following list applies to the changes in the software that were made in Version 3 Release 4:

- Frame Relay enhancements:
  - New Frame Handler (FH) support
  - PU throttling to handle bursts of traffic in support of 3745 controllers
  - New interface type (Frame Relay subinterface) to allow virtual interfaces on the same physical interface
  - Unnumbered IP support
- VPN enhancements:
  - CPE enhancements:
    - Policy information from LDAP servers is locally stored.
    - Policy quick configuration.
    - Policy consistency checking.
    - Policy information may now be retrieved from LDAP servers within an administrative domain.
    - IPSec tunnel ping.
  - IP enhancements:
    - Voice routing enhancements:
      - IP Header Compression on PPP (RFCs 2507, 2508, 2509)
      - Interleaving voice traffic between fragmented data packets on multi-link PPP
      - Interleaving voice traffic between fragmented data packets on Frame Relay
      - Bypassing PPP or Frame Relay packet compression and encryption for voice traffic
    - IP loopback address

      This support allows users to define IP addresses on a special interface to support TN3270 Gateway, Network Dispatcher, and IPSec requirements.
    - IPv6
      - An inter-domain routing function (BGP4+) is provided for IPv6 that supports IPv6 routing and addressing information and uses TCP6 for transport.
    - Multiple forwarding paths

      IP routing can use up to four equal-cost static routes to support multiple parallel links to a given address and mask.
    - IP route aggregation

- Multicast enhancements:
  - Protocol Independent Multicast-Dense Mode (PIM-DM) for IPv4.
  - Network administrators can now control the flow of IP multicast data into and out of their networks by using inbound and outbound traffic filters.
- Not-so-stubby area (NSSA)

  OSPF supports not-so-stubby area (NSSA) as defined in RFC 1587 and the latest Internet draft is now supported.
- Random Early Detection (RED)
- Differential services policing enhancements
- VRRP enhancements:
  - The hardware MAC address may be used instead of a virtual MAC address to identify a redundant gateway; this can offer a performance improvement.
  - When more than one backup candidate is available, preempt options can be configured.
  - For selecting the master IP router, additional criteria, such as available route or network interface, can be used to support non-IP functions.

- Dial-on-demand alternate interface for WAN reroute
- TN3270 enhancements
  - LU capping
  - LU-pool load balancing
  - Talk 5 disconnect of TN3270 sessions
  - Additional reporting information
  - Support of addresses 1 and 255
- Network Dispatcher enhancements
  - Advertising of network dispatcher cluster addresses by routing protocols
  - A new SSL Advisor
- DLSw SDLC PU1 support
- Ethernet encapsulation support for both ethernet type II (default) and 802.3 simultaneously on the same interface
- DHCP enhancements:
  - Hardfile backup for lease information
  - Multiple IP address support for DHCP interfaces
  - Short lease support
- RADIUS enhancements
  - Radius scalability
  - Login of Last Resort
- L2TP Scalability
- Thin Server enhancement

  Connection to an alternate or back-up master server
- Service file retrieval enhancements

Clarifications and corrections

In hard copy and PDF, the technical changes and additions are indicated by a vertical line (|) to the left of the change.

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.

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 2212. 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 ASRT protocol configuration process:

```
ASRT config> exit
Config>
```

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

Chapter 1. Using APPN

This chapter describes APPN® and includes the following sections:

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 16 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 1. 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 16.

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 1. Implementation of APPN Network Node Functions

APPN Function	Yes	No	Notes
Session services and supporting functions			
Multiple CP-CP sessions	X		
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

Table 1. Implementation of APPN Network Node Functions (continued)

APPN Function	Yes	No	Notes
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
   - X.25 SVC links
   - PPP links running over ISDN, V.25 bis, or V.34
   - Frame relay links running over ISDN
   - Token-ring links
   - Ethernet links
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, Frame Relay BAN ports, and Enterprise Extender Support for HPR over IP.

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

1124 Self-Configuring Branch Extender Backup

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

***Note::** When defining parallel TGs if using dynamic TG number assignment, either ALL of the links or NONE of the links must be defined between the two nodes.

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 QLLC protocol for X.25 direct data link control, the IEEE 802.2 LLC Type 2 protocol for token-ring, Ethernet, PPP, and Frame Relay and SDLC protocol for the SDLC data link control. APPN HPR, which is supported on token-ring, Ethernet, PPP, and Frame Relay, 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:

- For token-ring and Ethernet LAN ports:

  Each protocol that uses a port must have a unique SAP address, with the exception of DLSw (which may use the same SAP address as other protocols because DLSw frames will not be destined for the local MAC address, but rather a DLSw MAC 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.
- For Frame Relay ports:

  APPN ISR traffic and APPN HPR traffic transferred over a Frame Relay data link connection supports both the RFC 1490/2427 bridged frame format and the RFC 1490/2427 routed frame format.

  – RFC 1490/2427 routed frame format

APPN ISR traffic will be transferred over a Frame Relay data link connection using the connection-oriented multiprotocol encapsulation method defined in RFC 1490/2427 using:
- NLPID = X'08' (Q.933 encoding)
- L2PID = X'4C80' (Layer 2 protocol identifier indicating 802.2 LLC)
- L3PID = X'7083' (Layer 3 protocol identifier indicating SNA-APPN/FID2)

APPN HPR traffic transferred over a frame-relay data link connection does not use IEEE 802.2 LLC. It uses a different multiprotocol encapsulation as defined in RFC 1490/2427 using:
- NLPID = X'08' (Q.933 encoding)
- L2PID = X'5081' (Layer 2 protocol identifier for no Layer 2 protocol)
- L3PID = X'7085' (Layer 3 protocol identifier indicating SNA-APPN/HPR)

APPN HPR does not use a SAP for traffic transferred using the RFC 1490/2427 routed frame format because there is no Layer 2 protocol.

- – RFC 1490/2427 Bridged format

  APPN HPR uses a SAP for traffic transferred using the RFC 1490/2427 bridged frame format.

- For PPP ports:
  - APPN ISR traffic uses 802.2 LLC over the PPP connection.
  - Since there is no Layer 2 protocol used in HPR’s RFC 1490/2427 encapsulation, no SAP is used for HPR traffic.
- Enterprise Extender Support for HPR over IP

Refer to Table 2 on page 19 for a list of DLCs that support HPR.

Note: HPR is not supported over SDLC, X.25, or DLSw ports.

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.

See Table 2 on page 19 for the types of ports providing connection to the downstream PU (DSPU) that are supported.

Functions Supported

The APPN DLUR option includes the following functions:

- Support for SDLC-attached downstream T2.0 nodes containing dependent LUs that do not support XID exchange.
- 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.
- You must be able to establish an APPN-only or APPN/HPR-only session between DLUS and DLUR. The CPSVRMGR session cannot pass through a subarea network.

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 *IBM VTAM Resource Definition Reference* 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 1
************************************************************************
* Path statements are not required if the DSPU is initiating the
```

```
* connection to VTAM
************************************************************************
*PU20LU1  LU    LOCADDR=2          11
*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   1
************************************************************************
************************************************************************
*
* Following are examples of path statement coding for various
* DLC types.
*
 * 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.
*
************************************************************************
************************************************************************
* Below is SDLC
************************************************************************
*A20RT   PATH  PID=1,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,SDLCNS),
*              DLCADDR=(2,X,5353),  2  **port name
*              DLCADDR=(3,X,C1)     3a **station address

************************************************************************
* Below is Frame Relay
************************************************************************
*A20RT   PATH  PID=2,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,FRPVC),
*              DLCADDR=(2,X,4652303033),  2 **port name
*              DLCADDR=(3,X,04),       3 **SAP address
*              DLCADDR=(4,X,0024)      4 **DLCI
************************************************************************
* Below is Frame Relay BAN
************************************************************************
*A20RT   PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,FRPVC),
*              DLCADDR=(2,X,4652303033),        2 **port name
*              DLCADDR=(3,X,04),            3 **SAP address
*              DLCADDR=(4,X,0024),          4 **DLCI
*              DLCADDR=(6,X,400000000001)   5 **MAC addr
************************************************************************
* Below is DLSw
************************************************************************
*A20RT   PATH  PID=3,
*              DLURNAME=GOLD,
*              DLCADDR=(1,C,TR), 7
*              DLCADDR=(2,X,444C53323534), 2 **port name
*              DLCADDR=(3,X,04),            3 **SAP address
*              DLCADDR=(4,X,400000000001)   6 **MAC address
*
*************************************************************************
** Below is Token Ring
*************************************************************************
*PATHT20  PATH  PID=1,
*               DLURNAME=RED,
*               DLCADDR=(1,C,TR),
*               DLCADDR=(2,X,5452303030),   2 **port name
*               DLCADDR=(3,X,04),           3 **SAP address
*               DLCADDR=(4,X,400000011088)  6 **MAC address
*************************************************************************
** Below is Ethernet
*************************************************************************
*PATHE20 PATH  PID=1,
*               DLURNAME=PURPLE,
*               DLCADDR=(1,C,ETHERNET),
*               DLCADDR=(2,X,454E303030),   2 **port name
*               DLCADDR=(3,X,20),           3 **SAP address
*               DLCADDR=(4,X,400000011063)  6 **MAC address
```

```
**********************************************************************
* Below is X25 SVC
**********************************************************************
*A20RT   PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,X25SVC),
*              DLCADDR=(2,X,583235303033),    2 **port name
*              DLCADDR=(4,X,C3),      8 **Protocol identifier
*              DLCADDR=(21,X,000566666), 9 **Destination DTE address
**********************************************************************
* Below is X25 PVC
**********************************************************************
*A20RT   PATH  PID=3,
*              DLURNAME=GREEN,
*              DLCADDR=(1,C,X25PVC),
*              DLCADDR=(2,X,583235303033),   2 **port name
*              DLCADDR=(3,X,0001)            10 **Logical channel number
**********************************************************************

**********************************************************************
**********************************************************************
* LU statements
**********************************************************************
**********************************************************************
*PU21LU1  LU    LOCADDR=2         11
*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)
3a Station address for SDLC
4 DLCI must have 4 digits because it is a half-word
5 MAC address of the DSPU (noncanonical) for Frame Relay BAN
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
8 Protocol identifier
9 Destination DTE address (000566666, where:
00 is fixed
05 is the length of the DTE address
66666 is the DTE address)
10 Logical channel number. It must have 4 digits because it is a halfword.
11 LU coding

See “Chapter 2. Using TN3270” on page 67 for an example of an internal PU path statement.

APPN Connection Networks

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 23 on page 153 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 and hidden WAN topology from the BrNN.
- 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.

It is possible to configure two or more peer BrNNs in a single branch, each serving a set of ENs in the branch. When one of these BrNNs loses connectivity to its preferred network node server, it is desirable for one of the other BrNNs to take over serving the first BrNN's ENs.

You can configure peer BrNNs to automatically back each other up in this situation by shifting from a peer to a cascaded BrNN configuration.

Extended Border Nodes

Extended Border Nodes (BNs) allow networks with different network IDs to connect to one another. CP-CP sessions will be established across the network boundaries, and directory services flows and session establishment will be allowed to span the interconnected networks. Topology information will not be exchanged across the network boundary. This allows networks with different network IDs to establish CP-CP sessions and provides topology isolation between different networks.

In addition to allowing networks with different network IDs to interconnect, BNs provide a mechanism to subdivide networks with the same network ID into smaller “topology subnetworks”. This subdivision provides topology isolation between the two subnetworks while allowing directory services flows and sessions to span the subnetwork boundaries.

There must be a BN on one side of the subnetwork boundary in order to use this function. When a BN connects to a non-native NN, the BN looks like an EN to the non-native NN, even though the BN is actually a NN.

There may be two BNs, one on each side of the boundary, cooperating to perform this function. When two BNs connect across a subnetwork boundary, the BN will look like a NN to the non-native BN.

A BN will appear to be the NN server for all non-native resources accessible through the BN. This allows the existing APPN directory caching and route calculation functions to work, while enabling the BN to intercept and modify all Locate and BIND flows which cross an inter-subnetwork TG (ISTG).

BNs implement piece-wise optimal session route calculation. Each subnetwork calculates its own part of the session's route selection control vector (RSCV) to the entry point in the next non-native subnetwork. While the RSCV will be optimal through the native subnetwork, there is no guarantee that the end-to-end session path will be optimal.

Network Topology Example

Figure 1 shows many of the connectivity options provided by the BN function. In general, you can get from any network to any other network except that NetF can only reach network NetE and NetE is the only network that can reach NetF.

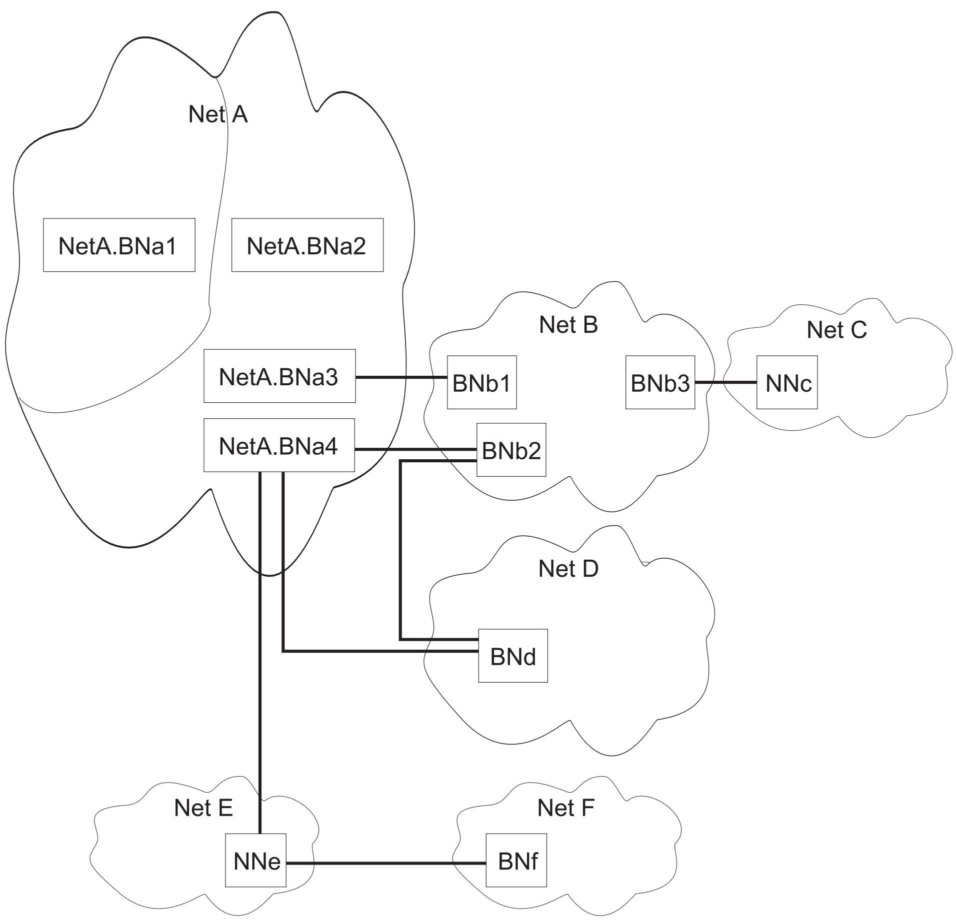


Figure 1. Extended Border Node Connectivity

Note: Solid lines represent intersubnetwork TGs.

In this figure:

- Netid subnetwork NetA has been divided into topology subnetworks. The left-most topology subnetwork contains BNa1 which is connected across an intersubnetwork TG to BNa2 in the right topology subnetwork. The netid of both BNa1 and BNa2 is NetA.
- BNa1 is non-native to all the other extended border nodes, including NetA2.
- BNa2, BNa3 and BNa4 are all native to the right topology subnetwork of NETA, and non-native to the other networks, including the subnetwork containing BNa1.
- A BN can interconnect multiple networks as BNa4 connects topology subnetwork of NetA to both NetB and NetD.
- Multiple links can connect two networks as the right topology subnetwork of NetA and NetB are connected by both BNa3/BNb1 and BNa4/BNb2.
- Both ends of an inter-network link must be BNs, unless one of the networks is a peripheral network. In this case, the peripheral network may use a conventional non-BN network node to connect to the BN in the adjoining network. This is shown where peripheral network NetC connects to NetB with NNc.
- Any LU in networks NetA, NetB, NetC, NetD, or NetE can get to any other LU in any of those networks. Both NetC and NetE are connected using conventional non-BN network nodes.
- Network NetE is connected using conventional non-BN network node NNe to BNs in NetA2 and NetF. You can not have a network node interconnecting non-peripheral networks, so it is not possible to get from NetF to any network other than NetE.
- You can get from NetA2 to NetE and from NetE to NetA2 since NNe is in a peripheral network. Similarly, you can get from NetF to NetE and from NetE to NetF.

Session Services Extensions (SSE) for NNS Support

The SSE function of a router is enabled when the router is enabled for APPN. This is true even if the Extended Border Node function is not enabled. This means that the router may act as the network node server for a VTAM end node. As such, it can handle NNS functions for end nodes requesting SLU-initiated sessions, third part initiated sessions, session request queuing, automatic login, session-release requests, and EN TG vector registration.

The SSE function is not used when the router is acting as a Branch Extender since down stream VTAMs are not allowed in that configuration.

Network Requirements

There are no requirements for other APPN nodes in a network as long as they are not directly connected to a BN across a topology boundary. APPN nodes that are connected to a BN across a topology boundary (across an ISTG) must meet one of these requirements:

- APPN Ver1 with option set 1013, Interoperability with peripheral extended border node
- APPN Ver2, where option set 1013 is part of the base software.

Nodes attached using ISTGs that do not meet either of these requirements will generate alerts and do not handle some of the new flows associated with BNs. However, if other paths through the network are available, you may still have end-to-end connectivity.

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)
- Extended Border Node
- TN3270 Base
- TN3270 Response Time

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 TN3270 Connection Rejection

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 32 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 2 shows the DLC ports supported by the device over APPN:

Table 2. Port Types Supported for APPN Routing

Port Type	Standard	HPR	ISR	DLUR[1]
Ethernet	Version 2	Yes	Yes	Yes
Ethernet	IEEE 802.3	Yes	Yes	Yes
TR	802.5	Yes	Yes	Yes
Serial PPP		Yes	Yes	No
Serial FR (bridged and routed)[2]		Yes	Yes	Yes
Frame Relay BAN		Yes	Yes	Yes
Serial LAN bridging		NA	NA	NA
SDLC		No	Yes	Yes
X.25	CCITT X.25	No	Yes	Yes
DLSw		No	Yes	Yes
APPN/PPP/ISDN		Yes	Yes	No
APPN/FR/ISDN		Yes	Yes	Yes
APPN/PPP/V.25 bis		Yes	Yes	No
APPN/PPP/V.34		Yes	Yes	No
HPR over IP		Yes	No	Yes
100Mbps Ethernet		Yes	Yes	Yes
100Mbps TR	802.5	Yes	Yes	Yes

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)
- Change of node function (EBN, BN, NN)
- 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
  - Delete TN3270E parameters
  - Routing lists
  - CoS mapping tables

| See"APPN Dynamic Reconfiguration Support" on page 252 for details on dynamic
| changes you can make to your APPN configuration.

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:

- LAN ports:
  - Token-ring
  - Ethernet
- Serial ports configured with:
  - PPP
  - Frame relay
  - X.25
  - SDLC
  - Dial circuits over ISDN
  - Dial circuits over V.25 bis
  - Dial circuits over V.34
- DLSw
- HPR over IP

| The `talk 6` code required to configure APPN or TN3270 resides on the
| corresponding load module (.ld file), and that module 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`

1. This column refers to the port providing the connection to the downstream PU (DSPU).
2. Use bridged format when you have two devices connected by Frame Relay and one of them does not have APPN. Otherwise, use routed format because of improved performance.

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" on page 22.

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: Because 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 21.

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:
   - Token-ring LAN port
   - Ethernet LAN port
   - Frame-relay serial port
   - PPP serial port
   - X.25
   - SDLC
   - DLSw
   - IP port
3. Enable APPN routing on APPN ports with the *enable APPN routing on this port* parameter.

Note: Because 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:
   a. Network ID
   b. 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:
   - Token-ring LAN port
   - Ethernet LAN port
   - Frame-relay serial port
   - PPP serial port
   - X.25
   - DLSw
   - SDLC
   - IP port
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 Full, Partial, or None to the *Enable Branch Awareness Support* question, depending on whether you want to limit the flow of topology information about the TGs between NNs and BrNNs.
   c. 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.
   d. 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.

Configuring Extended Border Nodes

To configure extended border node you must configure one or more of these parameters:

- Set node
- Add port
- Add link
- Add routing_list
- Add cos_mapping_table

Set node

The previously existing prompt used to enable branch extender has been expanded to allow you to choose the branch extender function, the extended border node function, or neither. Only if you enable the extended border node function will any of the other extended border node prompts appear.

Subnetwork visit count is the first prompt. This parameter defines the maximum number of topology subnetworks a session may span. The value defined here is used as the default value for the extended border node. You can specify different values for the subnetwork visit count when adding ports, links, or routing lists.

Cache search time is the next node level prompt. This specifies the number of minutes the extended border node will retain information on multi-subnetwork searches. The intention is for this to be the primary mechanism for limiting the size of this cache. However, the next parameter can also be used to control the size of this cache.

Maximum search cache size is next. This controls the same data structure controlled by the previous parameter. If set to zero, the maximum size is unlimited. Entries will be discarded only after the search cache time has expired. If you prefer to have a fixed maximum size for the search cache then specify that here. If this maximum is reached before any entries exceed the time limit the least recently entries are discarded.

List dynamics is the next prompt, and it allows you to control how the extended border node determines possible next hops when attempting to locate resources (LUs). The temporary list of possible next hop CPs is built dynamically by the operational code whenever the border node is attempting to locate a resource. This parameter specifies sources of next hop CP names the extended border node may use to build this temporary dynamic list of CP names.

After the temporary list is built, it is always ordered so that configured next-hop CPs are first followed by CPs associated with similarly named known resources. Additional reordering may be performed. Once all the reordering is complete, the extended border node starts searching for the target resource one CP after another.

Note that once the extended border node actually locates a resource it will remember the next hop CP and always use that next hop CP for that particular resource, ignoring the routing lists. Entries from this table of located resources can be quite long lived. They are discarded if the table reaches its maximum size, a later search to that CP fails to locate the resource, or if search from that LU comes from a different CP.

The list dynamics parameter is set to one of the following values. It is possible to respecify this value for individual routing lists when, and if, you configure individual routing lists.

None The LU name of the destination resource is compared to the LU names configured in the routing lists. The routing list with the best LU name match is selected, and the next hop CP names from that configured list are placed in the dynamically built list. This is the only source of possible next hop CP names when list dynamics is set to none.

Note that if an LU name does not appear in a routing list the LU will not be reachable by the extended border node when this list dynamics parameter is set to none.

Limited
This augments the list of next hop CP names obtained from the best match configured routing list with CP names obtained from the extended border node's knowledge of existing resources and topology. These additional CP names are obtained by:

- Adding all native extended border nodes
- Adding all non-native, adjacent extended border nodes and network nodes with NETIDs that match the NETID of the destination resource.
- Examining the table of resources already known to the extended border node due to the receipt of a find or found GDS variable. These resources are cached in the Directory Services database. For any entries where the Netid of the cached LU is the same as the destination of the current search, add the NNs of the cached LU to the list of next-hop CPs.

  None of these dynamically obtained next-hop CP names are permanently saved with the configuration data. The list is recreated whenever a resource needs to be located.

Full This functions the same as Limited, except the restriction on matching NETIDs is removed when adding all non-native, adjacent extended border nodes and network nodes.

If *list optimization* is enabled, the reordering process described on page 25 is repeated a second time and the CP names obtained from configured data are also eligible to be reordered.

If *load balance* across parallel inter-subnet boundaries is enabled, the router will attempt to balance the number of sessions across two or more parallel inter-subnet exit points. The relevant configuration has two or more routers serving as EBN exit points in one subnet, with the same number in the other subnet. Each router has an inter-subnet TG to a different router in the other subnet, forming two or more parallel links. (Note that these are not parallel TGs between any two routers.)

To enable this load balancing function, you must configure routing lists in each EBN router, so that sessions for different destination LU names have different preferred exit EBNs. You also configure the preferred inter-subnet boundary and can set backup paths.

Add port

If extended border node is enabled, two additional prompts are presented when you invoke the add port menu item. Both of these new items establish the default for analogous parameters at the link level. The values of these parameters at the link level determine link station behavior.

Subnetwork visit count is the first of these, and describes the same concept as defined at the node level. When a port is first configured this parameter is initialized to the node setting. With this parameter you allow individual ports to deviate from the node level setting.

Adjacent subnetwork affiliation is controlled by the other new extended border node prompt. This allows you to define whether or not the adjacent node is in the same network as the extended border node. The value specified here will be used as the default value for all links through the port. Allowed values are:

Native Adjacent node is in the same topology subnetwork as the extended border node.

Non-native
Adjacent node is not part of the extended border node's topology subnetwork.

Negotiable
Adjacent node may or may not be in the same topology subnetwork depending upon how the adjacent node is defined. The adjacent node is in the extended border node's topology subnetwork unless the adjacent node's corresponding link definition is one of:
- Non-native
- Negotiable and the adjacent node has a different network name
- Negotiable and the adjacent node has defined the link as non-native

Add link

If extended border node is enabled the same two additional prompts are presented when you invoke the add link menu item as were previously presented under add port.

Subnetwork visit count and *adjacent subnetwork affiliation* are the same concept as defined at the port level. They are initialized to the corresponding port setting when a link is first configured. You change the value here if you want different links to have different values even though they are on the same port.

Add Routing Lists

A configured routing list allows you to explicitly define one or more possible next hop CPs for one or more destination resources (LUs). A wildcard character "*" may be used when defining the LU names to reduce the amount of configured data. You can also vary some of the node level defaults for a given routing list.

You can define multiple routing lists. Typically a group of LUs with similar routing requirements would be configured into a single routing list. Additional groups of LUs, each group with its own routing requirements, would be configured into additional routing lists.

There are limits on the number of LU names and number of CP names used in routing lists. These limits vary according to the model router you have. See Table 35 on page 185 for the configuration command detail. Limits have been set to allow as much flexibility as possible in various environments. The ability of the router to handle the specification of many routing lists, each with many LU names and CP names, is limited by the availability of configuration nonvolatile memory, router memory, and APPN shared memory. See “APPN Node Tuning” on page 32 for a discussion of the APPN tuning parameters which control the amount of shared memory.

Recall from the discussion under the set node prompt that configured routing lists are never modified by operational code. When the extended border node uses a given routing list it copies the next hop CP names into a temporary routing list. This temporary dynamic routing list is augmented with dynamic entries as allowed by your configuration setting of the list dynamics parameter. This temporary list is short lived, and is discarded once the destination resource is found or the list is exhausted.

The *routing list name* is the first prompt you see when adding or modifying a routing list. This name is not used by the operational code at all. It’s purpose is to allow you to identify a specific routing list if you want to modify it or delete it at some later time.

Subnetwork visit count and *list optimization* are the next two prompts, and follow the same concept as the analogous parameters defined at the node level. A new routing list initializes these values with the current node level settings. You change these values for individual routing lists as your requirements dictate.

Destination LU prompt(s) are next. Here you may configure at least one, and optionally more, destination resources. Any of the FQLU names may be prematurely terminated with a trailing wildcard “*” to identify a group of LUs. You may not imbed a “*” in the middle of an FQLU name.

One of your routing lists may specify a standalone “*” as one of the destination LUs. If this is done, then that routing list is known as the default routing list, and it will be used by the extended border node for all destination LUs that do not better match the LUs specified in the other routing lists. This list is also used to find LUs when INAUTHENTIC NETID is indicated.

When modifying an existing routing list with many LU names the process of stepping through the LU names could be quite tedious. There are a number of shortcut keys defined to help speed stepping through an existing list of names. Those shortcut keys are defined in the section with the configuration command detail.

Routing CP prompts are the last part of entering a routing list. Here you supply the names of one or more CPs that may know how to reach the configured list of LUs. Along with each CP name you may configure an optional subnetwork visit count. This allows you to specify a different maximum number of subnetworks a session may traverse for different CPs.

In addition to explicitly configuring FQCP names there are a couple of keywords defined that equate to the local node’s CP name, all native extended border nodes, etc. See the section with configuration command detail for those keywords.

As with the LU name list, the same shortcut keys are available to speed stepping through an existing CP name list.

Add CoS Mapping Table

The class of service mapping table allows for the conversion of non-native CoS names to native CoS names and vice versa. Non-native networks using the same

CoS names as the extended border node's native network need not have a CoS mapping table defined. If only some of the non-native CoS names differ from the native CoS names, then only those that differ should be configured in a CoS mapping table.

A given CoS mapping table may apply to a single or multiple non-native networks. You may configure multiple CoS mapping tables as necessary.

There are limits on the number of non-native network names used in CoS mapping tables. These limits vary according to the model router you have. See Table 36 on page 189 for the configuration command detail. Limits have been set to allow as much flexibility as possible in various environments. The ability of the router to handle the specification of many CoS mapping tables, each with many non-native network names and CoS name pairs, is limited by the availability of configuration nonvolatile memory, router memory, and APPN shared memory. See "APPN Node Tuning" on page 32 for a discussion of the APPN tuning parameters which control the amount of APPN shared memory.

CoS mapping table name is the first prompt. As with the analogous name for routing lists, this parameter is not used by the operational code. It's purpose is to allow you to refer to a specific CoS mapping table so that you can modify or delete it. Different CoS mapping tables must have different names, but a given CoS mapping table may have an identical name as a routing list.

Non-native CP name(s) are prompted for next. These are use to specify the non-native network(s) that this CoS mapping table applies to.

As with LU names in a routing list, you may prematurely terminate any of the FQCP names at any point with a trailing wildcard "*" . This allows you to specify a range of non-native FQCP names in one or more non-native networks. You may not imbed a wildcard in the middle of a FQCP name.

One CoS mapping table in the extended border node may have a standalone wildcard "*" as one of the non-native CP names. Such a table is known as the *default CoS mapping table*, and will be the table used by the extended border node whenever no other table has a CP name that matches the non-native network.

CoS name pairs are the final part of configuring a CoS mapping table. Here you are prompted for one or more pairs of CoS names. Each CoS name pair consists of a native CoS name followed by the corresponding CoS name used in the non-native network.

The extended border node uses this table to translate from native to non-native networks and vise versa. If you need to map multiple native CoS names into a common non-native CoS name you should configure one CoS name pair for each possible mapping. Similarly you may need to map multiple non-native CoS names into a common native CoS name, and that too can be accomplished by configuring a CoS name pair for each possible mapping. If there are multiple possible mappings in a table the extended border node will use the first exact mapping found.

Each CoS mapping table may have one CoS name pair where the non-native CoS name is a wildcard "*" . This is the *default CoS mapping* entry for that table, and it is used to translate all unrecognized non-native CoS names into a single native CoS name. Each CoS mapping table may have one of these default CoS mapping entries. You can never code a "*" as the native CoS name.

High-Performance Routing

See Table 2 on page 19 for a list of ports that support HPR.

See “Configuration Requirements for APPN” on page 20 for information about configuring the protocols that support APPN and HPR routing over direct DLCs 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 2 on page 19 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 32 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 serial port PPP 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 behalf of the APPN.

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 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.
- 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 *IBM SNA APPN Architecture Reference* for a description of standard 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 Configuration Program or **talk 6** option of the command line interface.

  See the Web router support pages for a tool you can use to estimate the memory required for APPN and other router components.
- By selecting values for the *maximum number of ISR sessions*, *maximum number of adjacent nodes* and other parameters shown in Table 9 on page 107, and having the tuning algorithm automatically calculate the *maximum shared memory* and *maximum cached directory entries* tuning parameter values.

  Use the 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. You can allow the router to choose a general-purpose default for this value based on its installed memory.

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 auto-configured default unless you do a more careful analysis using the router storage tool.

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.

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 page 132 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 15 on page 129 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 Talk 6 **set management** 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 *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 Step 5 to Step 7 as long as the DSPU is requesting ACTPU.
  5. Wait for the amount of time specified by the Long retry timer parameter.

     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 to 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 to 7 as long as the DSPU is requesting ACTPU.
5. Wait for the amount of time specified by the Long retry timer parameter.

   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 2 on page 37. This support allows customers with DLSw networks to reach APPN without needing an external DLSw router. It also allows remote TN3270 servers to reach the host through subarea DLSw links.

Note: It is recommended to use APPN over direct DLCs when available instead of APPN over DLSw. However, local DLSw is the only way that a remote TN3270 server can use SDLC or X.25 QLLC subarea links to reach the host.

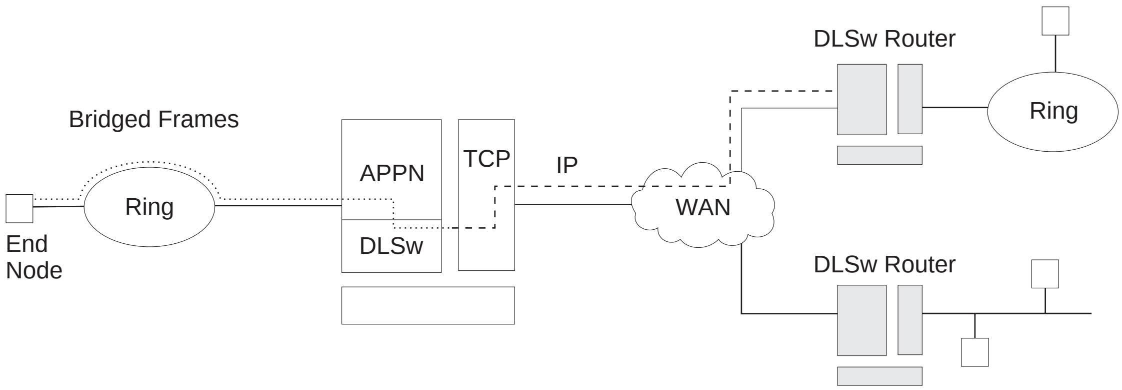


Figure 2. Data Flow in an APPN Configuration Using DLSw Port

APPN configuration restrictions using DLSw:

- Only one DLSw logical 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 21 to configure APPN using DLSw.

How APPN Uses DLSw ports to Transport Data

When APPN is configured on the router to use the Data Link Switching (DLSw) port, DLSw provides a connection-oriented interface (802.2 LLC type 2) between the APPN component in the router and APPN and SNA 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 address and one or more SAP addresses that enable 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. Multiple SAP addresses are required only when you are configuring the TN3270 server to reach the host through DLSw and you need more than one dependent PU.

APPN Frame Relay BAN Connection Network Implementation

The implementation of an APPN Frame Relay BAN connection network allows you to define an APPN Frame Relay port that supports the bridged Frame Relay format (BAN) to a connection network.

A shared-access transport facility (SATF) is a transmission facility, such as token-ring or Ethernet, in which nodes attached to the SATF can achieve any-to-any connectivity. This any-to-any connectivity allows direct connections between two nodes, eliminating routing through intermediate network nodes and the corresponding data traversing the SATF many times. TGs must be defined on each node to all other nodes in order to achieve this direct connectivity.

The SATF shown in Figure 3 on page 38 illustrates that the APPN NN in the router must define a link station to each node on the token-ring in order to initiate a connection to each node on the token-ring. The APPN NN must know the DLCI address for the Frame Relay link and the MAC address of each node on the token-ring. If the nodes on the token-ring want to initiate a connection to the APPN NN, they must define a link station in the APPN NN in the device and specify:

- BAN DLCI MAC address if the device connecting the token-ring to the frame relay network is performing the BAN function
- The Boundary Node Identifier MAC address if the device connecting the token-ring to the Frame Relay network is a bridge

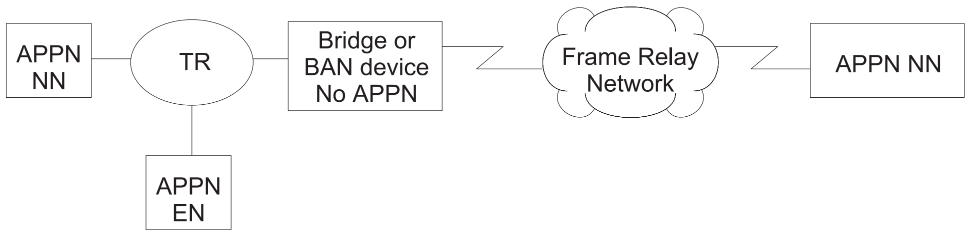


Figure 3. Logical View with Frame Relay Bridged Frame/BAN Connection Network Support

Note: In this diagram and in all the following Frame Relay BAN diagrams, the APPN resides in the 2212.

Defining connections between all possible pairs of nodes attached to the SATF results in a large number of definitions and a large number of topology database update flows on the network. APPN allows nodes to become members of a connection network to represent their attachment to the SATF.

Figure 4 on page 39 shows all nodes as members of the same connection network. Nodes use the connection network to establish communication with all other nodes, removing the necessity of creating connections to all other nodes on the SATF. 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 activated, a connection network TG is created by the APPN component to a Virtual Routing Node (VRN). This TG identifies the direct connection from the port to the connection network. The CP name of the VRN is the connection network name.

Since the connectivity is represented by a TG from a given node to a VRN, normal topology and routing services (TRS) can be used by the network node server to calculate the direct path between any two nodes attached to the 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.

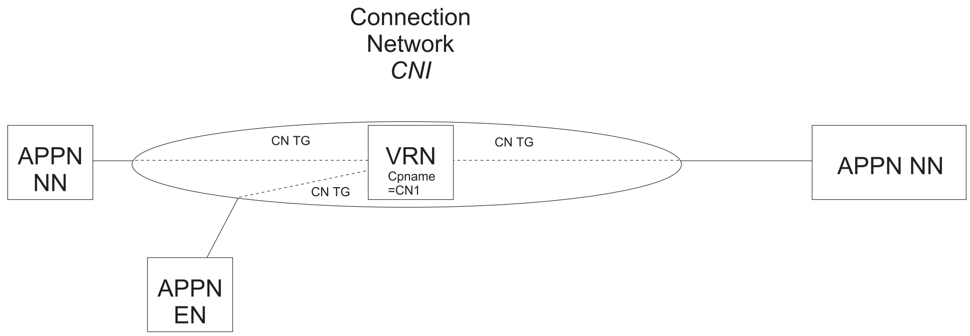


Figure 4. APPN Frame Relay Bridged Frame/BAN Connection Network

The following are limitations on using APPN Frame Relay BAN connection networks:

- The same connection network can be defined on only one SATF.
- All Frame Relay ports belonging to the same connection network on the router must use the same DLCI number to connect to the Frame Relay network.
- When bridging is used instead of BAN, all Frame Relay ports belonging to the same connection network on the router must have the same BNI MAC address/SAP pair defined.
- CP-CP sessions cannot be established over links established through a connection network.

Sample APPN Frame Relay BAN Connection Network Definitions

Example 1

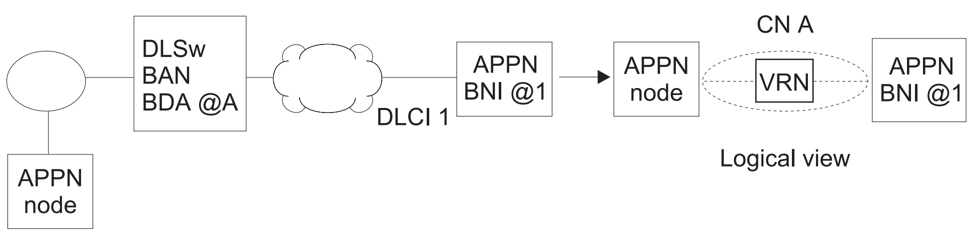


Figure 5. Single Connection Network using BAN with 1 Frame Relay Port

Note: The BDA address must be defined on the connection network definition.

Example 2

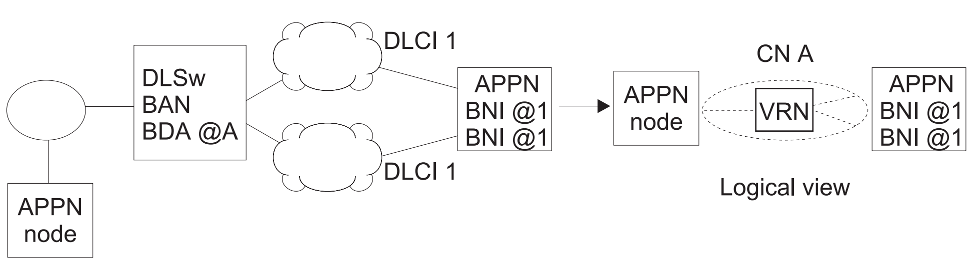


Figure 6. Single Connection Network using BAN with Multiple Frame Relay Ports

Notes:
1. The same DLCI number must be specified on both ports.
2. The BDA address must be defined on the connection network definition.
3. The BNI addressees on both ports can be the same or different.
4. If the APPN node initiates the connection to the device, the APPN port that gets chosen for the connection is dependent upon which port responds first to the test frame.

Example 3

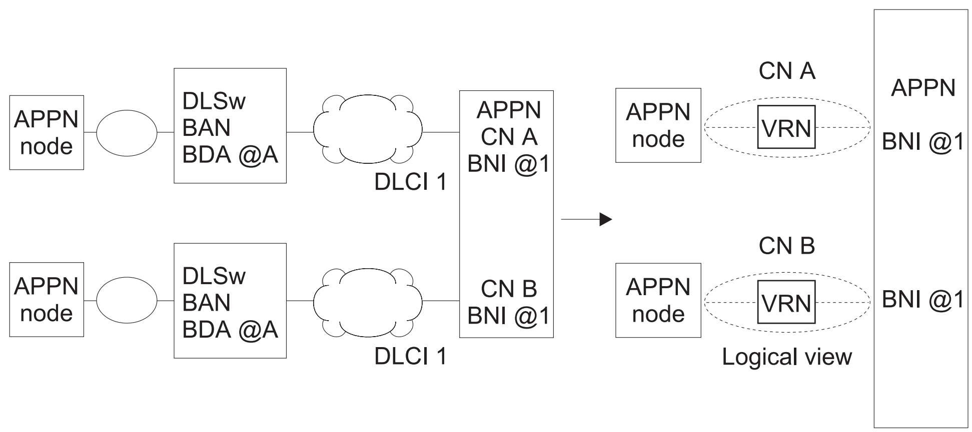


Figure 7. Multiple Connection Networks using BAN

Notes:
1. This configuration requires two connection network definitions since there are two SATFs.
2. The DLCI number specified on the ports can be the same or different.
3. The BDA MAC address must be defined on the connection network definition.
4. The BNI MAC address specified on the ports can be the same or different.

Example 4

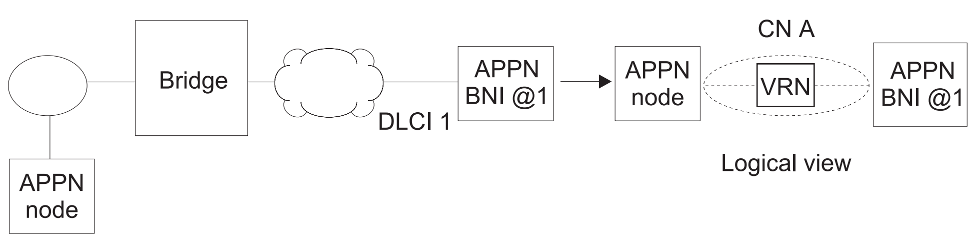


Figure 8. Single Connection Network using Bridging with One Frame Relay Port

Notes:
1. The BDA address is not defined on the connection network definition.

Example 5

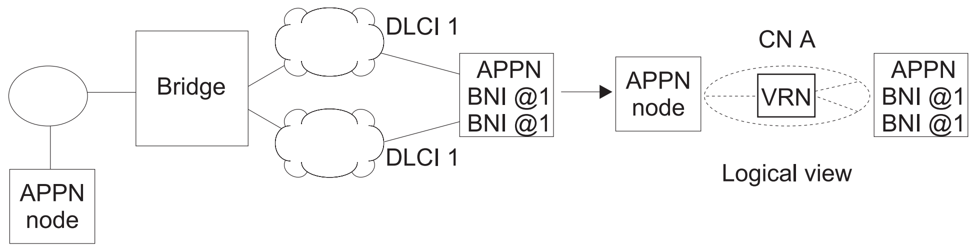


Figure 9. Single Connection Network Using Bridging with Multiple Frame Relay Ports

Notes:
1. The same DLCI number must be specified on both ports.
2. The same BNI MAC address/SAP pair must be specified on both ports.
3. No BDA MAC address is specified on the connection network definition.
4. If the APPN node initiates the connection to the device, the APPN port chosen for the connection depends upon which port responds first to the test frame.

Example 6

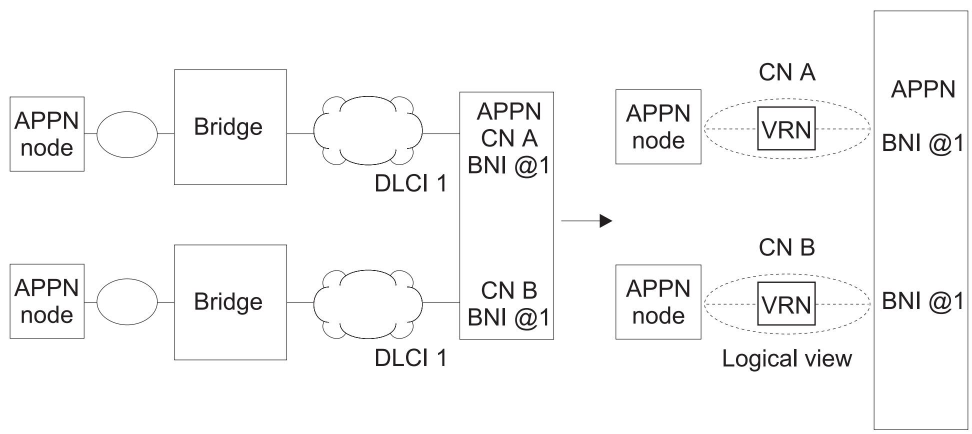


Figure 10. Multiple Connection Networks Using Bridging

Notes:
1. This configuration requires two connection network definitions since there are two SATFs.
2. The DLCI number specified on the ports can be the same or different.
3. The BDA MAC address is not defined on the connection network definition.
4. The BNI MAC address/SAP pair specified on the ports can be the same or different.

Port Level Parameter Lists

Use the following tables to configure APPN ports:

- “Port Configuration” on page 136
- “Port Definition” on page 141
- “Port Default TG Characteristics” on page 145
- “Port default LLC Characteristics” on page 149

Link Level Parameter Lists

Use the following tables to configure APPN link stations:

- "HPR Defaults" on page 152
- "Link Station - Detail" on page 154
- "Modify TG Characteristics" on page 165
- "Modify Dependent LU Server" on page 167
- "Modify LLC Characteristics" on page 168
- "Modify HPR Defaults" on page 171

LU Parameter List

Use the following table to configure an LU:

- "LEN End Node LU Name" on page 173

Node Level Parameter Lists

Use the following tables to configure an APPN node:

- "Local node basic characteristics" on page 93
- "High Performance Routing (HPR)" on page 98
- "HPR Timer and Retry Options" on page 99
- "Dependent LU Requester" on page 102
- "Connection Network - Detail" on page 174
- "TG Characteristics (Connection Network)" on page 176
- "APPN COS - Additional port to CN" on page 180
- "Node Level Traces" on page 112
- "Interprocess Signals Traces" on page 118
- "Module Entry and Exit Traces" on page 122
- "General Component Level Traces" on page 124
- "APPN Node Management" on page 132
- "TN3270E" on page 191
- Table 35 on page 185
- Table 36 on page 189

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 a Permanent Circuit Using ISDN

This example is a configuration of a permanent circuit using Frame Relay over ISDN from node 21 to node 1.

Note: You configure a permanent circuit by setting the idle timer value to 0.

```
************************************************************************
****  Configuring a PERMANENT circuit via ISDN from NN21 to NN1
****  Using Frame Relay over ISDN
************************************************************************

Config>n 6
Circuit configuration
FR Config>li all

 Base net                       = 3
 Destination name               = 2212-01
 Circuit priority               = 8
Destination address: subaddress = 99195551234:

 Inbound destination name       = 2212-01
Inbound dst address: subaddress = 99195551000:

 Inbound calls                  = allowed
 Idle timer                     = 0 (fixed circuit)   1
 SelfTest Delay Timer           = 150 ms

FR Config>ex

************************************************************************
**** Verify that a FR PVC is defined to NN1. This is required for APPN
************************************************************************

Config>n 6
Circuit configuration
FR Config>en
Frame Relay user configuration
FR Config>li perm

  Maximum PVCs allowable =      64
  Total PVCs configured  =       1

             Circuit              Circuit   Circuit   CIR     Burst  Excess
              Name                Number     Type    in bps   Size   Burst
 ------------------------------- ------- ---------- ------- ------- -------
2212-21-i6          2              16     Permanent 64000    64000     0

  = circuit is required and belongs to a required PVC group

FR Config>ex
Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC,  (S)DLC, (X)25,  (FD)DI, (D)LSw, (A)TM, (IP) [  ] ? f
Interface number(Default 0): [0 ] ? 6
Port name (Max 8 characters) [FR006 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
 Service any node: (Y)es (N)o [Y ] ?
 Limited resource: (Y)es (N)o [N ] ?
 High performance routing: (Y)es (N)o [Y ] ?
 Maximum BTU size (768-2044) [2044 ] ?
 Percent of link stations reserved for incoming calls (0-100) [0 ] ?
 Percent of link stations reserved for outcoming calls (0-100) [0 ] ?
 Local SAP address (04-EC) [4 ] ?
 Support bridged formatted frames: (Y)es (N)o [N ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>add li
APPN Station
Port name for the link station [  ] ? fr006
Station name (Max 8 characters) [  ] ? tonn1isdn
Station name (Max 8 characters) [  ] ? tonn1is
 Limited resource: (Y)es (N)o [N ] ?
 Activate link automatically (Y)es (N)o [Y ] ?
 DLCI number for link (16-1007) [16 ] ?
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0 ] ?
 High performance routing: (Y)es (N)o [Y ] ?
```

```
Edit Dependent LU Server: (Y)es (N)o [N ] ?
 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 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>ex

APPN config>li all
NODE:
        NETWORK ID: STFNET
        CONTROL POINT NAME: NN21
        XID: 00000
        APPN ENABLED: YES
        MAX SHARED MEMORY: 4096
        MAX CACHED: 4000
DLUR:
        DLUR ENABLED: YES
        PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
              CN NAME       LINK TYPE  PORT INTERFACES
        ------------------------------------------------------------
COS:
        COS NAME
        --------
           BATCH
         BATCHSC
         CONNECT
           INTER
         INTERSC
         CPSVCMG
        SNASVCMG
          USRBAT
          USRNOT
MODE:
         MODE NAME  COS NAME
        ---------------------
         #USRBAT     #USRBAT
         #USRNOT     #USRNOT
PORT:
          INTF     PORT      LINK      HPR    SERVICE   PORT
         NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
        ------------------------------------------------------
            0      TR000   IBMTRNET    YES      YES      YES
            1    SDLC001       SDLC     NO      YES      YES
          254     DLS254        DLS     NO      YES      YES
            6      FR006         FR    YES      YES      YES  3
STATION:
         STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
          NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
        -----------------------------------------------------------
          TONN25    TR000    0004ACA2A407       YES     YES       0
          TONN31    TR000    4FFF00001031       YES      NO       0
           SDLC1  SDLC001              C1        NO      NO       2
         TONN103   DLS254    400000000103        NO      NO       0
         TONN1IS    FR006              16       YES     YES       0  4
LU NAME:
              LU NAME        STATION NAME          CP NAME
        -----------------------------------------------------------
APPN config>
```

Note:

1 Idle timer = 0 gives a fixed circuit
2 Frame relay PVC is defined
3 This is the ISDN port
4 This is the link station

Configuring APPN Over Dial on Demand Circuits

APPN is supported over dial on demand circuits for the following DLC types:

- APPN/PPP/ISDN
- APPN/FR/ISDN
- APPN/PPP/V.25 bis

- APPN/PPP/V.34

Refer to the *Software User’s Guide* for additional information about dial on demand circuits.

PU 2.1 Node Considerations

When configuring an APPN link station for PU 2.1 nodes over a Dial on Demand link, you should specify yes for the *limited resource* link station parameter. This allows APPN to:

- Consider this link as a viable link to be used for route computation, even though the link is not actually active. The link will automatically become active during LU-LU session activation for a session needing to use it.
- Deactivate the link station when there are no active sessions using this link.

You should not configure CP-CP sessions over a dial on demand link. CP-CP sessions are persistent sessions. That is, they should remain active as long as the link is active. Since the active session count will not go to zero in this case, the link will remain active.

Note: If you specify yes for the *limited resource* parameter for a PU 2.1 node, you must specify an adjacent CPNAME and a TG number in the range of 1 to 20.

PU 2.0 Node Considerations

When configuring an APPN link station for PU 2.0 nodes over a Dial on Demand link, you can specify yes for the *limited resource* link station parameter. This allows APPN to deactivate the link station when there are no active sessions using it.

Note: If *limited resource* is yes, link activation for this link station must be initiated by either the DSPU (the PU 2.0) or by VTAM.

Considerations When Using DLUR for T2.0 or T2.1 Devices

For T2.0 or T2.1 nodes utilizing DLUR for dependent session traffic, an SSCP-PU and an SSCP-LU session must be active in order to establish an LU-LU session. These sessions are included in the session count for the link to the DSPU. Therefore, if *limited resource* is yes, the link will remain active as long as the SSCP-PU session is active or LU-LU sessions are active over this link.

If you specify no for the *limited resource* parameter, link deactivation is controlled by the node that initiated the connection.

If the link to the DSPU was activated due to the DSPU calling into the DLUR node or the DLUR node calling out to the DSPU (i.e. the link station to the DSPU has been configured in the router and *activate link automatically* is yes), when the active session count goes to zero the link is deactivated by APPN DLUR only if the DSPU requested DACTPU. In this case, if the DLUS sends a DACTPU request to DLUR, DLUR will deactivate the SSCP-PU session. However, it will not deactivate the link to the DSPU. DLUR will attempt to reestablish the SSCP-PU session to the DLUS or the backup DLUS until it is successful or until the DSPU no longer needs this session.

If the link to the DSPU was activated by the DLUS and the session count goes to zero, the link is deactivated by APPN DLUR only if the DLUS sends a DACTPU request to DLUR.

The following is a dial on demand configuration example. This configuration is similar to the ISDN permanent connection except:

- You must specify that the link is a limited resource.
- You must define the adjacent CP name.
- You must specify a TG number.

You configure both sides of the communication link the same way.

Note: If you allow CP-CP sessions on this link, the link will not disconnect.

```
*t 6
Gateway user configuration
Config>
**************************************************************************
****  This is the NN6 configuration for a   NN6----NN15  dial on demand link.
****  The NN15 config will look just like this.
****  interface 9 is a Dial On Demand link with destination = NN15

**************************************************************************
Config>n 9
Circuit configuration
FR Config>li all

Base net                       = 6
Destination name               = 2212-15
Circuit priority               = 8

Inbound destination name       = 2212-15

Inbound calls                  = allowed
Idle timer                     = 60 sec  1
SelfTest Delay Timer           = 150 ms

FR Config>ex

**************************************************************************
**** Configure APPN Port for the  Interface
**************************************************************************

Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC,  (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (IP) [  ] ? p
Interface number(Default 0): [0 ] ? 9
Port name (Max 8 characters) [PPP009 ] ?

Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
 Service any node: (Y)es (N)o [Y ] ?
 Limited resource: (Y)es (N)o [Y ] ?  2
 ****  note that limited resource = YES
 High performance routing: (Y)es (N)o [Y ] ?
 Maximum BTU size (768-2044) [2044 ] ?
 Local SAP address (04-EC) [4 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.

**************************************************************************
**** Configure the linkstation for the DOD link to NN15
**************************************************************************
APPN config>add li
APPN Station
Port name for the link station [  ] ? ppp009
Station name (Max 8 characters) [  ] ? to15dod
 Limited resource: (Y)es (N)o [Y ] ?  2
**** < note limited resource= YES
 TG Number (1-20) [1 ] ?    3
**** < note TG number is required input for limited resource
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node [0 ] ?
 High performance routing: (Y)es (N)o [Y ] ?
 Allow CP-CP sessions on this link (Y)es (N)o [Y ] ? N  4
**** < Be sure to NOT allow CP-CP sessions, or link won't hang up
Fully-qualified CP name of adjacent node (netID.CPname) [ ] ? stfnet.NN15
**** < Adjacent node name required for limited resource links 5
Edit TG Characteristics: (Y)es (N)o [N ] ?
```

```
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>li all
NODE:
 NETWORK ID: STFNET
 CONTROL POINT NAME: NN6
 XID: 00000
 APPN ENABLED: YES
 MAX SHARED MEMORY: 4096
 MAX CACHED: 4000
DLUR:
 DLUR ENABLED: YES
 PRIMARY DLUS NAME: NETB.MVSC

 CONNECTION NETWORK:
       CN NAME       LINK TYPE  PORT INTERFACES
 ------------------------------------------------------------
 COS:
 COS NAME
 --------
BATCH
BATCHSC
CONNECT
INTER
INTERSC
CPSVCMG
SNASVCMG
USRBAT
USRNOT

MODE:
  MODE NAME  COS NAME
 ---------------------
   USRBAT      USRBAT
   USRNOT      USRNOT
 PORT:
   INTF     PORT      LINK      HPR    SERVICE   PORT
  NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
 ------------------------------------------------------
     0      TR000   IBMTRNET    YES      YES      YES
     1     PPP001        PPP    YES      YES      YES
     2         SS       SDLC     NO      YES      YES
     3                  SDLC     NO      YES       NO
     4                   PPP    YES      YES       NO
     5      TR005   IBMTRNET    YES      YES      YES
   254                   DLS     NO      YES       NO
    17     PPP017        PPP    YES      YES      YES
     9     PPP009        PPP    YES      YES      YES   6
 STATION:
  STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
   NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
 ------------------------------------------------------------
    TONN1    TR000    0004AC4E7505       YES     YES       1
    TONN2    TR000    550020004020       YES     YES       1
    TONN9    TR000    0004AC4E951D       YES     YES       1
    TOPC4    TR000    0004AC9416B4       YES     YES       1
  TOVTAM1    TR000    400000003888       YES     YES       1
   TONN35   PPP001    000000000000       YES     YES       0
  TO15DOD   PPP009    000000000000       YES      NO       0   7
 LU NAME:
       LU NAME         STATION NAME           CP NAME
 ------------------------------------------------------------
```

Note:

- 1 Idle timer > 0 means dial on demand
- 2 This is a limited resource
- 3 TG number is required for a limited resource
- 4 Do not allow CP-CP sessions on this link
- 5 Provide a fully-qualified CP name
- 6 This is the port
- 7 This is the link station

Configuring WAN Reroute

WAN reroute lets you set up an alternate route so that if a primary link fails, the router automatically initiates a new connection to the destination through the alternate route.

You can use any type of link as the alternate link and any type of link as the primary link. The alternate link does not need to be connected to the same end point as the primary link.

If HPR is used on the primary link and alternate link, when the primary link fails, HPR's Non-disruptive Path Switch function will automatically reroute traffic to the alternate link without disrupting end user sessions.

In this configuration example, the router performing the WAN reroute function is configured with two APPN link station definitions; one link station is defined over the primary interface and the other is over the alternate interface. The destination router needs to have APPN enabled on the port. If the destination router has a link station defined, that link station should not try to bring up the connection in order to avoid extra traffic.

In this example, Frame Relay is the primary route from NN22 to NN6.

```
*************************************************************************
**** The configuration is  NN22---primary FR
****                           ---Alternate WRR to NN6
*************************************************************************
****
**** This is the NN22 configuration
*************************************************************************
```

```
Ifc 0 Token Ring                    Slot: 1   Port: 1
Ifc 1 V.35/V.36 Frame Relay         Slot: 8   Port: 0
Ifc 2 V.35/V.36 Frame Relay         Slot: 8   Port: 1
Ifc 3 ISDN Primary T1/J1            Slot: 7   Port: 1
Ifc 4 PPP Dial Circuit
       (Disabled)
Ifc 5 PPP Dial Circuit
       (Disabled)
Ifc 6 Frame Relay Dial Circuit
       (Disabled)
*************************************************************************
* Ifc 4 is the ALTERNATE with Ifc 1 configured as PRIMARY.
* Note that interface 4 should be 'Disabled' here.
* Wan Reroute function will 'Enable' it when the
* Primary fails
*
* NN6 (2212-06) is going the be the destination of the Wan Reroute
*************************************************************************
Config>n 4
Circuit configuration
FR Config>li

 Base net                       = 3
 Destination name               = 2212-06  3
 Circuit priority               = 8
Destination address: subaddress = 99199991201:

 Outbound calls                 = allowed
 Idle timer                     = 0 (fixed circuit)
 SelfTest Delay Timer           = 150 ms
```

```
Config>ex
**************************************************************************
*
**** Configure the Wan Reroute Primary and Alternate circuit
*
**************************************************************************
Config>fea wan  4
WAN Restoral user configuration
WRS Config>en wrs
WRS Config>add alt
Alternate interface number  [0 ] ? 4  2
Primary interface number  [0 ] ? 1  1
WRS Config>li all

WAN Restoral is enabled.
Default Stabilization Time:       0 seconds
Default First Stabilization Time: 0 seconds

[No Primary-Secondary pairs defined ]
                       Alt.     1st  Subseq TOD Revert Back
Primary Interface  Alternate Interface     Enabled  Stab  Stab  Start    Stop
-----------------  ----------------------  -------  ----  ----  -------  -------
 1 - WAN Frame Re   4 - PPP Dial Circuit     No     dflt  dflt  Not Set  Not Set


**************************************************************************
*
**** Set Default and first stabilization times
*
**************************************************************************
*
WRS Config>set default firs 30
WRS Config>set def stab 10
WRS Config>li all
WAN Restoral is enabled.
Default Stabilization Time:       10 seconds
Default First Stabilization Time: 30 seconds
[No Primary-Secondary pairs defined ]
                       Alt.     1st  Subseq TOD Revert Back
Primary Interface  Alternate Interface     Enabled  Stab  Stab  Start    Stop
-----------------  ----------------------  -------  ----  ----  -------  -------
 1 - WAN Frame Re   4 - PPP Dial Circuit     No     dflt  dflt  Not Set  Not Set

WRS Config>en alt
Alternate interface number  [0 ] ? 4
WRS Config>ex

**************************************************************************
*
*Configure APPN PORTS and LINKSTATIONS for the
*ALTERNATE and PRIMARY interfaces
**************************************************************************
Config>p appn
APPN user configuration
APPN config>add p  5
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC,  (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (IP) [  ] ? p
Interface number(Default 0): [0 ] ? 4
Port name (Max 8 characters) [PPP004 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?
Port Definition
 Service any node: (Y)es (N)o [Y ] ?
 Limited resource: (Y)es (N)o [N ] ?
 High performance routing: (Y)es (N)o [Y ] ?
 Maximum BTU size (768-2044) [2044 ] ?
 Local SAP address (04-EC) [4 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>add li  6
APPN Station
Port name for the link station [  ] ? ppp004
Station name (Max 8 characters) [  ] ? toNN6WRR
 Limited resource: (Y)es (N)o [N ] ?
 Activate link automatically (Y)es (N)o [Y ] ?
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node [0 ] ?
```

```
 High performance routing: (Y)es (N)o [Y ] ?
 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 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
APPN config>add li   6
APPN Station
Port name for the link station [  ] ? fr001
Station name (Max 8 characters) [  ] ? tonn1pri
 Activate link automatically (Y)es (N)o [Y ] ?
 DLCI number for link (16-1007) [16 ] ? 121
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node [0 ] ?
 High performance routing: (Y)es (N)o [Y ] ?
 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 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.

 APPN config>li all
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN22
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
 DLUR:
  DLUR ENABLED: NO
  PRIMARY DLUS NAME:
 CONNECTION NETWORK:
        CN NAME       LINK TYPE  PORT INTERFACES
  -------------------------------------------------------------
 COS:
  COS NAME
  --------
    BATCH
  BATCHSC
  CONNECT
    INTER
  INTERSC
  CPSVCMG
 SNASVCMG
   MODE NAME  COS NAME
  ---------------------
 PORT:
    INTF     PORT      LINK      HPR    SERVICE   PORT
   NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
  ------------------------------------------------------
      0      TR000   IBMTRNET    YES      YES      YES
**** < this is the Primary port
      1      FR001         FR    YES      YES      YES 7
**** < this is the alternate port
      4     PPP004        PPP    YES      YES      YES    8
 STATION:
   STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
    NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
  ------------------------------------------------------------
    TONN25    FR001            132        YES     YES      0
    TONN31    FR001            141        YES      NO      0
   TONN103    FR001            153        YES      NO      0
**** < this is the alternate to NN6
  TONN6WRR   PPP004    000000000000       YES     YES      0  9
**** < this is the Primary to NN1
  TONN1PRI    FR001            121        YES     YES      0  10
 LU NAME:
        LU NAME         STATION NAME          CP NAME
  ------------------------------------------------------------
 APPN config> ex
```

```
*************************************************************************
*************************************************************************
*************************************************************************
Config>
*************************************************************************
**** The configuration is  NN22---primary FR
****                           ---Alternate WRR to NN6
****
** This is the NN6 configuration which is the destination side for the
*  NN22 Wan Reroute
*  interface 17 has the ISDN lid for 2212-22 so when NN22 calls into NN6,
*  it will map to interface 17
*
*************************************************************************
 11
Config> n 17
Circuit configuration
FR Config>fea      li all

Base net                       = 6
Destination name               = 2212-22
Circuit priority               = 8

Inbound destination name       = 2212-22

Inbound calls                  = allowed
Idle timer                     = 0 (fixed circuit)
SelfTest Delay Timer           = 150 ms

FR Config>ex
**** on this side, the interface must be ENABLED all the time
Config>ena in 17
Interface enabled successfully

*************************************************************************
* Define the APPN PORT; NN22 will call into NN6 and dynamically create
* the linkstation when NN22 does a Wan Reroute.
*
*************************************************************************
Config>p appn
APPN user configuration
APPN config>add p        12
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC,  (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (IP) [  ] ? p
Interface number(Default 0): [0 ] ? 17
Port name (Max 8 characters) [PPP017 ] ?
Enable APPN on this port (Y)es (N)o [Y ] ?

Port Definition
 Service any node: (Y)es (N)o [Y ] ?
 Limited resource: (Y)es (N)o [N ] ?
 High performance routing: (Y)es (N)o [Y ] ?
 Maximum BTU size (768-2044) [2044 ] ?
 Local SAP address (04-EC) [4 ] ?
Edit TG Characteristics: (Y)es (N)o [N ] ?
Edit LLC Characteristics: (Y)es (N)o [N ] ?
Edit HPR defaults: (Y)es (N)o [N ] ?
Write this record? [Y ] ?
The record has been written.
 APPN config>li al
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN6
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
 DLUR:
  DLUR ENABLED: YES
  PRIMARY DLUS NAME: NETB.MVSC
 CONNECTION NETWORK:
        CN NAME       LINK TYPE  PORT INTERFACES
  -------------------------------------------------------------
 COS:
  COS NAME
  --------
    BATCH
  BATCHSC
  CONNECT
```

```
    INTER
  INTERSC
  CPSVCMG
 SNASVCMG
   USRNOT
 MODE:
   MODE NAME  COS NAME
  ---------------------
    USRBAT      USRBAT
    USRNOT      USRNOT

 PORT:
    INTF     PORT      LINK      HPR    SERVICE   PORT
   NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
  -----------------------------------------------------
      0      TR000   IBMTRNET    YES      YES      YES
      1     PPP001        PPP    YES      YES      YES
      2         SS       SDLC     NO      YES      YES
      3                  SDLC     NO      YES       NO
      4                   PPP    YES      YES       NO
      5      TR005   IBMTRNET    YES      YES      YES
    254                   DLS     NO      YES       NO
     17     PPP017        PPP    YES      YES      YES
 STATION:
   STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
    NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
  -----------------------------------------------------------
     TONN1    TR000    0004AC4E7505       YES     YES       1
     TONN2    TR000    550020004020       YES     YES       1
     TONN9    TR000    0004AC4E951D       YES     YES       1
     TOPC4    TR000    0004AC9416B4       YES     YES       1
   TOVTAM1    TR000    400000003888       YES     YES       1
    TONN35   PPP001    000000000000       YES     YES       0
 LU NAME:
       LU NAME         STATION NAME           CP NAME
  -----------------------------------------------------------
 APPN config>
```

Note:

1 The primary route is interface 1, Frame Relay
2 The alternate route is interface 4 and is disabled
3 Destination of WAN reroute is NN6
4 Configure WAN reroute primary and alternate
5 Add the APPN port to NN22
6 Link station on APPN port (NN22)
7 Primary port
8 Alternate port
9 Alternate station to NN6
10 Primary station to NN6
11 Destination configuration
12 APPN port on destination; link station will be dynamically created when WAN reroute occurs.

Configuring WAN Restoral

The following example shows APPN over a primary PPP link. For APPN, no unique definitions are needed. Both sides of the communication link are enabled for WAN restoral and are similarly configured.

```
*************************************************************************
*** Configuration of NN6 with a Wan Restoral link to NN35
*** interface 1 is the primary, interface 8 is the Secondary
*** NN35 must also have Wan Restoral configured for its primary/secondary
*** interfaces
**** Note that for APPN, there are NO unique definitions needed.
*************************************************************************

Circuit configuration
FR Config>li al

Base net                       = 6
Destination name               = 2212-35
```

```
Circuit priority              = 8

Inbound destination name      = 2212-35

Inbound calls                 = allowed
Idle timer                    = 0 (fixed circuit)
SelfTest Delay Timer          = 150 ms

FR Config>ex
Config>fea wan
WAN Restoral user configuration
WRS Config>li all

WAN Restoral is enabled.      1
Default Stabilization Time:       0 seconds
Default First Stabilization Time: 0 seconds

                                                     Secondary
   Primary Interface       Secondary Interface     Enabled
-----------------------  -----------------------  --------
 1 - WAN PPP             8 - PPP Dial Circuit       Yes
[No Primary-Alternate pairs defined ]
WRS Config>ex
Config>p appn
APPN user configuration
APPN config>li al
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN6
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
 DLUR:
  DLUR ENABLED: YES
  PRIMARY DLUS NAME: NETB.MVSC
 CONNECTION NETWORK:
        CN NAME       LINK TYPE  PORT INTERFACES
  -------------------------------------------------------------
 COS:
  COS NAME
  --------
    BATCH
  BATCHSC
  CONNECT
    INTER
  INTERSC
  CPSVCMG
 SNASVCMG
 USRBAT
    USRNOT
 MODE:
   MODE NAME  COS NAME
  --------------------
    USRBAT      USRBAT
    USRNOT      USRNOT
 PORT:
    INTF     PORT      LINK      HPR    SERVICE   PORT
   NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
  ------------------------------------------------------
      0      TR000   IBMTRNET    YES      YES      YES
**** < This is the port that will get backed up
      1     PPP001        PPP    YES      YES      YES  2
      2         SS       SDLC     NO      YES      YES
      3                  SDLC     NO      YES       NO
      4                   PPP    YES      YES       NO
      5      TR005   IBMTRNET    YES      YES      YES
    254                   DLS     NO      YES       NO
     17     PPP017        PPP    YES      YES      YES
      9     PPP009        PPP    YES      YES      YES

 STATION:
   STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
    NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
  ------------------------------------------------------------
     TONN1    TR000    0004AC4E7505       YES     YES       1
     TONN2    TR000    550020004020       YES     YES       1
     TONN9    TR000    0004AC4E951D       YES     YES       1
     TOPC4    TR000    0004AC9416B4       YES     YES       1
   TOVTAM1    TR000    400000003888       YES     YES       1
```

```
**** < this linkstation will get backed up
    TONN35   PPP001    000000000000       YES     YES       0 3
   TO15DOD   PPP009    000000000000       YES      NO       0
 LU NAME:
        LU NAME         STATION NAME           CP NAME
  ------------------------------------------------------------
 APPN config>ex
Config>
*logout
Connection closed.
```

Note:

1 WAN restoral is enabled on both sides.
2 Port that will get backed up
3 Link station that will get backed up

Configuring V.25 bis

The following is a sample V.25 bis configuration that could be used when APPN traffic uses PPP over V.25 bis:

```
Config> list device


Ifc 2 WAN V.25bis              CSR 81640, CSR2 80E00, vector 92
Ifc 0 Token Ring                      Slot: 1   Port: 1
Ifc 1 EIA-232E/V.24 PPP               Slot: 8   Port: 0
Ifc 2 EIA-232E/V.24 X.25              Slot: 8   Port: 1
Config>set data v25 2.
Config>list device



Ifc 0 Token Ring                      Slot: 1   Port: 1
Ifc 1 EIA-232E/V.24 PPP               Slot: 8   Port: 0
Ifc 2 EIA-232E/V.24 V.25bis           Slot: 8   Port: 1
Config>add v25
Assign address name (1-23) chars []? brown
Assign network dial address (1-30 digits) []? 555-1211
Assign address name (1-23) chars []? gray
Assign network dial address (1-30 digits) []? 555-1212
Config>list v25

Address assigned name             Network Address
---------------------             ---------------

brown                             555-1211
gray                              555-1212
Config>add device dial
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use net 3 command to configure circuit parameters
Config>net 3
Circuit configuration
Circuit config:   3>list all.

Base net                       = 0
Destination name               =
Circuit priority               = 8

Outbound calls                 = allowed
Inbound calls                  = allowed
Idle timer                     = 60 sec    1
SelfTest Delay Timer           = 150 ms

Circuit config:   3>set net
Base net for this circuit [0]? 2
Circuit config:   3>set idle 0             2
Circuit config:   3>set dest
Assign destination address name []? brown

Circuit config:   3>list all


 Base net                       = 2
 Destination name               = brown
 Circuit priority               = 8
```

```
Destination address: subaddress = 555-1211

 Outbound calls                 = allowed
 Inbound calls                  = allowed
 Idle timer                     = 0 (fixed circuit)
 SelfTest Delay Timer           = 150 ms

Circuit config:   3>ex
Config>net 2
V.25bis Data Link Configuration
V25bis Config>list all
         V.25bis Configuration
Local Network Address Name    = Unassigned
No local addresses configured

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Cable type                    = RS-232 DTE

Speed (bps)                   = 9600
V25bis Config>set local
Local network address name   []? gray
V25bis Config>list all
         V.25bis Configuration
Local Network Address Name    = gray
Local Network Address         = 555-1212

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Cable type                    = RS-232 DTE

Speed (bps)                   = 9600
V25bis Config>
```

Note:

1 A non-zero value for Idle Timer results in a dial-on-demand link

2 A zero value results in a leased link

Configuring APPN Using SDLC

APPN supports the following SDLC stations:

- Primary point-to-point
- Secondary point-to-point
- Negotiable point-to-point
- Primary multipoint
- Secondary point-to-point (multi-APPN link stations)

Using the **talk 5** command interface for SDLC, you can:

- Enable/disable a SDLC link
- Update SDLC station parameters.

In order to activate an APPN connection to the remote SDLC link station, you must configure and activate the APPN SDLC link station in the router. This enables the APPN link station in the router to receive an activation XID from the remote SDLC link station. This is different from other DLC types, such as Token ring or Ethernet, whose APPN link stations do not need to be explicitly defined for APPN in the router since APPN has the capability to dynamically define these types of link stations.

Refer to the Software User's Guide for additional information about SDLC network layer configuration.

```
***********************************************************************
*
* The following examples show how to configure different SDLC stations.
*
***********************************************************************
*Configuring a Primary Point-To-Point SDLC Station:  1
***********************************************************************
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role primary
SDLC 1 Config>list link
list link
Link configuration for: LINK_1   (ENABLED)

Role:        PRIMARY          Type:        POINT-TO-POINT
Duplex:      FULL             Modulo:      8
Idle state:  FLAG             Encoding:    NRZ
Clocking:    INTERNAL         Frame Size:  2048
Speed:       64000            Group Poll:  00
Cable:       RS-232 DCE

Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
           RTS hold delay:     DISABLED
           Inter-frame delay:  DISABLED
           Inactivity timeout: 30.0 sec

Counters:  XID/TEST retry:  8
           SNRM retry:      6
           Poll retry:      10
SDLC 1 Config>ex
Config> CTRL p
* restart
Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>list port sdlc001
PORT:
  Interface number(DLSw = 254): 1
  PORT enable: YES
  Service any node: YES
  Link Type: SDLC
  MAX BTU size: 2048
  MAX number of Link Stations: 1
  Percent of link stations reserved for incoming calls: 0
  Percent of link stations reserved for outgoing calls: 0
  Cost per connect time: 0
  Cost per byte: 0
  Security:(0 = Nonsecure, 1 = Public Switched Network
     2 = Underground Cable, 3 = Secure Conduit,
     4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
  Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
     3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 2
  Effective capacity: 45
  First user-defined TG characteristic: 128
```

```
  Second user-defined TG characteristic: 128
  Third user-defined TG characteristic: 128
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOSECSTN
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C1]?
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
 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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>list link tosecstn
STATION:
  Port name: SDLC001
  Interface number(DLSw = 254): 1
  Link Type: SDLC
  Station address: C1
  Activate link automatically: YES
  Allow CP-CP sessions on this link: YES
  CP-CP session level security: NO
  Fully-qualified CP name of adjacent node:
  Encryption key: 0000000000000000
  Use enhanced session security only: NO
  Cost per connect time: 0
  Cost per byte: 0
  Security:(0 = Nonsecure, 1 = Public Switched Network
     2 = Underground Cable, 3 = Secure Conduit,
     4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
  Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
     3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 2
  Effective capacity: 45
  First user-defined TG characteristic: 128
  Second user-defined TG characteristic: 128
  Third user-defined TG characteristic: 128
  Predefined TG number: 0
APPN config>act
***********************************************************************
* Configuring a Secondary Point-To-Point SDLC Station:  2
***********************************************************************
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role secondary
SDLC 1 Config> set link cable rs-232 dte
SDLC 1 Config>list link       **(will show link configuration)

SDLC 1 Config>add station
Enter station address (in hex) [C1]?
Enter station name [SDLC_C1]?
Include station in group poll list ([Yes] or No): no
Enter max packet size [2048]?
Enter receive window [7]?
Enter transmit window [7]?
SDLC 1 Config>list station all
Address    Name      Status    Max BTU  Rx Window  Tx Window
-------  --------  ----------  -------  ---------  ---------
  C1     SDLC_C1     ENABLED      2048      7          7
SDLC 1 Config>ex
Config> CTRL p
* restart
Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

```
APPN config>list port sdlc001   **(will show port definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOPRISTN
 Activate link automatically (Y)es (N)o [Y]?
(Note: "Y" to accept activation from the primary or negotiable station)
 Station address(1-fe) [C1]?
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
 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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>list link topristn  **(will show link station definitions)
APPN config>act
**********************************************************************
* Configuring a Negotiable Point-To-Point SDLC Station: 3
**********************************************************************
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role negotiable
SDLC 1 Config>list link      **(will show link configuration)
SDLC 1 Config>ex
Config> CTRL p
* restart
Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>list port sdlc001        **(will show port definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOREMSTN
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C1]?
 (Note: C1 may be used if this station is becoming a secondary station)
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
 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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>list link toremstn   **(will show link station definitions)
APPN config>act
**********************************************************************
* Configuring a Primary Multipoint SDLC Station:  4
**********************************************************************
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role primary
SDLC 1 Config> set link type multipoint
SDLC 1 Config>list link      **(will show link configuration)
SDLC 1 Config>ex
Config> CTRL p
* reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
```

```
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 Maximum number of link stations (1-127) ? 2
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>list port sdlc001            **(will show port definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOSTNC1
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C1]?
      (Note: C1 must match to the remote secondary station)
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
 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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.

APPN config>list link tostnc1    **(will show link station definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOSTNC2
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C2]?
      (Note: C2 must match to the remote secondary station)
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
 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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>list link tostnc2     **(will show link station definitions)
APPN config>act

****************************************************************************
* Configuring a Secondary point-to-point (Multi APPN link station):   5
****************************************************************************
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role secondary
SDLC 1 Config> set link type point-to-point
SDLC 1 Config>list link       **(will show link configuration)
SDLC 1 Config>ex
Config> CTRL p
* reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
 Service any node: (Y)es (N)o [Y]?
 Maximum number of link stations (1-127) ? 2
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>list port sdlc001             **(will show port definitions)
APPN config>add link sdlc001
```

```
APPN Station
Station name (Max 8 characters) [ ]? TOSTNC1
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C1]?
      (Note: C1 must match to the remote secondary station)
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
 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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

```
APPN config>list link tostnc1    **(will show link station definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOSTNC2
 Activate link automatically (Y)es (N)o [Y]?
 Station address(1-fe) [C2]?
      (Note: C2 must match to the remote secondary station)
 Adjacent node type: 0 = APPN network node, 1 = APPN end node
 2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
 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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>list link tostnc2     **(will show link station definitions)
APPN config>act
```

Note:

1 Configuring a primary point-to-point SDLC station
2 Configuring a secondary point-to-point SDLC station
3 Configuring a negotiable point-to-point SDLC station
4 Configuring a primary multipoint SDLC station
5 Configuring secondary point-to-point (multi APPN link stations)

Configuring APPN Over X.25

This example shows APPN configuration for an X.25 port and two link stations. One link station is a PVC and one is an SVC. The SVC is configured as a limited resource. The SVC will be activated when needed and brought down when it is not.

```
Boats Config>p appn
APPN user configuration
Boats APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC,  (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (IP)[ ]? x
Interface number(Default 0):[0]? 2
Port name (Max 8 characters)[X25002]?
Enable APPN on this port (Y)es (N)o[Y]?
Port Definition
        Service any node: (Y)es (N)o[Y]?
        Maximum number of link stations (1-65535)[65535]?
        Percent of link stations reserved for incoming calls (0-100)[0]?
        Percent of link stations reserved for outgoing calls (0-100)[0]?
Edit TG Characteristics: (Y)es (N)o[N]?
Write this record?[Y]?
The record has been written.
```

```
Boats APPN config>add link
APPN Station
Port name for the link station[ ]? x25002
Station name (Max 8 characters)[ ]? x25svc1
        Limited resource: (Y)es (N)o[N]? Y
        Activate link automatically (Y)es (N)o[N]?
        Link Type (0 = PVC , 1 = SVC)[0]? 1
        DTE Address [0]? 2222
        Adjacent node type: 0 = APPN network node,
```

```
        1 = APPN end node or Unknown node type
        2 = LEN end node, 3 = PU 2.0 node[1]?
Edit Dependent LU Server: (Y)es (N)o[N]?
        Allow CP-CP sessions on this link (Y)es (N)o[Y]? N
        CP-CP session level security (Y)es (N)o[N]?
        Configure CP name of adjacent node: (Y)es (N)o[N]?
Edit TG Characteristics: (Y)es (N)o[N]?
Write this record?[Y]?
The record has been written.

Boats APPN config>add link
APPN Station
Port name for the link station[ ]? x25002
Station name (Max 8 characters)[ ]? x25pvc1
        Limited resource: (Y)es (N)o[N]?
        Activate link automatically (Y)es (N)o[Y]?
        Link Type (0 = PVC , 1 = SVC)[0]?
        Logical channel number (1-4095)[1]?
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type
        2 = LEN end node, 3 = PU 2.0 node[1]?
Edit Dependent LU Server: (Y)es (N)o[N]?
        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]?
Edit TG Characteristics: (Y)es (N)o[N]?
Write this record?[Y]?
The record has been written.

Boats APPN config>list port x25002
PORT:
       Interface number(DLSw = 254): 2
       PORT enable: YES
       Service any node: YES
       Link Type: X25
       MAX BTU size: 2048
       MAX number of Link Stations: 239
       Percent of link stations reserved for incoming calls: 0
       Percent of link stations reserved for outgoing calls: 0
       Cost per connect time: 0
       Cost per byte: 0
       Security:(0 = Nonsecure, 1 = Public Switched Network
          2 = Underground Cable, 3 = Secure Conduit,
          4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
       Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
          3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3
       Effective capacity: 45
       First user-defined TG characteristic: 128
       Second user-defined TG characteristic: 128
       Third user-defined TG characteristic: 128
Boats APPN config>list link x25svc1
STATION:
       Port name: X25002
       Interface number(DLSw = 254): 2
       Link Type: X25
       Link Type (0 = PVC , 1 = SVC): 1
       DTE Address: 2222
       Activate link automatically: YES
       Allow CP-CP sessions on this link: YES
       CP-CP session level security: NO
       Fully-qualified CP name of adjacent node:
       Encryption key: 0000000000000000
       Use enhanced session security only: NO
       Cost per connect time: 0
       Cost per byte: 0
       Security:(0 = Nonsecure, 1 = Public Switched Network
          2 = Underground Cable, 3 = Secure Conduit,
          4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
       Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
          3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3
       Effective capacity: 45
       First user-defined TG characteristic: 128
       Second user-defined TG characteristic: 128
       Third user-defined TG characteristic: 128
       Predefined TG number: 0

Boats APPN config>list link x25pvc1
STATION:
       Port name: X25002
       Interface number(DLSw = 254): 2
       Link Type: X25
```

```
       Link Type (0 = PVC , 1 = SVC): 0
       Logical Channel number: 1
       Activate link automatically: YES
       Allow CP-CP sessions on this link: YES
       CP-CP session level security: NO
       Fully-qualified CP name of adjacent node:
       Encryption key: 0000000000000000
       Use enhanced session security only: NO
       Cost per connect time: 0
       Cost per byte: 0
       Security:(0 = Nonsecure, 1 = Public Switched Network
          2 = Underground Cable, 3 = Secure Conduit,
          4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
       Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
          3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3
       Effective capacity: 45
       First user-defined TG characteristic: 128
       Second user-defined TG characteristic: 128
       Third user-defined TG characteristic: 128
       Predefined TG number: 0
Boats APPN config>li all
NODE:
       NETWORK ID: STFNET
       CONTROL POINT NAME: BOATS
       XID: 00000
       APPN ENABLED: YES
       MAX SHARED MEMORY: 4096
       MAX CACHED: 4000
DLUR:
       DLUR ENABLED: NO
       PRIMARY DLUS NAME:
CONNECTION NETWORK:
             CN NAME       LINK TYPE  PORT INTERFACES
       ------------------------------------------------------------
COS:
       COS NAME
       --------
           BATCH
         BATCHSC
         CONNECT
           INTER
         INTERSC
         CPSVCMG
        SNASVCMG
        MODE NAME  COS NAME
       ---------------------

PORT:
         INTF     PORT      LINK      HPR    SERVICE   PORT
        NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
       -----------------------------------------------------
           2     X25002        X25     NO      YES      YES
           5      TR005   IBMTRNET    YES      YES      YES
STATION:
        STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
         NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
       ------------------------------------------------------------
        X25SVC1   X25002            2222        NO      NO       1
        X25PVC1   X25002               1        NO     YES       1
LU NAME:
             LU NAME        STATION NAME          CP NAME
       ------------------------------------------------------------
Boats APPN config>ex

Boats Config>n 2
X.25 User Configuration
Boats X.25 Config>li all

X.25 Configuration Summary

Node Address:       1111
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:          64000         Clocking:  External
MTU:             2048         Cable:     V.35 DTE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DCE)
PVC            low: 1    high: 4
Inbound        low: 0    high: 0
```

```
Two-Way         low: 10   high: 20
Outbound        low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400


X.25 National Personality Configuration

Follow CCITT: on       OSI 1984:    on       OSI 1988:      off
Request Reverse Charges:  off   Accept Reverse Charges:     off
Frame Extended seq mode:  off   Packet Extended seq mode:   off
Incoming Calls Barred:    off   Outgoing Calls Barred:      off
Throughput Negotiation:   off   Flow Control Negotiation:   off
Suppress Calling Addresses: off
DDN Address Translation:  off
Call Request Timer:     20 decaseconds
Clear Request Timer:    18 decaseconds (1 retries)
Reset Request Timer:    18 decaseconds (1 retries)
Restart Request Timer:  18 decaseconds (1 retries)
Min Recall Timer:       10 seconds
Min Connect Timer:      90 seconds
Collision Timer:        10 seconds
T1 Timer:  4.00 seconds     N2 timeouts: 20
T2 Timer:  0.00 seconds     DP Timer:    500 milliseconds
Standard Version:        2      Network Type: CCITT
Disconnect Procedure: passive
Window Size     Frame:   7      Packet:  2
Packet Size     Default: 128    Maximum: 256

X.25 protocol configuration

Prot         Window      Packet-size        Idle     Max     Station
Number       Size      Default Maximum      Time     VCs      Type
30 -> APPN    7          128     1024        0        4       PEER

X.25 PVC configuration

Prtcl        X.25_address     Active Enc  Window    Pkt_len   Pkt_chan
30  (APPN)   6666               NONE      2         128       1

X.25 address translation configuration

IF #  Prot #       Active Enc  Protocol       -> X.25 address
2     30 (APPN)       NONE     appn           -> 6666
Boats X.25 Config>
```

Configuring APPN Over Frame Relay

The following example shows configuration of APPN over Frame Relay.

```
nada207 Config>p appn
APPN user configuration
nada207 APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC,  (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (IP) [  ] ?f
Interface number(Default 0): [0]? 4
Port name (Max 8 characters) [FR004]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-2048) [2048]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Support bridged formatted frames: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config>add link
APPN Station
Port name for the link station []? fr004
Station name (Max 8 characters) []? tonn
        Activate link automatically (Y)es (N)o [Y]?
        DLCI number for link (16-1007) [16]?
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type
```

```
        2 = LEN end node, 3 = PU 2.0 node [1]? 0
        High performance routing: (Y)es (N)o [Y]?
Edit Dependent LU Server: (Y)es (N)o [N]?
        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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config>act
nada207 APPN config>exit
nada207 Config>write
Config Save: Using bank B and config number 2
```

Configuring APPN Over Frame Relay BAN

The following example shows configuration of APPN over Frame Relay BAN.

```
nada207 Config>p appn
APPN user configuration
nada207 APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC,  (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (IP) [  ] ?f
Interface number(Default 0): [0]? 4
Port name (Max 8 characters) [FR004]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-2048) [2048]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Support bridged formatted frames: (Y)es (N)o [N]? y
  Boundary node identifier (hex-noncanonical) [4FFF00000000]?
 41235fad
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config> add link
APPN Station
Port name for the link station []? fr004
Station name (Max 8 characters) []? tonn
        Activate link automatically (Y)es (N)o [Y]?
        DLCI number for link (16-1007) [16]?
        Support bridged formatted frames: (Y)es (N)o [N]? y
        MAC address of adjacent node (hex-noncanonical) [000000000000]? 3456
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type
        2 = LEN end node, 3 = PU 2.0 node [1]? 0
        High performance routing: (Y)es (N)o [Y]?
Edit Dependent LU Server: (Y)es (N)o [N]?
        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]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config>act
nada207 APPN config>exit
nada207 Config>write
Config Save: Using bank B and config number 2
```

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, (FD)DI, (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.
```

Configuring an Extended Border Node

```
Spurs APPN config>p app
Spurs APPN config>set node
Enable APPN (Y)es (N)o [N]? y
Network ID (Max 8 characters) [STFDDD3]?
Control point name (Max 8 characters) [SPURS]?
Enable branch extender or extended border node
(0=Neither, 1=Branch Extender, 2=Border Node)[2]?
Subnet visit count(1-255) [3]?
Cache searches for (0-255) minutes [8]?
Maximum number of searches to cache (0(unlimited)-32765) [0]?
Dynamic routing list updates (0=None, 1=Full, 2=Limited) [1]?
Enable routing list optimization (Y)es (N)o [Y]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
Spurs APPN config>act
APPN is not currently active
Spurs APPN config>add rout
Routing list name []? list1
Subnet visit count (1-255) [3]?
Dynamic routing list updates (0=None, 1=Full, 2=Limited) [1]?
Enable routing list optimization (Y)es (N)o [Y]?
Destination LUs found via this list:
  (netID.LUname)[] ? net1*
  (netID.LUname) []?
Routing CPs (with optional subnet visit count):
  (netID.CPname   ?)    [  3]? net2.router2
  (netID.CPname   ?)    [  3]?
Write this record? (Y)es (N)o [Y]?
The record has been written.

Spurs APPN config>add cos
COS mapping table name []? cos1
Non-native network (netID.CPname) []?net2.router2
Non-native network (netID.CPname) []?
Native and non-native COS name pair [   ]? #inter
Native and non-native COS name pair [   ]?
Write this record? (Y)es (N)o [Y]?
The record has been written.
```

Chapter 2. Using TN3270

This section introduces TN3270 and summarizes the TN3270E server function implemented in IBM routers. It includes the following topics:

Overview

Many companies today are consolidating their WAN traffic onto IP-only backbones. Companies are also simplifying their workstation configurations and attempting to run only the TCP/IP protocol stack at the desktop. However, most of these companies still require access to SNA application hosts.

TN3270 meets these requirements by allowing you to run IP from the desktop over the network and attach to your SNA host through a TN3270 server. The clients connect to the server using a TCP connection. The server provides a gateway function for the downstream TN3270 clients by mapping the client sessions to SNA dependent LU-LU sessions that the server maintains with the SNA host. The TN3270 server handles the conversion between the TN3270 data stream and an SNA 3270 data stream.

To deploy a TN3270 solution, you install TN3270 client software on desktop workstations[3] and TN3270 server software in one of several places discussed below. Client software is available from IBM and many other vendors, and runs on top of the TCP/IP stack in the workstation. A given client product provides one of two possible levels of standards support:

- Base TN3270 client

  These clients conform to RFC 1576 (TN3270 Current Practices) and/or RFC 1646 (TN3270 Extensions for LU name and Printer Selection).
- TN3270E client

  These clients conform to RFC 1647 (TN3270 Enhancements), and RFC 2355 (TN3270 Enhancements).

A server implementation that can support TN3270E clients is called a TN3270E server.

Placement of the TN3270 Server Function

The TN3270 server function can be placed in a variety of products and positions within a network, including:

- In the SNA host itself

  IBM and several other vendors provide host TN3270 server software that sits on top of the host TCP/IP stack and connects within the host to VTAM.
- In a router or in the network

  IBM and other vendors provide TN3270 server function in networking hardware products. You can place these products directly adjacent to the SNA host, or at any position in the network where you have SNA connectivity to the host. If you

3. You can also find small, dedicated TN3270 client products that represent printers.

are using IBM routers and your host is running APPN, you can use Enterprise Extender technology to place the server at any position where you have IP connectivity to the host.

- In a software product in the network

  IBM and other vendors provide TN3270 server software products that you install on mid-range servers that use operating systems such as AIX, OS/2, or Windows/NT. You can place these products at any position in the network where you have SNA connectivity to the application host.

The choice of TN3270 server product and network position is a complex one, involving such factors as:

- Host capacity and cycle impact
- Price for performance and capacity
- Availability
- Impact of server failure
- Scalability

IBM routers provide a high-performing TN3270E server implementation that scales to large networks. By combining this implementation with the Network Dispatcher feature, you can implement server redundancy and load sharing in large TN3270 installations. You can also place an IBM router out into an SNA or IP network away from the data center and get the same advantages of scalability, incremental addition, and reduced impact of server failure.

TN3270E Server Function

Standards Compliance

The IBM router implementation of TN3270E server supports these RFCs:

RFC 1576 TN3270 Current Practices

RFC 1646 TN3270 Extensions for LU names and Printers

RFC 1647 TN3270 Enhancements

RFC 2355 TN3270 Enhancements (obsoletes RFC 1647)

It can handle both base TN3270 and TN3270E clients at the same time.

Host Connectivity

The path from a TN3270 client to the SNA host consists of two pieces:

- A TCP connection over IP from the client to the server
- An SNA LU-LU session from the server to the host

The form of the SNA connection from the server to the host depends on how the server represents PUs and dependent LUs. When you are using an IBM router as your TN3270 server, you can configure either of two different ways to establish links and represent PUs and LUs to VTAM:

- Using SNA subarea links

  You configure this way when you are not running APPN at the host (even though the router is still APPN-capable). You configure a separate DLC-layer link to the host for every PU (maximum of 255 LUs per PU). Multiple PUs require multiple parallel host links. SNA frames arriving at the router on one of these links flow directly to the corresponding internal PU.

  Subarea host links must be a single DLC-layer hop to the product providing the SNA subarea boundary function. Typically, this product is either NCP running in a FEP (front-end processor), or is VTAM itself in the host. The subarea link from the router can traverse bridges or other DLC-layer forwarding mechanisms (such as protocol converters or external DLSw routers). IBM routers support the following link types for subarea host attachment (where the link type is available on a given router product):

- Token-Ring: physical, ATM LAN emulation, or channel LSA
- Ethernet: physical, ATM LAN emulation, or channel LSA
- FDDI: physical only
- Frame relay PVCs: bridged or routed RFC 1490/2427 formats
- DLSw (note that local DLSw can provide access to SDLC and QLLC upstream links)

• Using an APPN Dependent LU Requester (DLUR) link

You configure this way when you are running APPN with its Dependent LU Server (DLUS) function at the host. At the DLUR router, you configure one or more DLUS(es) to support the TN3270 internal dependent PUs (and any external dependent PUs that may exist). A router running DLUR can either be directly connected to the DLUS host, or can be located remotely across several APPN links. Only one link is required to carry the first or only hop of the DLUR-DLUS ″pipe″, even if you are defining multiple local PUs (to have more than 255 total LUs). SNA frames arriving on the DLUR-DLUS pipe flow to the DLUR function, which redirects them to the correct internal or external PU.

When you are using DLUR, you can route through an APPN network using either ISR or HPR routing to reach the host. IBM routers support the following link types as the ″first hop″ APPN link to the host (where the link type is available on a given router product):

- Token-Ring: physical, ATM LAN emulation, or channel LSA
- Ethernet: physical, ATM LAN emulation, or channel LSA
- FDDI: physical only
- Frame relay PVCs: bridged or routed RFC 1490/2427 formats
- ATM (native, not LAN emulation): HPR only
- Channel MPC+: HPR only
- PPP
- SDLC: ISR only
- X.25: ISR only
- DLSw: ISR only
- IP (Enterprise Extender): HPR only

Note especially that when using DLUR and HPR routing, you can place a TN3270E server across an IP network from the SNA application host. Enterprise Extender maintains session-level class of service and transmission priority across the IP network.

If an LU-LU session exists when the TN3270 client disconnects from the TN3270 server, an UNBIND or TERM-SELF request will be sent to the host to terminate the LU-LU session. The default is UNBIND cleanup. The local PU or link station must be configured appropriately for TERM-SELF to flow. TERM-SELF should be configured if a session manager (front end) application is being used to get to applications such as TSO or CICS.

SNA Management Support

From a VTAM or NetView/390 operator console, you can control the links, PUs, and LUs involved with TN3270. For LUs, when a TN3270 client connects in, the router reports the client’s IP address and TCP port number to VTAM on its session activation flows (via CV64). VTAM console display commands such as ″/D NET,ID=(lu name),E″ have the ability to display the TCP/IP address information associated with particular LUs. This permits problem determination for TN3270 clients from a VTAM operator console.

VTAM support for receiving and displaying client IP addresses is in CS for OS/390 V2R6 base code. It was also PTF'd to CS for OS/390 V2R5 (VTAM APAR OW31454, TCP/IP APAR PQ12574).

In addition to enabling this console support, APPN generates SNA alerts for a variety of error configurations, and can forward alerts from other SNA devices. There are no alerts specific to the TN3270 server function, but alerts that the router itself generates may relate to SNA resources involved with TN3270.

SNMP MIB and Trap Support

IBM routers support an Internet Draft version of both of these standard MIBs for TN3270 server function:

- TN3270 Base MIB (now RFC 2561)
- TN3270 Response Time MIB (now RFC 2562)

IBM router support for these MIBs includes the ability to:

- View server configuration, status, and statistics
- Set up client groups for response time collection
- View the mapping of LU names from VTAM name to local name to client IP address
- View the mapping of client IP addresses to VTAM LU names
- Collect response time data for current client groups

In addition, the following enterprise-specific MIB shows the reasons why clients were not able to successfully connect to the TN3270 server:

- IBM TN3270 Connection Rejection

These TN3270-related MIBs supplement the extensive IBM router MIB support for APPN and SNA resources.

TN3270 Host On-Demand Client Caching

Some IBM router products (currently the 2216 and 2212) support a ″Web Server Cache″ function, where they can sit in front of an HTTP server and offload the server by caching Web objects and serving them up to requesting clients. Among the objects these routers can cache are Java applets that provide TN3270 client function.

Host On-Demand (HOD) Client Caching allows one of these routers or the IBM Network Utility to cache TN3270 client function applets from an HOD host Web server and serve them to client browsers upon request. The browsers then launch the TN3270 terminal emulation applets. These applets connect to an SNA host either through the router's TN3270 server function, or through some other TN3270 server.

Host On-Demand support is packaged with the TN3270 server function, but you configure the two independently. The router can cache HOD clients but not be configured as a TN3270 server. Likewise, the router can be a TN3270 server with no HOD caching enabled. The Web Server Cache router code loads that do not include TN3270 server function (only on 2216 and 2212) can also cache HOD client applets if so configured.

Because the HOD client cache function is completely separate from the Server function, it is not further discussed in this chapter. See the chapter entitle “Configuring and Monitoring IBM eNetwork Host On-Demand Client Cache” in the *Using and Configuring Features* publication, for more information on this function.

General TN3270E Server Configuration

This section covers general information about configuring TN3270 server support. For specific example configurations, see “Example Configurations” on page 83.

Loading the TN3270 Server Code

Depending on your router type and configuration method, you may have to take extra steps to load APPN and TN3270 code and be able to access their command-line configuration and monitoring prompts:

- Load to disk a router code package that includes both APPN and TN3270. If you boot the router with a configuration from the Configuration Program, the router will load APPN and TN3270 from disk if you have configured those protocols. If you boot the router with no configuration or a non-TN3270 command-line configuration, the router does not load these protocols into memory be default. Use the **load add** command for both the APPN and TN3270E packages, save your configuration, and reboot with the saved configuration in order to configure these protocols.

For details about the **load add** command, see the chapter entitled “The CONFIG Process (CONFIG - Talk 6) and Commands” in the *Software User’s Guide*.

Configuring TN3270 under the APPN Protocol

In the IBM router implementation of TN3270 server, all SNA functions are bundled within the APPN protocol. This means that even when you are configuring SNA subarea host attachment and your SNA host is not running APPN, you must use the configuration and console services of the APPN protocol. In particular:

- You must go through the APPN protocol at the command line and at the Configuration Program to configure ports, links, and TN3270 server functions
- You must go through the APPN protocol at the command line to use TN3270 monitoring commands
- You must configure APPN at the node level

When you configure SNA subarea support, the router does in fact still function as an APPN network node, but only on links to other APPN nodes. If the only ports and links you configure are those for SNA subarea host attachment, then the APPN function itself does not run.

Server IP Address

To enable the TN3270 server function, you must configure an IP address to which the TN3270 clients will connect. The IBM router TN3270 implementation supports only a single server IP address (but multiple destination TCP ports). The address you configure for TN3270 must match one of the following addresses you configure for IP, otherwise TN3270 will not initialize.

- An interface address

  You can assign any number of addresses to an interface. The interface can be either physical or a virtual ″loopback″ interface. Physical interface addresses are active only when the associated interface is up, but loopback interface addresses are always active.
- The internal address

This is a single address that represents the entire router and is active independent of the state of any particular interface.

When you choose the IP address for the TN3270 function, you must consider that administrative users also need to be able to establish regular Telnet sessions, to bring up remote router consoles. The default destination port for both Telnet and TN3270 is the same (23), so unless you want one or the other sets of users to use a non-default destination port, you must set aside different IP addresses for Telnet and TN3270 users.

If you are using router code V3.4 or higher, the recommended procedure is to define a loopback interface and use one of the IP addresses on that interface as your TN3270 server IP address. If you are using router code before V3.4, you need to choose either to use a physical interface address for TN3270 and leave the internal address for Telnet, or vice versa. One important consideration in this choice is whether you have multiple parallel TN3270 servers, each of which needs the same server address but different Telnet addresses for maintenance.

Server TCP Ports

When you configure the server IP address, you also specify a destination TCP port number to which the TN3270 clients will connect. You must provide at least one port number as part of server’s general configuration (`TN3270E config> set` command, Configuration Program TN3270E Server/General panel). Optionally, you can configure additional TCP ports for the TN3270 server to ″listen″ on (`TN3270E config> add port` command, Configuration Program TN3270E Server/Ports panel).

The following are reasons you might want to configure more than one server TCP port:

- Segregate ″E″ and ″non-E″ clients

  The TN3270 protocol requires an E-capable server to initiate certain negotiations with clients. Some old non-E clients fail instead of simply ignoring these negotiations. You can configure the router so that it treats clients connecting to a given destination port as non-E clients, and does not send them the offending request. You then configure the non-E clients to attach to that port.
- Map clients to SNA resources using a port number

  Many clients cannot request an SNA resource by name, but they all connect to a destination TCP port. When you configure a destination port, you associate an LU pool with that port number (there is a global default pool if you do not specify a particular one). Clients that connect to this port and do not specify an LU name will be assigned an LU from this pool.
- Disable IP address mapping for some clients

  If you have globally enabled the mapping of client IP addresses to LU or LU pool names, the router chooses the LU using the IP address mapping rules rather than using the port to LU pool association. You may want to have a set of clients that are exempt from this mapping (note that clients who fail to match the configured mappings are refused a connection). You can configure a destination port so that when a client connects to that port, IP address mapping is ignored. When you select this option, the LU pool associated with that port is used instead to choose the LU.
- Map clients to SNA resources using port-specific IP address mapping

  If you have globally enabled the mapping of client IP addresses to LU or LU pool names, you may want to have different IP mapping rules apply to different sets of clients. When you configure an IP mapping table entry, you can specify a destination TCP port number (the default is ″all ports″). When you do so, only the clients that connect to that port number are checked against that mapping entry.

Defining PUs

You must always define dependent PUs in the router, to contain the LUs that the router associates with incoming TN3270 client TCP connections. Each PU you define must have a corresponding PU definition in VTAM.

If you are using DLUR for your host connection, the internal PUs you define each appear to have an ″inside the box″ logical link to the DLUR function. This logical link is always active when APPN and TN3270 are active. DLUR may at the same time be serving other dependent PUs external to the router.

You need to define only as many PUs as you need to contain your LUs, where each PU can have 255 LUs. If you are defining more than one local PU, you distinguish them by specifying different local node IDs. To configure a local PU for DLUR using the command line, use the **add local-pu** command. From the Configuration Program, select Local PUs from under the TN3270E Server protocol in the Navigation window.

If you are using subarea links for your host connection, each link is bound to an associated internal PU. The router creates this internal PU automatically when you configure a subarea link; you do not explicitly configure internal PUs the way you do with DLUR. The link associated with each PU is a real external link which can go up or down. Some users distribute the LUs that are in a single pool across multiple subarea PUs, so that if one link fails there may be another available to service client reconnection attempts.

To configure a subarea link using the command line, use the add link command. Respond yes to the question ″Solicit SSCP session?″, and no to the question ″Does link support APPN function?″. From the Configuration Program, select Interfaces from under the APPN protocol in the Navigation Window, then click on the Link stations column heading. If you are configuring more than one subarea link under the same physical port, you must enable that port to support multiple PUs. You distinguish the PUs by local node ID as well as by local addressing information such as the SAP address.

Defining LUs

When a TN3270 client is fully connected, its TCP connection is paired with an SNA LU representation in the server. VTAM also has a representation for the same LU. Each of these LU representations has a name, and it is possible but not necessary for the server LU name to match the VTAM LU name. Since a typical TN3270 configuration involves thousands of LUs to satisfy as many potential clients, various schemes have been developed to ease the burden of configuring LUs and to make it possible for the server and VTAM names to match.

The IBM router implementation of TN3270 server currently supports the following LU definition methods. See the sections that follow for a detailed description of each method. All these methods are available regardless of whether your host link attachment is DLUR or subarea.

- Static in the router, static in the host

  With this method, you configure LUs in the router either individually by name or in groups using name seeds. You define corresponding LUs in VTAM by hand using the same or different LU names. The PU ID and LU's NAU addresses are what relate the router's LUs to VTAM's LUs.

- Static in the router, dynamic in the host (DDDLU - Dynamic Definition of Dependent LUs)

  With this method also, you configure LUs in the router either individually by name or in groups using name seeds. In VTAM, you code model LU definitions and associate them with the dependent PUs defined in the router. When a TN3270 client connects in to the router, the router selects an LU and sends its configured information about that LU to VTAM (both NAU address and name). Passing the router LU name in this manner is referred to as “name pushing”. VTAM creates the LU definition dynamically, using either its own name seed or the LU name ″passed″ by the router.

  When a TN3270 client disconnects, the router sends a notification of this event. Later levels of VTAM have the ability to destroy the dynamic LU. Earlier versions do not destroy the LU but simply deactivate it pending usage by another client. Dynamic creation and deletion make it possible to have the same named LU be served by any of a number of parallel load-balanced TN3270 servers.

- Dynamic in the router, static in the host (HIDLU - Host-Initiated Dynamic LUs)

  With this method, you are not required to configure LUs in the router. You simply configure on a PU basis that a PU supports host-initiated dynamic LUs. In VTAM, you define PUs and LUs by hand as normal. When you activate the LUs at VTAM, the ACTLUs cause the router to dynamically create corresponding LUs using the VTAM LU name. The dynamic LUs are treated as explicit LUs or are placed into implicit LU pools based on whether you configure a pool name for the HIDLU-capable PU.

You can choose any of these LU definition methods, based on the size of your network configuration, level of router and VTAM code, LU naming requirements, and server load balancing requirements. You can combine HIDLU with the other methods by configuring some LUs in the router and allowing the rest to be dynamically created, even within the same PU.

Configured LUs

You need to configure LUs in the router unless you are using Host-Initiated Dynamic LUs. You can configure individual LUs or groups of LUs. Normally, you configure individual LUs when you want to fully specify the LU name and fix it at a particular NAU address. You configure groups of LUs when you have a large number of similar LUs to define and you want the router to generate the LU names.

To configure an individual LU from the command line, use the **add lu** command. You specify the name of the PU (or subarea link) for the LU, and the LU's name, type, and NAU address. To configure an individual LU from the Configuration Program, select LUs from under the TN3270E Server protocol in the Navigation Window, then click on the LUs column heading.

To configure a group of LUs from the command line, use the **add implicit-pool** command. This command defines a group of LUs under a single PU and places them in a pool. You can use this command several times to place different groups of LUs in the same pool, such as LUs from different PUs.

Each time you add a group, you specify the name of the PU, name of the pool, and LU type information. Instead of a single NAU address, you specify either a range of addresses, or the number of LUs you want to add. At initialization time, the router fixes the NAU addresses for configured individual LUs, then assigns the remaining addresses in the range, or number of addresses, to LUs in the group.

Instead of a single LU name, for a group you specify an LU name mask. When the router initializes, it assigns LU names by suffixing this mask with the LU's NAU address in decimal (not padded with leading zeros). For example, a mask of ″@LU1A″ might result in the LU names @LU1A1, @LU1A2, and so forth.

If you specify a NAU address range, the router generates names appending the NAU address starting with the bottom of the range going to the top, as just shown with @LU1A. If you specify the number of LUs instead of an NAU address range, the router generates names starting with NAU 2, incrementing up to 255, and ending with 1. For example, a mask of @LU2A for 10 LUs would generate the names @LU2A2, @LU2A3, ..., @LU2A11. The server code starts with 2 for migration consistency with prior code releases that did not support the NAU value 1. To see the exact names the router generates for LUs under a particular PU, use the `Talk 5` TN3270 **list pu** *name* command.

To configure a group of LUs from the Configuration Program, you must first name the target pool by selecting Pools from under the TN3270E Server protocol in the Navigation Window. Then select LUs from the Navigation window and click the Implicit Pool column heading.

Dynamic Definition of Dependent LUs (DDDLU)

As summarized in Defining LUs, you may use DDDLU to avoid duplicate definition of LUs in both VTAM and the router. DDDLU allows you to configure LUs in one place only, the router. In VTAM, you only need to define one or more PUs depending on the number of LUs you need. Implementation of DDDLU also eliminates the effort of VTAM definitions and maintenance for future LU definition requirements.

Creating LUs at VTAM

When a TN3270E client requests a connection using one of the LUs defined in the router, the router sends a Reply PSID NMVT command to VTAM on the SSCP-PU session. In this command, the router sends the following information:

- Local NAU address of the LU
- Router name for the LU
- Power on/off indicator
- Device type and model number of the device
- Other optional device-dependent information

On receipt of this NMVT, VTAM sees from the PU definition that there is no definition for the LU in question. VTAM then uses the PU definition and the information in the NMVT to choose a model LU statement and create an LU definition.

The name that VTAM chooses for the dynamic LU is driven by an exit routine for Selection of Definitions for Dependent LUs (SDDLU). If you use the standard IBM-supplied user exit routine, VTAM constructs a name using the LUSEED value on the PU statement, suffixed by the NAU address. You must also code the LUGROUP operand to specify a model major node. These operations are described in *VTAM Network Implementation Guide*, SC31-8370, under the section entitled ″Defining Dependent LUs Dynamically″.

If you want VTAM to use the LU name that the router sends in the Reply PSID NMVT command, you must replace the standard SDDLU user exit with one available from the IBM router support download Web pages. This routine ignores the LUSEED operand and simply uses the name pushed from the router. To download this routine from the 2216 Web pages, for example, go to **http://www.networking.ibm.com/support/downloads/2216** , select the link to ″APPN/TN3270 Files″, and select the user exit package. The package is common to all IBM routers.

Deleting LUs from VTAM

When a TN3270 client disconnects from the router, it sends VTAM another Reply PSID NMVT indicating that the device has powered off. VTAM can then delete the dynamically created LU. This frees up storage and makes the name available for reuse.

VTAM support for dynamic LU deletion on client disconnect is in the base code of CS for OS/390 V2R6, and is PTF'd to CS for OS/390 V1R3 and above with APAR OW29773.

Dynamic LUs and Network Dispatcher

IBM's Network Dispatcher (ND) can provide a TCP load balancing function when installed between clients and two or more TN3270 servers. The IBM router version of ND and TN3270 Server work together so that ND sends new client connections to the least busy TN3270 server. Previously, when using ND to load balance between TN3270 servers going to the same VTAM, you could not have LUs that needed a fixed VTAM LU name. This is because ND could route the client TCP connection to any of the servers, but you could not have duplicate LU names active at VTAM at the same time.

With LU name pushing and deletion, you can configure the desired LU name at all the potential TN3270 servers. When the client connects in, the server that ND selects sends the name to VTAM for dynamic creation. When the client disconnects, VTAM can delete it. This makes it available to be created again through whichever TN3270 server ND selects the next time the client connects in.

Additional Details

The following example shows a VTAM PU definition for DDDLU. Note that several static LUs that require specific LU names and 3270 printers on specific ports are also defined under the same switched major node.

Example:

```
DDDPU VBUILD TYPE=SWNET
DDPU   PU ADDR=02,            x
       IDBLK=077,             x
       IDNUM=22160,           x
       PUTYPE=2,              x
       USSTAB=US327X,         x
       LUGROUP=GROUP1,        x
       LUSEED=DDLU###,        x
       DLOGMOD=D4C32XX3
SALE01  LU   LOCADDR=98,                  x 1
             DLOGMOD=D4C32XX3,            x
             LOGAPPL=CICSA
SALEPRT LU   LOCADDR=99,                  x 2
             LOGMODE=SAL3287,             x
             LOGAPPL=CICSA
```

1 In this sample definition, the LU 'SALE01' was requested to be on LOCADDR=98 because of specific requirements. Therefore, this specific LU is defined under this 'DDDPU' to meet the requirements.

2 In this definition, the printer must also be on a specific address. This especially happens for some SNA applications (e.g. CICS). The application for the sales department needs a printer on address 99, with LOGMODE=SAL3287, and it needs to be connected to application CICSA when it is activated.

For users who wish to write their own or modify one of the VTAM SDDLU exit routines, the router sends LU information in the Reply PSID NMVT as follows:

- SV10, subfield 11 contains one of the device and model type values listed in Table 3.
- SV86, subfield 00 contains IBMTN3270LUNAME to indicate an LU name is being pushed up
- SV86, subfield 10 contains the actual LU name in EBCDIC

An example of these subvectors follows:

```
191000 161103130012F3F2F7F0F0F0F2         (3270 device - mod 2)
1D86   1100C9C2D4E3D5F3F2F7F0D3E4D5C1D4C5 (IBMTN3270LUNAME)
       0A10C1C1C1C1C2C2C2C2               (LU name is AAAABBBB)
```

Table 3. Device/model type Values

Device/Model	NMVT Vector
3270 mod 2 display	3270002
3270 mod 3 display	3270003
3270 mod 4 display	3270004
3270 mod 5 display	3270005
3270 printer	3270P
SCS printer	SCSP

Host-Initiated Dynamic Definition of Dependent LUs (HIDLU)

As summarized in “Defining LUs” on page 73, HIDLU removes the burden of configuring LUs in the router by having the router dynamically create LUs as they are activated from VTAM. This is essentially the opposite of DDDLU, where you configure the LUs in the router and dynamically create them in VTAM. HIDLU allows LUs to be defined in VTAM only. In the router you define only a PU, or as many PUs you need, but no LUs for these PUs.

When VTAM activates the PU and its LUs, the VTAM LU names are conveyed to the router in ACTLU commands in Control Vector 0E. LUs defined in this manner have the same name in both VTAM and the router.

To configure HIDLU in the router, you must still define local dependent PUs in the router either for DLUR or subarea links, as described in “Defining PUs” on page 73. When you configure the DLUR PU or the subarea link, you simply indicate that Host-initiated dynamic LUs should be allowed for this PU. You also indicate whether these dynamic LUs are to be placed in a pool or not, by optionally specifying a pool name. If you do not specify a pool name, the LUs will be treated only as workstation LUs. If you do specify a pool name, you can indicate whether they are workstation or printer LUs. All pooled HIDLU LUs under a given PU must be in the same pool and have the same type. You can use the same pool name for multiple PUs if you want more than 255 LUs in the pool or you want the pool to span multiple subarea links.

If you place HIDLUs into a pool, you do not need to configure clients to explicitly request a particular LU. The clients can request an LU by pool name, using an IP address to pool mapping, or using a TCP port to pool mapping. You can also mix explicit LUs with HIDLU pooled LUs by configuring an individual LU under a PU that is configured with a host-initiated pool. When the ACTLU arrives for the configured individual LU, the router does not create a dynamic LU.

To configure HIDLU in VTAM, you must define the dependent LUs in the major node and specify INCLUD0E=YES on the PU statement. The INCLUD0E keyword is supported by VTAM V4R4 with APARs OW31805 and OW31436. For remote subarea connections through NCP, V7R6 is needed for INCLUD0E keyword support.

If the host is a DLUS and the PU is being serviced by a DLUR in another node, then CV0E of the ACTLU request may not be forwarded to the PU from the DLUR. In this case, the LUs will not be created dynamically. Once LUs have been created dynamically, they can only be removed by rebooting or manually deleting via configuration. If the LU names are changed in the host major node file after the LUs have been created dynamically, the local names in the router will not be changed.

Client to LU Mapping

When a TN3270 client connects to a server, the server must choose an LU to associate with that client, or deny the connection. There are a number of ways you can configure your clients and server to control which LUs will be chosen, and which clients will be denied. The IBM router implementation of TN3270 server supports the following methods:

- The client can request an individual LU name
- The client can request an LU pool name
- You can configure the router to map client IP addresses to configured individual LU or LU pool names
- You can configure the router to associate destination TCP port numbers with configured LU pool names

The following sections describe background concepts, how to configure each of these methods, and how they work.

Concepts

LU Pools and Individual LUs: As described above in “Configured LUs” on page 74, you can configure individual LUs or groups of LUs in the router. In addition, dynamic host-initiated LUs can be treated individually or in groups. An LU pool is simply a named group of LUs. For example, you might call a pool MYPOOLA.

The LUs in a pool can come from one or many different PUs. Except for host-initiated dynamic LUs, the LUs under a PU can be placed in multiple pools. The LUs that you place into a specific pool would typically have similar VTAM definitions and characteristics such as using the same USSMSG10. Using pools is your primary means to group similar LUs together and you will ultimately map a set of like TN3270 client end users to specific pools.

The Global Default Pool: There is always at least one pool defined to TN3270E Server, referred to as the Global Default Pool. You name this pool when you initially configure TN3270E Server, and by default it is named PUBLIC. Whatever you name the default pool, you can refer to that name in other parts of the server configuration using the special character string <DEFLT >. This permits you to later change the pool name in only one place without having to change all references to it. Note however that the string <DEFLT> has special meaning when used in an IP address mapping table entry, so you should be careful to understand that meaning when defining such mappings.

You may not need to have a default pool, but it will exist regardless. You do not, however, have to put any LUs into this pool.

Explicit and Implicit LUs: LUs in the TN3270 server can be divided into two categories, based on how clients are allowed to access them. Implicit LUs are always members of a pool, and clients can access them either by their individual name or by any of the methods that use pool names. You configure implicit LUs either by adding a group of them to a pool, or by adding individual ones to a pool. Explicit LUs are never members of a pool (even the global default pool), so they can be accessed only by clients requesting their individual name, or by IP address mappings to that name. The server function will never assign an explicit LU to a client that requests or is mapped to a pool name.

Clients Requesting LU Names

Client implementations that support RFCs 1646 or 2355 can request a resource name when they connect to a TN3270 server. In the IBM router server, this name is treated either as an individual LU name or as a pool name. In the client configuration, it may be called an LU name even though the same name is configured in the router as a pool name.

If your LU definition method involves different LU names at the router and at VTAM, the name passed by the client must match the router's LU name, not the LU name in VTAM.

In the absence of IP address and TCP port mapping, the server attempts to satisfy the client's request as follows:

- If the client requests a valid individual LU name and it is available, the LU is assigned. If it is not available, the server denies the connection.
- If the client requests a valid pool name and one LU in that pool is available, the LU is assigned. If there are no LUs available, the server denies the connection.
- If the name requested is invalid, the server denies the connection.

See the sections below for what happens when a client a name and one of the mapping methods also applies.

Client IP Address to LU/Pool Mapping

You can configure the router's TN3270 server function to map client IP addresses either to individual LU names or to LU pool names. You may want to do this if your clients do not have the ability to request resource names, or you do not want to configure the clients individually. You may also want to use this function as a security mechanism, to deny connections to any clients that are not on the IP mapping access list.

To configure this mapping function, you first enable it globally as part of overall TN3270 server configuration. If you wish clients connecting to certain server TCP ports to be exempt from IP address mapping, you can disable this function on a port-by-port basis when you configure the ports. You then create a table of IP address mapping entries, each of which maps a set of IP addresses to a single LU or pool name. By default, a given entry applies to all server TCP ports, but you can specify that an entry should be used only for connections made to a certain destination TCP port. This allows you to have clients from different IP networks use the same set of port numbers but map to different LU pools based on both their network and the destination server port number.

The key fields in each mapping entry are: an IP address, and IP address mask, and an LU or LU pool name. The IP address mask indicates which bits of the configured IP address are to be compared against the corresponding bits in the incoming client's source IP address. This allows you to map either individual clients or entire subnets.

For example, if your mapping entry is defined as:

```
IP Address: 1.2.3.4
Subnet Mask: 255.255.255.255
Pool or LU: MYLU
```

If a TN3270 client connects in using IP address 1.2.3.4, then the TN3270E Server will assign MYLU to this client. Here we are mapping an individual IP address to an Individual LU. Specific clients can also be mapped to a pool.

If your mapping entry is defined as:

```
IP Address: 1.2.3.4
Subnet Mask: 255.255.255.0
Pool or LU: YOURPOOL
```

If a TN3270 client connects in using an IP address of 1.2.3.1, or 1.2.3.2, or 1.2.3.3, ..., etc. then TN3270E Server will assign the client an LU from YOURPOOL. Since the subnet mask is 255.255.255.0, all clients in this subnet would match this mapping entry. Masks that are not 255.255.255.255 must be mapped to a pool rather than to an individual LU.

Suppose you define both of the above mapping entries. Note that client 1.2.3.4 would match both of these mapping entries. TN3270E Server will always use the most specific match first. In this example, the client would get mapped to the LU called MYLU.

Suppose again that both of the above mapping entries are defined and client 1.2.3.4 connects in. TN3270 will choose the most specific mapping entry and attempt to connect with the LU called MYLU. However, for some reason the server cannot successfully establish the session with MYLU; MYLU could already be in use, or it may not be activated by VTAM. After unsuccessfully attempting to connect to MYLU, the server normally scans the IP address mapping table to see if there is another less specific match for this client. In our example there is another match and TN3270E Server would connect the client to an LU from YOURPOOL.

There are cases where you may not want the router to use a less-specific match after a more specific match fails. To control this behavior, you can optionally configure an entry as the ″final LU mapping connection attempt″. If this yes/no flag is set, the server function does not look for less specific matches following a failed match on this entry.

The TN3270 server makes the following checks when a client connects to the router and does not pass in a specific name request:

1. If mapping is globally enabled, is mapping enabled on the destination port? If not, incoming requests are treated without using IP address mapping.
2. If so, try to match the incoming client IP address against the mapping entries in this order:
   a. entries for the specific destination port, most specific IP address first

   b. entries for all destination ports, most specific IP address first
3. If there is a match, try to pair the connection with the indicated LU or an LU in the indicated pool, honoring the LU type (workstation or printer) requested by the client
4. If there is a problem and this is not the ″final″ mapping entry, repeat for less specific matches. Continue until all matches are exhausted or the connection is satisfied, before denying the connection.
5. If there is no match at all, deny the connection

When a client connects in and makes a request for a specific name, the matching logic is different. In order to successfully connect, a mapping entry must exist whose IP address and mask match the client and whose resource name is the exact same as the name passed in by the client. If the client requests an individual LU name, that name must be in the mapping table, not just the name of a pool containing that LU. The server does not search the mapping table for the most specific IP address and mask match. If the connection to the LU/pool with the requested name cannot be satisfied, the server does not re-scan the mapping table for other matching entries.

You can use the TN3270 Talk 5 command list mapping to see the order in which mapping entries will be searched. You can put a specific IP address as a parameter to this command, to see only those mapping entries that apply to that IP address.

Here are a number of important additional considerations for constructing IP address mapping entries:

- If you have multiple entries that are equally specific, the most recently defined ones are used first.
- If the global default pool has the name PUBLIC and you configure a mapping entry with the name PUBLIC, the server connects incoming clients to LUs in that pool. If instead you configure a mapping entry with the name <DEFLT>, the server does not connect clients to the PUBLIC pool. Rather, it switches to TCP Port association rules and connects the client to the pool associated with the destination server port to which the client connected.
- The IP address mapping table is initially built by the TN3270E server with a default entry containing the IP address 0.0.0.0, subnet mask 0.0.0.0, and pool name <DEFLT>. This entry will match all incoming client addresses. As mentioned above, it will cause the server to map clients to LUs in the pool associated with the destination TCP port(s). If you prefer not to have this default entry in the LU Name Mapping Table, you can create a similar entry above it mapping to a named pool, and indicate that yours is the last to be searched. If the named pool is the global default pool, you can choose not to configure any LUs in that pool.
- The LU and pool names you configure in IP mapping entries must be configured in the router in order to become active. You cannot, for example, configure individual host-initiated dynamic LU names in IP mapping entries, since these names are not known to the router at initialization time. You can configure HIDLU pool names, however, since these are configured in the router.
- For individual workstation LUs with associated printers, both the workstation and printer LUs need to have an IP mapping table entry with the same client IP address.
- Specifying a port number in an IP address mapping table entry does not cause the TN3270 server to define the port and listen on it for client connections. You must configure the port explicitly (using **add port**) before a reference to it in this table will have any meaning.

Server TCP Port to Pool Association

You can configure the router's TN3270 server function to map incoming client connections to LU pools based on the TCP port number to which the clients are connecting. You may want to do this if your clients do not have the ability to request resource names, or you do not want to configure the clients individually. You may also be migrating an existing network where clients already connect to different TCP port numbers based on application needs.

To configure TCP port to pool association, you specify a pool name with the port when you configure the port (see "Server TCP Ports" on page 72). Clients obviously each have to connect in through one of the defined ports and the server function assigns an LU based on what pool is associated with the port. If you do not specify a pool name for a port, or you give the special value <DEFLT>, the global default pool is associated with that port. This is the same pool you associate with the globally defined server port when you first configure the TN3270 server.

If a client connects in and does not pass a resource name, the TN3270 server function assigns an LU from the pool associated with the destination port. If no LUs are available, the connection is rejected.

If a client connects in and passes a specific LU or LU pool name, the following rules apply:

- If the port is associated with the exact same LU or pool name as that is passed in by the client, then the client will be connected with the LU or an LU from the pool (if available).
- If the port is defined with a null pool name or with the name <DEFLT>, the client will be connected to the specific LU or an LU from the pool that was passed in from the client as long as that exact LU or pool name is configured somewhere in the TN3270E server. An individual LU can be explicit or implicit. The LU or pool type (workstation or SCS printer or 3270 printer) must match the request. If the name is an LU name, it does not matter what pool, if any, the LU is grouped into.
- If neither of the above two conditions apply, or the specified LU(s) are not available, the connection is rejected.

The above description assumes IP mapping is disabled. If IP address mapping is enabled, then by default the IP address mapping function applies to all ports and will override TCP port to pool mapping. You can change this default behavior by disabling IP address mapping on a TCP port basis, as described earlier. Note also the special case where an IP address mapping entry with the <DEFLT> pool can cause LU allocation from the pool associated with the TCP port.

Port and IP Address Mapping Combined

It is possible to use a combination of both IP address mapping and TCP port to pool association. The following is an example of how one user combined these methods to meet their mapping needs.

- The user had IP address mapping enabled and had defined mapping entries to map specific client IP subnets to specific pools.
- The same end user's clients realized a need to occasionally connect to a group of LUs that presented a different USSMSG10 logon screen.
- Since this was the same set of clients, they would be using the same IP addresses, so adding additional mapping entries to the IP address mapping table would not resolve their needs.

- The user defined a new pool of LUs, defined a new port and associated it with the new pool. Also, they defined this new port not to use the IP address mapping table since that would result in using the original pools.
- The clients were then configured at the end user workstations to connect to the new port.

Load Balancing among Multiple PUs

It is common to define a large pool of LUs that reside in multiple PUs. Any pool with more than 255 LUs must include more than one PU. Spreading a pool's LUs across multiple PUs can lessen the number of clients affected by any given link or PU failure. How the server allocates LUs from among these multiple PUs also determines how many clients are affected by a link or PU failure. For example, if the server allocated all the LUs in one PU before allocating any from the second PU, failure of the first might affect as many as 255 clients needlessly.

The IBM router implementation of TN3270 generally does round-robin allocation of LUs from among multiple PUs in a pool. All other things being equal, it will allocate LU1 from PU1, LU1 from PU2, and so on. At the same time the allocation algorithm favors those PUs that are currently active (avoiding the delay of an activation attempt), and it favors LUs that provide an exact match to the model type requested by the client.

The rules for LU selection are as follows:

- An exact match based on model type is always returned if found in an active PU.
- If an exact match can't be found in an active PU, then an acceptable LU in an active PU will be returned before an exact match in an inactive PU
- To be an "acceptable" match, the LU type (workstation, SCS printer, or 3270 printer) must match what the client is requesting. The model type for a workstation LU must give the same or a smaller screen size than that requested by the client. For example, if a client requested a mod 4, a mod 4 LU would be an exact match, and mod 3 or mod 2 LUs would be acceptable matches.

Based on whether an exact or acceptable match is found, PUs are moved on a list to provide general round-robin allocation while keeping less desirable PUs from always being searched first.

Example Configurations

This section contains sample VTAM and router command-line configurations for basic TN3270 server scenarios. For more advanced scenarios and Configuration Program information, see "Other Example Configurations" on page 88.

Configuring TN3270 using DLUR

If you are using DLUR to communicate with the host, the local PUs used by the TN3270E Server need to be configured in the host as DLUR internal PUs. The following code is an example of the host VTAM configuration:

```
PUJOE7      PU        ADDR=12,
                      IDBLK=077, IDNUM=EEEE7,  1
                      MAXPATH=8,
                      ISTATUS=ACTIVE,
                      MODETAB=LMT3270,
                      USSTAB=STFTSNA2,
                      ANS=CONT,
                      MAXDATA=521,
                      IRETRY=YES,
                      MAXOUT=7,
```

```
                        DLOGMOD=G22NNE,
                        NETID=STFNET,
                        PASSLIM=5,
                        PUTYPE=2
 JCPATH7    PATH        PID=1,
                        DLURNAME=VLNN01,
                        DLCADDR=(1,C,INTPU),
                        DLCADDR=(2,X,07711111)
 JC7LU2     LU           LOCADDR=2
 JC7LU3     LU           LOCADDR=3
 JC7LU4     LU           LOCADDR=4
 JC7LU5     LU           LOCADDR=5
 JC7LU6     LU           LOCADDR=6
```

Note: **1** 07711111 represents the ID block/ID number of the local PU. The 077 part of this value is not configurable at the router.

The following example shows how to configure the router to use an upstream DLUR connection for TN3270, using the command line.

```
APPN config>
APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [STFNET]?
Control point name (Max 8 characters) [VLNN2]?
Enable branch extender (Y)es (N)o [N]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
APPN config>
APPN config>
APPN config>set dlur
Enable DLUR (Y)es (N)o [Y]?
Fully-qualified CP name of primary DLUS [STFNET.MVS8]?
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds)[120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.
APPN config>
APPN config>tn3270e
TN3270E config>set
TN3270E Server Parameters
    Enable TN3270E Server (Y/N) [Y]?
    TN3270E Server IP Address[4.3.2.1]?
    Port Number[23]?
    Enable Client IP Address to LU Name Mapping (Y/N) [N]
    Default Pool Name[PUBLIC]?
    NetDisp Advisor Port Number[10008]?
    Keepalive type:
     0 = none,
     1 = Timing Mark,
     2 = NOP[2]?
    Frequency ( 1 - 65535 seconds)[60]?
    Automatic Logoff (Y/N)[N]?
Write this record?[Y]?
The record has been written.
```

```
TN3270E config>exit
APPN config>
APPN config>add loc
Local PU information
     Station name (Max 8 characters) []? link1
     Fully-qualified CP name of primary DLUS[STFNET.MVS8] ?
     Fully-qualified CP name of a backup DLUS[]?
     Local Node ID (5 hex digits)[11111]?
     Autoactivate (y/n)[Y]?
Write this record?[Y]?
The record has been written.


APPN config>tn3270
TN3270E config>add im
TN3270E Server Implicit definitions
     Pool name (Max 8 characters)[<DEFLT>]?
     Station name (Max 8 characters)[]? link1
     LU Name Mask (Max 5 characters) [@01LU]?
     LU Type     ( 1 - 3270 mod 2 display
                   2 - 3270 mod 3 display
                   3 - 3270 mod 4 display
                   4 - 3270 mod 5 display) [1]?
     Specify LU Address Range(s) (y/n) [n]
     Number of Implicit LUs in Pool(1-255) [50]?
Write this record?[Y]?
The record has been written.
TN3270E config>
TN3270E config>add lu
TN3270E Server LU Definitions
     LU name(Max 8 characters) []? printer1
     NAU Address (1-255) [0] 2
     Station name (Max 8 characters) []? link1
         Class:
          1 = Explicit Workstation,
          2 = Implicit Workstation,
          3 = Explicit Printer,
          4 = Implicit Printer[3]?
     LU Type ( 5 - 3270 printer
               6 - SCS printer) [5]?
Write this record[Y]?
The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: N        Timeout: 30
        Enable IP Precedence: N
Link Station: link1
        Local Node ID: 11111
        Auto activate : YES
        Implicit Pool Informationø
                Number of LUs: 50
                LU Mask: @01LU
        LU Name   NAU addr     Class             Assoc LU Name   Assoc  NAU addr

        ---------------------------------------------------------------- --------
        printer1      2       Explicit Printer

TN3270E config>exit
APPN Config>exit
```

```
Config>
Config>p ip
Internet protocol user configuration
IP config>li all
Interface addresses
IP addresses for each interface:
   intf  0   9.1.1.20        255.0.0.0        Local wire broadcast, fill 1
   intf  1                                    IP disabled on this interface
   intf  2                                    IP disabled on this interface
Internal IP address: 4.3.2.1

Routing

Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
TFTP Server: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: disabled
BGP: disabled
RIP: disabled

IP config>
*
```

Configuring TN3270E Using a Subarea Connection

The following example shows how to configure the router to use an SNA subarea (non-APPN) upstream host connection for TN3270, using the command line. In this example, the router appears to VTAM as multiple downstream PUs.

```
Config>p appn
APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [STFNET]?
Control point name (Max 8 characters) [VLNN2]?
Enable branch extender (Y)es (N)o [N]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
APPN config>


APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  []?fr
Interface number(Default 0): [0]? 2
Port name (Max 8 characters) [F00002]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
    Support multiple subarea (Y)es (N)o [N]? y
All active port names will be of the form <port name sap>
    Service any node: (Y)es (N)o [Y]?
    High performance routing: (Y)es (N)o [Y]? n
    Maximum BTU size (768-8136) [2048]?
    Percent of link stations reserved for incoming calls (0-100) [0]?
```

```
    Percent of link stations reserved for outgoing calls (0-100) [0]?
    Local SAP address (04-EC) [4]?
    Support bridged formatted frames: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>add link
APPN Station
Port name for the link station [ ]? f00002
Station name (Max 8 characters) [ ]? suba1
    Activate link automatically (Y)es (N)o [Y]?
    DLCI number for link (16-1007) [16]? 23
    Adjacent node type: 0 = APPN network node,
    1 = APPN end node or Unknown node type,
    2 = LEN end node [0]?
    Solicit SSCP Session: (Y)es (N)o [N]? y
         Local Node ID (5 hex digits) [00000]? 12345
    Local SAP address (04-EC) [4]? c
    Allow CP-CP sessions on this link (Y)es (N)o [Y]? n
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
APPN config>act

APPN config>
APPN config>tn3270e
TN3270E config>set
TN3270E Server Parameters
    Enable TN3270E Server (Y/N) [Y]?
    TN3270E Server IP Address[4.3.2.1]?
    Port Number[23]?
    Enable Client IP Address to LU Name Mapping (Y/N) [N]
    Default Pool Name[PUBLIC]?
    NetDisp Advisor Port Number[10008]?
    Keepalive type:
     0 = none,
     1 = Timing Mark,
     2 = NOP[2]?
    Frequency ( 1 - 65535 seconds)[60]?
    Automatic Logoff (Y/N)[N]?
Write this record?[Y]?
The record has been written.
TN3270E config>exit
APPN config>
Write this record?[Y]?
The record has been written.


APPN config>tn3270
TN3270E config>add im
TN3270E Server Implicit definitions
     Pool name (Max 8 characters)[<DEFLT>]?
     Station name (Max 8 characters)[]? suba1
     LU Name Mask (Max 5 characters) [@01LU]?
     Specify LU Address Range(s) (y/n) [N]
     Number of Implicit LUs in Pool(1-255) [50]?
Write this record?[Y]?
The record has been written.
TN3270E config>
TN3270E config>add lu
TN3270E Server LU Definitions
     LU name(Max 8 characters) []? printer1
     NAU Address (1-255) [2]
```

```
     Station name (Max 8 characters) []? suba1
         Class:
          1 = Explicit Workstation,
          2 = Implicit Workstation,
          3 = Explicit Printer,
          4 = Implicit Printer[3]?
          LU Type ( 5 - 3270 printer
                    6 - SCS printer) [5]?
Write this record[Y]?
The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: N        Timeout: 30
        Enable IP Precedence: N
Link Station: suba1
        Local Node ID: 12345
        Auto activate : YES
        Implicit Pool Informationø
                Number of LUs: 50
                LU Mask: @01LU
        LU Name   NAU addr     Class            Assoc LU Name   Assoc  NAU addr

        ------------------------------------------------------------- --------
        printer1      2       Explicit Printer

TN3270E config>exit
APPN Config>exit

APPN config>act
```

Other Example Configurations

The TN1 model of the Network Utility product was designed to be used as a TN3270 server, and it shipped with example TN3270 configuration information that can be helpful to users of the 2216, 2212, and 2210. This information is available both in product publications and in example binary configuration files on the Web.

The publication *Network Utility: Installation, Getting Started, and User’s Guide*, GA27-4167-02, documents the router configuration (usually both the command-line and Configuration Program) and sample VTAM configurations for the following network configurations:

- Subarea host connection through token-ring to an NCP (same for channel gateway or OSA)
- Parallel subarea TN3270 servers load balanced by two Network Dispatcher routers
- DLUR host connection through token-ring to a Network Node
- DLUR host connection through Enterprise Extender to an IBM router or gateway
- Dynamic definition of dependent LUs (DDDLU)
- Host-initiated Dynamic LU Definition (HIDLU)
- Host On-Demand (HOD) Client Cache
- Subarea host connection over DLSw
- Subarea host connection over channel via LSA loopback

Some of the above configurations are supplemented on the Web by both router-format and Configuration Program-format binary configuration files. Use your browser to reach these as follows:

1. Open the Network Utility downloads page at: **http://www.networking.ibm.com/support/downloads/networkutility**
2. Follow the link to ″Configuration Program″ files
3. Find the code release you are using (the file contents have already been upgraded for each release)
4. Open the package named ″Example Configuration Files″

Some of the documentation tables are specific to Network Utility because that product pre-sets certain configurable tuning parameters. To understand how to map the documentation to a IBM 2212 of similar memory capacity, read the instructions in the ″Example Configuration File″ Web packages mentioned above. The Configuration Program format files may be usable only on a Network Utility, except as an example you can browse using the Configuration Program.

Chapter 3. 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 92
- "APPN Dynamic Reconfiguration Support" on page 252

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 4. 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 xxviii.	
Enable/Disable	Enables/disables the following:	92
	APPN	
	Dependent LU Requestor	
	Port *port name*	
Set	Sets the following:	
	Node	93
	Traces	112
	HPR	98
	DLUR	102
	Management	132
	Tuning	107
Add	Adds or updates the following:	
	Port *port name*	136
	Link-station *link station name*	153
	LU-Name *LU name*	173
	Connection-network *connection network name*	174
	Additional-port-to-connection-network	180
	Mode	179
	Focal_point	181
	local-pu	182
	Routing_list	185
	COS_mapping_table	189

Table 4. 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 • Routing_list • COS_mapping_table	190
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 • Routing_list • COS_mapping_table	191
Activate_new_config	Reads the configuration into non-volatile configuration memory.	191
TN3270	Accesses the `TN320E config>` command prompt	191
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxviii.	

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 5. 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, Frame Relay and PPP direct DLC ports.
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 5. 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 or border node **Valid Values** 0 (enable neither) 1 (enable branch extender) 2 (enable border node) **Default** 0 **Description** This parameter specifies whether branch extender function, border node function, or neither will be enabled on this node. If either function is enabled, appropriate additional questions will be asked.

Table 5. Configuration Parameter List - APPN Routing (continued)

Parameter Information
Parameter Enable Branch Awareness Support **Valid Values** 0 (Full), 1 (Partial), 2 (None) **Default** 0 (Full) **Description** This parameter specifies whether you want to limit the flow of topology information regarding Branch Extender topology. *Full* means that the node will broadcast all Branch Extender TGs into the network when they are learned. *Partial* means that the node will not broadcast local Branch Extender topology, but will store and broadcast non-local Branch Extender topology. *None* means that the node will not broadcast local Branch Extender topology and it will ignore any Branch Extender topology received from the network and the node will not store or broadcast non-local Branch Extender topology.
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. **Note:** This question is asked only if **Enable Branch Extender or Border Node** parameter is set to *branch extender*.
Parameter Subnet visit count **Valid Values** 1 — 255 **Default** 3 **Description** Specifies the node level default for the maximum number of subnetworks that a multi-subnetwork session may traverse. The default may be overridden as part of port, link, or routing list configuration. **Note:** This is the first of the questions asked only if border node has been enabled.

Table 5. Configuration Parameter List - APPN Routing (continued)

Parameter Information
Parameter Cache searches for (0-255) minutes **Valid Values** 0 - 255 **Default** 8 **Description** Specifies how many minutes the BN retains information in the multi-subnet search cache once the search terminates.
Parameter Maximum number of searches in cache **Valid Values** 0 - 32765 (0=unlimited) **Default** 0 **Description** Specifies the maximum number of entries in the multi-network search cache. Once this limit is reached, the oldest entries are discarded. **Note:** The primary mechanism for deletion of these entries is the cache search time value specified in **cache searches for (0–255) minutes**.
Parameter Dynamic routing list updates **Valid Values** 0 (none) - No dynamic entries are added. 1 (full) - All native border nodes, all adjacent non-native border and network nodes, and nodes that know of similarly named destination LUs are added. 2 (limited) - All native border nodes, all adjacent non-native border nodes and network nodes ***with the same NETID***, and nodes that know of similarly named destination LUs are added. **Default** 2 **Description** Indicates the degree to which, if any, that a BN can supplement configured routing list data with topology data learned by the operational code. This supplemental data is not saved in SRAM.

Table 5. Configuration Parameter List - APPN Routing (continued)

Parameter Information
Parameter Enable routing list optimization **Valid Values** Yes or No **Default** Yes **Description** Indicates whether or not a BN may reorder the operational code's temporary copy of a subnetwork routing list so that entries that are more likely to be successful are found first.
Parameter Load balance across parallel inter-subnet boundaries **Valid Values** Yes or No **Default** No **Description** This parameter specifies whether the router should attempt to balance the number of sessions across two or more parallel inter-subnet exit points when it is functioning as an EBN. The relevant configuration has two or more IBM routers serving as EBN exit points in one subnet, with the same number in the other subnet. Each router has an inter-subnet TG to a different router in the other subnet, forming two or more parallel links. (Note that these are not parallel TGs between any two routers.) To configure session load balancing among the parallel exit points: 1. Set this parameter to *yes*. 2. Configure routing lists (see 188) in each EBN router, so that sessions for different destination LU names have different preferred exit EBNs. You also configure the preferred inter-subnet boundary and can set backup paths. 3. Configure the routing lists with **dynamic routing list updates** set to *none*, and **Enable routing list optimization** set to *no*. **Note:** This is the last of the questions asked only if border node has been enabled.
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.

Table 5. Configuration Parameter List - APPN Routing (continued)

Parameter Information
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 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.

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 6. Configuration Parameter List - High-Performance Routing (HPR)

Parameter Information
Parameter Maximum sessions for HPR connections **Valid Values** 1 to 65 535 **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 7. Configuration Parameter List - HPR Timer and Retry Options

Parameter Information
Low 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 *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

Table 7. 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 *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.
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.

Table 7. 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 high 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 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.

Table 7. 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 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 8. 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.

Table 8. Configuration Parameter List - Dependent LU Requester (continued)

Parameter Information
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.
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.

Table 8. Configuration Parameter List - Dependent LU Requester (continued)

Parameter Information
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 34 for a description of the retry algorithm.
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 34 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 34 for a complete description of the retry algorithm.

Table 8. Configuration Parameter List - Dependent LU Requester (continued)

Parameter Information
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 34 for a complete description of the retry algorithm.
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 34 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 34 for a complete description of the retry algorithm.

Table 8. Configuration Parameter List - Dependent LU Requester (continued)

Parameter Information
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 34 for a complete description of the retry algorithm.
Parameter Take down the dependent link when there is no session **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether the router should deactivate the link to a dependent PU when the PU is deactivated and there are no active LU-LU sessions on it. Set this parameter to *yes* if you have an older SNA product that doesn't support receiving ACTPU following a DACTPU, without an intervening link deactivation. Such a product would appear hung after a deactivate/activate sequence.

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 9. Configuration Parameter List - APPN Node Tuning

Parameter Information
Parameter Maximum number of adjacent nodes **Valid Values** 1 to 8 000 **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 9. Configuration Parameter List - APPN Node Tuning (continued)

Parameter Information
Parameter Maximum number of ISR sessions **Valid Values** 10 to 60 000 **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 9. 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 9. Configuration Parameter List - APPN Node Tuning (continued)

Parameter Information
Parameter Override tuning algorithm **Valid Values** Yes, No **Default Value** Yes **Description** When enabled, this parameter overrides the tuning calculations generated by the tuning input parameters and enables you to specify explicit values for the Maximum shared memory parameter, the percent buffer 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 9. Configuration Parameter List - APPN Node Tuning (continued)

Parameter Information
Parameter Maximum shared memory **Valid Values** 0 - 16 777 215 KB **Default Value** Auto-configured (configure based on installed memory) **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 either input a value in Kilobytes, or select to have the router pick a reasonable general purpose default value at boot time based on its installed memory. Note that the default value the router chooses is not based on the size of the APPN configuration. Default values assume you are running a medium-size APPN or TN3270 network, and some other non-trivial routing function. The default value may not fit if you also configure another extremely memory-intensive router function. As you select the *auto-configured* value from the command-line prompt, you can see what this value will be if you boot the configuration on the router you are using. If you select this value from the Configuration Program, you must download and activate the configuration before you can see what the result will be. This parameter is configurable using the Configuration Program and from the command line.
Parameter Percent of APPN shared memory to be used for buffers **Valid Values** 5 to 50 **Default** 11% 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 4KB RU size by setting *maximum shared memory* to at least 1 MB, and setting *percent of APPN shared memory used for buffers* to a sufficiently large value to allow at least 1 MB of memory to be available to the buffer manager. This parameter is configurable using the Configuration Program and from the command line.

Table 9. Configuration Parameter List - APPN Node Tuning (continued)

Parameter Information
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 the command line.

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 10. 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 11 on page 113 for the set of questions you will be asked if this option is enabled.

Table 10. Configuration Parameter List - Trace Setup Questions (continued)

Parameter Information
Parameter Edit Interprocess Signals **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. See Table 12 on page 118 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 13 on page 122 for the set of questions you will be asked if this option is enabled.
Parameter Edit General **Valid Values** Yes, No **Default Value** No **Description** This parameter enables or disables this APPN trace option. See Table 14 on page 124 for the set of questions you will be asked if this option is enabled.

Table 11. 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.

Table 11. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
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.
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.

Table 11. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
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.
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.

Table 11. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
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.
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.

Table 11. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
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.
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.

Table 11. Configuration Parameter List - Node Level Traces (continued)

Parameter Information
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 12. 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.

Table 12. Configuration Parameter List - Inter-process Signals Traces (continued)

Parameter Information
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.
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.

Table 12. Configuration Parameter List - Inter-process Signals 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 inter-process signals 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 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.

Table 12. Configuration Parameter List - Inter-process Signals Traces (continued)

Parameter Information
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.
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.

Table 12. Configuration Parameter List - Inter-process Signals Traces (continued)

Parameter Information
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.
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 13. 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.

Table 13. Configuration Parameter List - Module Entry and Exit Traces (continued)

Parameter Information
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.
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.

Table 13. Configuration Parameter List - Module Entry and Exit Traces (continued)

Parameter Information
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.
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 14. 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.

Table 14. Configuration Parameter List - General Component Level Traces (continued)

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 general information from the address space manager component.
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.

Table 14. Configuration Parameter List - General Component Level 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 general information from the directory services 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 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.

Table 14. Configuration Parameter List - General Component Level Traces (continued)

Parameter Information
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.
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.

Table 14. Configuration Parameter List - General Component Level Traces (continued)

Parameter Information
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.
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.

Table 14. Configuration Parameter List - General Component Level Traces (continued)

Parameter Information
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.
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 15. 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 Trace RTP Headers **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace all headers of RTP flows. This option is available only if **Data link control transmissions and receptions** is *yes*.

Table 15. Configuration Parameter List - Miscellaneous Traces (continued)

Parameter Information
Parameter Include payload in RTP trace **Valid Values** Yes, No **Default Value** No **Description** If this parameter is enabled, the APPN trace facility will trace the payload data in RTP flows. This option is available only if **trace RTP headers** is *yes*.
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*
Parameter Length to trace **Valid Values** 1 - 3600 **Default Value** 100 **Description** This parameter specifies the number of bytes of trace data to accumulate.

Table 15. Configuration Parameter List - Miscellaneous Traces (continued)

Parameter Information
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.
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.

Table 15. Configuration Parameter List - Miscellaneous Traces (continued)

Parameter Information
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 16. 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.
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.

Table 16. Configuration Parameter List - APPN Node Management (continued)

Parameter Information
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.
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 17. Configuration Parameter List - APPN ISR Recording Media

Parameter Information
Memory Parameters

Table 17. Configuration Parameter List - APPN ISR Recording Media (continued)

Parameter Information
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.
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.

Table 17. Configuration Parameter List - APPN ISR Recording Media (continued)

Parameter Information
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 Topology safe store **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether the topology data base is to be saved on the hardfile. This function is not supported if compact Flash memory is used. It can only be used when a hardfile is present.
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 16 on page 132) 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 18. Configuration Parameter List - Port Configuration

Parameter Information
Parameter Link type **Valid Values** Ethernet (E) Token ring (T) DLSw (D) PPP (P) Frame relay (F) SDLC (S) X.25 (X) IP **Default Value** None **Description** This parameter specifies the type of link associated with this port.
Parameter Interface number **Valid Values** 0 to 65 533 **Default Value** 0 **Description** This parameter defines the physical interface number of the hardware interface to which this device is attached.

Table 18. 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 • FR (Frame Relay) • X25 (X.25) • SDLC (SDLC) • PPP (point-to-point) • 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.
Parameter Support multiple PU **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether the port will support multiple subarea.

Table 18. 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 Treat non-configured callers as LEN nodes **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether APPN should treat dynamic Network Node callers that do not request CP-CP sessions as LEN nodes. It is applicable only if **service any node** is *yes*. If this parameter is *yes*: • the router treats the adjacent node as a LEN node regardless of the node type in the received XID3 • the router sends XID3s stating that the router is a LEN node (an EN with no CP-CP session and no HPR support)
Parameter High-performance routing (HPR) supported **Valid Values** Yes, No **Default Value** Yes for token-ring, Ethernet, Frame Relay, and PPP ports. **Description** This parameter indicates whether link stations on this port will support HPR. This value may be overridden on the link station definition.

Table 18. Configuration Parameter List - Port Configuration (continued)

Parameter Information
Parameter IPv4 Precedence **Valid Values** Yes or No **Default Value** No **Description** This parameter sets the IPv4 precedence value, which allows BRS precedence filtering of IPv4 encapsulated packets.
Parameter Limited Resource (PPP and FR over dial circuits only) **Valid Values** Yes, No **Default Value** If the dial circuit is *dial on demand*, the default is Yes. Otherwise, the default is No. **Description** This parameter specifies whether link stations on this port are a limited resource. This value may be overridden on the link station definition.
Parameter Support bridged formatted frames (Frame relay only) **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether the Frame Relay port will support bridged formatted frames. If you are configuring Frame Relay to support bridged format, you will also need to configure a boundary node identifier.
Parameter Boundary node identifier (Frame Relay only) **Valid Values** X'0000 0000 0001' to X'7FFF FFFF FFFF' **Default Value** X'4FFF 0000 0000' **Description** This parameter specifies the boundary node identifier MAC address. The router uses this MAC address to recognize that the frame is a Frame Relay bridged frame destined for APPN.

Table 18. Configuration Parameter List - Port Configuration (continued)

Parameter Information
Parameter Subnet visit count **Valid Values** 1 - 255 **Default Value** Default taken from the equivalent node level parameter **Description** This parameter specifies this port's default for the maximum number of subnetworks that a multi-subnet session may traverse. **Note:** This question is asked only if the border node function is enabled on this node.
Parameter Adjacent node subnet affiliation **Valid Values** • 0 (native) • 1 (non-native) • 2 (negotiable) **Default Value** 2 **Description** This parameter specifies the default for all links through this port as to whether the adjacent node is in this node's native APPN subnetwork or in a non-native APPN subnetwork. A value of *2* instructs the node to negotiate at link activation time to determine whether the adjacent link station is native or non-native. **Note:** This question is asked only if the border node function is enabled on this node.

Table 19. Configuration Parameter List - Port Definition

Parameter Information
Parameter Maximum BTU size **Valid Values** 768 to 1496 bytes for Ethernet 768 to 17 745 bytes for token-ring 768 to 4096 bytes for IP 768 to 8136 bytes for Frame Relay 768 to 8132 bytes for Frame Relay over ISDN and V.25 bis 768 to 4086 bytes for PPP 768 to 4082 bytes for PPP over ISDN and V.25 bis X.25 will take value from network level 768 to 2048 bytes for all other ports **Default Value** 1289 bytes for Ethernet 2048 bytes for token-ring 1469 bytes for IP 2048 bytes for Frame Relay or PPP 2044 bytes for Frame Relay or PPP over ISDN and V.25 bis 2048 bytes for SDLC X.25 will take value from network level **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 127 for SDLC ports | 1 to 65 535 for all other ports **Default Value** | If SDLC is configured as multipoint and primary, then this parameter defaults to 127. **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 19. Configuration Parameter List - Port Definition (continued)

Parameter Information
Parameter Percent of link stations reserved for incoming calls (Ethernet, token-ring, FR, X.25 only) **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%. If SDLC primary and multipoint, then valid value is 100. **Default Value** 0 If SDLC primary and multipoint, then default value is 100. **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 65 535 **Default Value** 11 000 **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 19. Configuration Parameter List - Port Definition (continued)

Parameter Information
Parameter UDP port number for network priority traffic **Valid Values** 1024 to 65 535 **Default Value** 11 001 **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 65 535 **Default Value** 11 002 **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 65 535 **Default Value** 11 003 **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 65 535 **Default Value** 11 004 **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 19. 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 (Ethernet and token-ring only) **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 20. Configuration Parameter List - Port Default TG Characteristics

Parameter Information	
Parameter	Cost per connect time
Valid Values	0 to 255
Default Value	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.
Parameter	Cost per byte
Valid Values	0 to 255
Default Value	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 20. 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 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 20. 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 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 20. 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** FR=X'45' (64 kbps) PPP=X'45' (64 kbps) DLSw=X'75' (4 Mbps) SDLC=X'45' (64 kbps) X.25=X'45' (64 kbps) Token ring: X'75' when minimum is 4 Mbps Token ring: X'85' when minimum is 16 Mbps Ethernet/802.3 ports: X'80' for 10 Mbps 100Mbps Ethernet: X'9A' 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.
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.

Table 20. Configuration Parameter List - Port Default TG Characteristics (continued)

Parameter Information
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 21. 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.

Table 21. Configuration Parameter List - Port default LLC Characteristics (continued)

Parameter Information
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.
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).

Table 21. Configuration Parameter List - Port default LLC Characteristics (continued)

Parameter Information
Parameter Reply timer (T1) **Valid Values** 1 to 254 seconds **Default Value** 2 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).
Parameter Receive acknowledgment timer (T2) **Valid Values** 1 to 254, measured in tenths of a second **Default Value** 1 **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.

Table 21. Configuration Parameter List - Port default LLC Characteristics (continued)

Parameter Information
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 22. 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.
Parameter Reply timer override for HPR (HPR T1) **Valid Values** 1 to 254 seconds **Default Value** 2 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.

Table 22. Configuration Parameter List - HPR Override Defaults (continued)

Parameter Information
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 23. 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 23. 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) • FR (Frame Relay) • X25 (X.25) • SDLC (SDLC) • PPP (point-to-point) • IP 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.
Parameter Link type (X.25 only) If *limited resource* = yes is configured for this link station, then the link type parameter defaults to a value of 1 (SVC) and is not configurable. **Valid Values** If PVC, then specify a logical channel number in the range of 1 - 4095 If SVC, then specify a DTE address that is variable length up to 15 digits **Default Value** 0, unless it is a limited resource. **Description** This parameter specifies whether the X.25 link is a PVC or SVC.

Table 23. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter MAC address of adjacent node (required) (Ethernet, token-ring, DLSw, FR bridged format only) **Valid Values** Token-ring and DLSw ports: • 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} **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 (Enterprise Extender only) **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 23. 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.
Parameter XID node identification **Valid Values** A string of 8 hex digits (0-F) **Default Value** X'00000000' **Description** This parameter specifies the ID block and ID number fields that identify the adjacent node. It is applicable only when the **Adjacent node type** field is set to *LEN end node*. If you choose *yes* for **replace inbound XID3 CP name and XID with configured values**, the value of this field replaces the corresponding parameters in the received XID.

Table 23. 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 Replace inbound XID3 CP name and XID with configured values **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether or not the router should override the node id and CP name parameters received in XIDs from a configured LEN node. It is applicable only when the **adjacent node type** field is set to *LEN end node*. If you have a large number of LEN nodes that are not configured adequately to participate in a full APPN network, you can configure their identity at the router and have the router override the values in their XIDs before forwarding those XIDs on.

Table 23. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
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.
Parameter Retry link activation unconditionally **Valid Values** Yes, No **Default Value** No **Description** This parameter specifies whether or not the router should always try to reactivate the link regardless of the cause of link failure. It is applicable only for dial-out capable links where **activate link automatically** is *yes*. Normally if a link fails to start or comes down due to some event other than an operator command, the router selectively chooses whether to reactivate it. If the failure cause is likely to require reconfiguration of one of the two nodes, the router does not automatically restart the link. This avoids a periodic repeat (with logging, alerting, etc.) of the unsuccessful connection attempt. If you want to override this behavior and have links always attempt to reconnect, select *yes* for this parameter.
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.

Table 23. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
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.
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.

Table 23. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter DLCI number for link (Frame Relay only) **Valid Values** 16 to 1007 **Default Value** 16 **Description** The DLCI parameter identifies the frame-relay logical data link connection with the adjacent node.
Parameter Station address of adjacent node (SDLC only) **Valid Values** Address in the range of (1 - FE) **Default Value** C1 **Description** This parameter specifies the address of the adjacent node.
Parameter Limited Resource (PPP, X.25 FR over dial circuits) **Valid Values** Yes, or No **Default Value** No If the *link type* is PPP or FR, the default will be taken from the *limited resource* parameter for the associated port. **Description** This parameter specifies whether the TG for this link station is a limited resource. If you answer *yes*, then the **Virtual Channel Type** is *SVC*.
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*

Table 23. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
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.
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** If *limited resource* is Yes, valid values are 1 - 20. If *limited resource* is No and *link type* is X.25 SVC, valid values are 0 - 20. Otherwise, valid values are 0 - 20. **Default Value** If *limited resource* is Yes, default is 1. If *limited resource* is No, default is 0. Otherwise, default value is 0. **Description** This parameter uniquely identifies a TG between adjacent nodes.

Table 23. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter Solicit SSCP session **Valid Values** Yes or No **Default Value** No If the **link station name** is the same as the **CP name**, then the default is *yes*. **Description** This parameter indicates whether this link is to solicit SSCP sessions.
Parameter Local Node ID **Valid Values** 5 hexadecimal digits **Default Value** X'00000' **Description** This parameter specifies the local node identifier that represents the local dependent PU to VTAM. This question is asked only if Solicit SSCP session is yes. The local node id must be unique.
Parameter Enable Host Initiated Dynamic LU Definition **Valid Values** Yes or No **Default Value** No **Description** This parameter indicates whether or not dependent LUs will be created dynamically (as opposed to having to be configured.) If *yes* is specified, LUs will be defined for this PU as ACTLU requests (with CV0E) are received. With this feature, LUs for the TN3270E Server do not have to be configured. **Note:** This question is asked only if Solicit SSCP session is yes.

Table 23. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information

Parameter
Pool Name for Host-initiated Dynamic LUs

Valid Values
A string of 1 to 8 characters:

- First character: A to Z, $, #, @, or <
- Second to eighth characters: A to Z, 0 to 9, $, #, @, >, or <

Default Value
None

Description
This parameter specifies the name of a pool to be created to contain LUs that the host activates on this subarea link. This parameter is applicable only if **Solicit SSCP session** is *yes*, and **Enable Host Initiated Dynamic LU Definition** is *yes*.

You do not need to use the **add implicit-pool** command to define this pool; specifying the name and other parameters here is sufficient to cause the pool to be created. If you do enter a pool name, you will be prompted to enter values for the following parameters:

- Pool class (See Table 39 on page 196)
- LU type (See Table 39 on page 196)

You can provide the same pool name for multiple subarea links, if you wish.

By specifying pool information, you cause host-initiated LUs that are not already configured at the router to be placed into the specified pool. TN3270 clients can then be assigned to them by requesting the pool name, or by mapping client IP addresses or destination ports to that pool.

If you do not specify pool information, these host-initiated LUs are treated as explicit LUs and can only be assigned to clients that request them by their individual LU names.

Parameter
Local SAP address

Valid Values
Any valid SAP address between X'04' and X'EC'.

Default Value
Value taken from port

Description
This parameter specifies local SAP address.

Notes:

1. This question is displayed only if there are multiple PUs defined on the port.
2. If the local SAP address is not the main local SAP address on the port,
3. the port name and SAP name will display in monitoring and SNMP display output.

Table 23. Configuration Parameter List - Link Station - Detail (continued)

Parameter Information
Parameter Send Terminate-Self when TN3270 Client Disconnects **Valid Values** Yes or No **Default Value** No **Description** This parameter indicates whether or not a terminate_self request will be sent to the SSCP when the TN3270 client disconnects. If *yes* is specified, terminate_self will be sent and the host will be responsible for terminating the LU-LU session (i.e., the SLU will NOT send an UNBIND request.)
Parameter Subnet visit count **Valid Values** 1 - 255 **Default Value** Default taken from the equivalent port level parameter **Description** This parameter specifies the default for the maximum number of subnetworks that a multi-subnet session may traverse. **Note:** This question is asked only if the border node function is enabled on this node.
Parameter Adjacent node subnet affiliation **Valid Values** • 0 (native) • 1 (non-native) • 2 (negotiable) **Default Value** Default is taken from the equivalent port level parameter **Description** This parameter specifies whether the adjacent node is in this node's native APPN subnetwork or in a non-native APPN subnetwork. A value of *2* instructs the node to negotiate at link activation time to determine whether the adjacent link station is native or non-native. **Note:** This question is asked only if the border node function is enabled on this node.

Table 24. 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.
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.

Table 24. Configuration Parameter List - Modify 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** 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.
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.

Table 24. Configuration Parameter List - Modify TG Characteristics (continued)

Parameter Information
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 25. 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.

Table 25. Configuration Parameter List - Modify Dependent LU Server (continued)

Parameter Information
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 26. 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.

Table 26. Configuration Parameter List - Modify LLC Characteristics (continued)

Parameter Information
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.
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).

Table 26. Configuration Parameter List - Modify LLC Characteristics (continued)

Parameter Information
Parameter Reply timer (T1) **Valid Values** 1 to 254 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).
Parameter Receive acknowledgment timer (T2) **Valid Values** 1 to 254, measured in tenths of a second **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.

Table 26. Configuration Parameter List - Modify LLC Characteristics (continued)

Parameter Information
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 27. 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.
Parameter Reply timer override for HPR (HPR T1) **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 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.

Table 27. Configuration Parameter List - Modify HPR Defaults (continued)

Parameter Information
Parameter Maximum number retransmission (HPR N2) **Valid Values** 1 to 216 000 **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.
Parameter Limited Resource Timer **Valid Values** 1 to 216 000 seconds **Default Value** Default value is taken from the associated port parameter. **Description** This parameter specifies the timer value associated with the limited resource.

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 28. 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 29. 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 **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 29. 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, 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.
Parameter Limited Resource Timer **Valid Values** 1 to 216 000 seconds **Default Value** 180 **Description** This parameter specifies the timer value associated with a limited resource.
Parameter DLCI number **Valid Values** 16 to 1007 **Default Value** None **Description** This parameter specifies the DLCI number used by the router to connect to the Frame Relay network. When the router initiates a connection to a link station on the LAN through the connection network, it will use this DLCI number to connect to the Frame Relay network.

Table 29. Configuration Parameter List - Connection Network - Detail (continued)

Parameter Information
Parameter BAN destination address (BDA) **Valid Values** X'0000 0000 0000' to X'7FFF FFFF FFFF' **Default Value** X'0000 0000 0000' **Description** This parameter specifies the BAN destination address configured in the node that is performing the BAN function. If you are using bridging to connect the LAN network to the Frame Relay network, specify X'0000 0000 0000' as the value of this parameter. In this case, the MAC address reported to the APPN topology for the connection network TG is the BNI MAC address coded on the APPN port associated with this connection network definition.

Table 30. 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.

Table 30. Configuration Parameter List - TG Characteristics (Connection Network) (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** 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.
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.

Table 30. Configuration Parameter List - TG Characteristics (Connection Network) (continued)

Parameter Information
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.
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 31. 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 32 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.
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 32. 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.

Table 32. Configuration Parameter List - APPN Additional port to Connection Network (continued)

Parameter Information
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 33. 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 34. 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.
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.

Table 34. Configuration Parameter List - APPN Local PU (continued)

Parameter Information
Parameter Autoactivate **Valid Values** Yes or No **Default Value** Yes **Description** This parameter specifies whether to activate this link at start-up. **Note:** If the local link will be used for a DDDLU PU, you should specify *yes* to this question. If the local link is not set to autoactivate, then the first attempt to use the local pu (that is, the first attempt to establish a TN3270 session) will fail because the link is not yet up. While this attempt will fail, it causes the link to come up, and that link will be available for the next attempt. Since the link comes up when the SSCP-PU session is established, and that is when the link is identified as a DDDLU link. No DDDLU sessions can be established until the link is identified as a DDDLU link.
Parameter Enable Host Initiated Dynamic LU Definition **Valid Values** Yes or No **Default Value** No **Description** This parameter indicates whether or not dependent LUs will be created dynamically (as opposed to having to be configured.) If *yes* is specified, LUs will be defined for this PU as ACTLU requests (with CV0E) are received. LUs for the TN3270E Server do not have to be configured.

Table 34. Configuration Parameter List - APPN Local PU (continued)

Parameter Information
Parameter Pool Name for Host-initiated Dynamic LUs **Valid Values** A string of 1 to 8 characters: • First character: A to Z, $, #, @, or < • Second to eighth characters: A to Z, 0 to 9, $, #, @, >, or < **Default Value** None **Description** This parameter specifies the name of a pool to be created to contain LUs that the host activates on this local PU. This parameter is applicable only if **Enable Host Initiated Dynamic LU Definition** is *yes*. You do not need to use the **add implicit-pool** command to define this pool; specifying the name and other parameters here is sufficient to cause the pool to be created. If you do enter a pool name, you will be prompted to enter values for the following parameters: • Pool class (See Table 39 on page 196) • LU type (see Table 39 on page 196) You can provide the same pool name for multiple local PUs, if you wish. By specifying pool information, you cause host-initiated LUs that are not already configured at the router to be placed into the specified pool. TN3270 clients can then be assigned to them by requesting the pool name, or by mapping client IP addresses or destination ports to that pool. If you do not specify pool information, these host-initiated LUs are treated as explicit LUs and can only be assigned to clients that request them by their individual LU names.
Parameter Send Terminate-Self when TN3270 Client Disconnects **Valid Values** Yes or No **Default Value** No **Description** This parameter indicates whether or not a terminate_self request will be sent to the SSCP when the TN3270 client disconnects. If *yes* is specified, terminate_self will be sent and the host will be responsible for terminating the LU-LU session (i.e., the SLU will NOT send an UNBIND request.)

Syntax:

add routing_list

Note: These questions are asked only if you have configured the node as a border node.

There are a number of editing shortcut keys available to speed the modification of existing data in a previously configured routing list. These shortcut keys may be used when you are prompted for the Destination LUs and the Routing CPs.

- Pressing **Enter** alone will retain the currently displayed name.
- Pressing the **Space bar** followed by **Enter** will delete the currently displayed name.
- Entering character data followed by pressing **Enter** will replace the currently displayed name with the new character data.
- Entering **9** followed by pressing **Enter** will jump to the end of the list where new names can be appended.
- At the end of a list, pressing **Enter** alone completes the list.

Table 35. Configuration Parameter List - Routing List Configuration

Parameter Information
Parameter Routing list name **Valid Values** Character string up to 20 characters in length with no imbedded blanks. Mixed case and special characters are allowed. **Default Value** Blank **Description** This parameter identifies a specific routing list for modification. listing, or deletion by the configuration code. It is not used by the operational code. Up to 255 routing lists may be configured depending upon availability of configuration memory. Case is respected.
Parameter Subnet visit count **Valid Values** 1 to 255 **Default Value** Default taken from corresponding node level parameter **Description** This parameter specifies how many networks a locate search procedure may traverse.

Table 35. Configuration Parameter List - Routing List Configuration (continued)

Parameter Information
Parameter Dynamic routing list updates **Valid Values** 0 (none) 1 (full) 2 (limited) **Default Value** Default value taken from corresponding node level parameter **Description** This parameter controls whether entries can be automatically added to the node's temporary subnet routing list. It can be set to the same values as the analogous node level parameter. If this function is enabled the automatically added entries are only added to the temporary copy of the routing list.
Parameter Enable routing list optimization **Valid Values** Yes or No **Default Value** Yes **Description** Indicates whether the node is allowed to reorder the subnetwork routing list so that entries most likely to succeed come first. This reordering occurs in the internal temporary copy of the routing list.

Table 35. Configuration Parameter List - Routing List Configuration (continued)

Parameter Information
Parameter Destination LU found via this list **Valid Values** A fully-qualified LU name with optional trailing wildcard. Legal characters for the LU name are: A-Z, @, $, #, 0-9. The first character of the NETID part and of the LU name part must be non-numeric. Any of the FQ LU names may be terminated with a wild card “*” character to designate the range of LUs. For example, • * • NETI* • NETI.LUA* **Default Value** Blank **Description** This parameter specifies a list of destination LUs that can be found via this routing list. This question will be repeated until terminated with a null entry. **Notes:** 1. Only a single entry among all of the routing lists may have a standalone “*” . This will match all LUs, and the routing list containing it is known as the default routing list. 2. All the editing shortcuts described at the beginning of this table are available to speed modification of a previously configured routing CP(s) list. 3. Any given LU name may not be duplicated in another routing list. 4. Maximum number of LU names that may be specified: • 2212 - 126

Table 35. Configuration Parameter List - Routing List Configuration (continued)

Parameter Information
Parameter Routing CP and optional subnet visit count **Valid Values** A fully-qualified CP name consisting of 1 to 17 characters followed by an optional numeric subnet visit count. Legal characters for the CP name are: A-Z, @, $, #, 0-9 The first character of the NETID part and of the CP name part must be non-numeric. The optional subnet visit count range is 1 to 255 and should be separated from the fully-qualified CP name by one or more spaces. **Default Value** Blank for fully-qualified CP name and node-level setting for subnet visit count. **Description** This parameter specifies a list of one or more fully-qualified CP names of CPs that might know how to reach one or more of the previously configured destination LUs. Each of the following special keywords may be used once in any given routing list: • “*” - equivalent to specifying all native BNs, all adjacent non-native BNs, and all adjacent non-native NNs. • “*SELF” - equivalent to specifying the local node’s fully-qualified CP name • “*EBNS” - equivalent to specifying all native BNs This question will be repeated until terminated with a null entry. **Notes:** 1. All the editing shortcuts described at the beginning of this table are available to speed modification of a previously configured routing CP list. 2. If you configure “*SELF” as a CP name, you cannot configure the local node’s CP name. 3. Any given routing list can have the following maximum number of CP names and keywords: • 2212 - 144 4. Across all routing lists, you may use no more than the following number of different CP names and keywords: • 2212 - 144 5. Any given CP name or keyword may appear in no more than 255 routing lists.

Syntax:

add cos_mapping_table

Note: These questions are asked only if you have configured the node as a border node.

The editing shortcut keys specified at the beginning of the routing list table are also valid here. Use them to speed modification of the non-native CP names and COS name pairs.

Table 36. Configuration Parameter List - COS Mapping Table Configuration

Parameter Information
Parameter COS mapping table name **Valid Values** Character string up to 20 characters in length, with no imbedded blanks. Mixed case and special characters are allowed. **Default Value** Blank **Description** This parameter identifies a specific COS mapping table. It allows you to identify the table for modification, listing, or deletion by the configuration software. It is not used by the operational software. Up to 255 COS mapping tables may be configured depending upon availability of configuration memory. Case is respected.
Parameter Non-native NETID or CP name **Valid Values** A fully-qualified CP name with optional trailing wildcard. Legal characters for the CP name are: A-Z, @, $, #, 0-9 The first character of the NETID part and of the CP name part must be non-numeric. Any of the fully-qualified CP names may be terminated with a wildcard “*” character to designate a range of CPs. For example: • * • NET1* • NET1.LUA* **Default Value** Blank **Description** This parameter specifies a list of one or more non-native networks that this mapping table applies to. This question is repeated until terminated with a null entry. **Notes:** 1. Only a single entry among all the routing lists may have a standalone “*” . This will match all non-native networks, and is known as the default routing list. 2. Any given CP name may not be duplicated in another COS mapping table. 3. Maximum number of CP names that may be specified: • 2212 - 126

Table 36. Configuration Parameter List - COS Mapping Table Configuration (continued)

Parameter Information
Parameter Native and non-native COS-name pair **Valid Values** A pair of COS names, separated by a blank. Legal characters are: A-Z, @, $, #, 0-9 The first character of each name must be non-numeric. **Default Value** Blank **Description** This parameter identifies a pair of COS names. A native COS name is followed by the corresponding non-native COS name. For any given COS mapping table, one of the COS name pairs may specify the non-native COS name as "*" . This designates the default entry to use for all non-native COS names that do not explicitly match another entry in the table. One COS name pair cannot exactly match another COS name pair in a given table. However, a given native COS name can be used in multiple entries, and it is also okay for a given non-native COS name to be used in multiple entries. The operational software will use the first entry it finds. This question will be repeated until terminated with a null entry. **Notes:** 1. The native and non-native names cannot be identical. Only COS names that need to be changed should be specified. 2. A given native or non-native COS name may appear in multiple entries, but you cannot have two identical COS name pairs. 3. When you have multiple native COS names mapping to the same non-native COS name, the border node will use the first of those mappings when it needs to map from non-native to native. Similarly, when you have multiple non-native COS names mapping to a common native COS name, the border node will use the first of those mappings when it needs to map from native to non-native. 4. Any given COS mapping table can have the following maximum number of COS name pairs: • 2212 - 46 5. Across all COS mapping tables, you may use no more than the following number of native COS names: • 2212 - 144 There is no analogous limit for non-native COS names. 6. Any given native COS name may appear no more than 255 times across all routing lists.

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

routing_list *routing list name*

cos_mapping_table *mapping table name*

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

routing_list *routing list name*

cos_mapping_table *mapping table name*

Activate_new_config

Use the **activate_new_config** command to read the configuration into non-volatile memory.

Syntax:

activate_new_config

TN3270E

Table 37. TN3270E 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 xxviii.	
Set	tn3270e	195

Table 37. TN3270E Configuration Command Summary (continued)

Command	Function	See page:
Add	Adds or updates the following:	
	implicit-pool	196
	lu	199
	mapping	203
	port	204
Delete	Deletes the following: • implicit-pool • lu • mapping • port	205
List all	Lists the configuration memory	207
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.	

Syntax:

set

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 38. Configuration Parameter List - Set TN3270E

Parameter Information
Parameter Enable TN3270E Server **Valid Values** Yes or No **Default Value** Yes **Description** This parameter specifies whether TN3270E Server support will be enabled.
Parameter TN3270E Server IP Address **Valid values** Any IP address is accepted as valid input. However, the address must also be configured in IP either as an interface address or as the router's internal IP address. **Default Value** None **Description** This parameter is the IP address associated with the TN3270E Server.

Table 38. Configuration Parameter List - Set TN3270E (continued)

Parameter Information
Parameter Port number **Valid Values** 1 to 65 535 **Default Value** 23 **Description** This parameter specifies the port number associated with the TN3270E Server.
Parameter Enable Client IP address to LU name mapping? **Valid values** Yes or No **Default Value** No **Description** This parameter specifies whether client IP address to LU name mapping occurs.
Parameter Default pool name **Valid Values** Any alphanumeric string of 1 to 8 characters **Default Value** PUBLIC **Description** This parameter specifies the name of the default pool. This pool is used when TN3270 clients connect and do not specify an LU/pool name.
Parameter NetDisp Advisor Port Number **Valid Values** 1 to 65 535 **Default Value** 10 008 **Description** This parameter sets the port number for the Network Dispatcher Advisor.

Table 38. Configuration Parameter List - Set TN3270E (continued)

Parameter Information
Parameter Keepalive type **Valid Values** **0** None **1** Timing mark **2** NOP **Default Value** 0 **Description** This parameter specifies the Keepalive type. A Keepalive type of *Timing mark* requires responses from the client within the amount of time specified using the **Timer** parameter. A Keepalive type of *NOP* specifies that the client will not send back a response to the Keepalive message. Notification that the client is no longer there will come from TCP.
Parameter Frequency **Valid Values** 1 to 65 535 seconds **Default Value** 60 **Description** This parameter specifies how often the Keepalive message is sent to the client.
Parameter Timer **Valid Values** 1 to 65535 seconds **Default Value** 10 **Description** This parameter sets the timer value to be used with the Keepalive function.
Parameter Automatic logoff **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether automatic logoff will be enabled.

Table 38. Configuration Parameter List - Set TN3270E (continued)

Parameter Information
Parameter Time **Valid Values** 1 to 65 535 minutes **Default Value** 30 **Description** This parameter sets the time that the TN3270E link can be idle before being automatically logged off.
Parameter IPv4 Precedence **Valid Values** Yes or No **Default Value** No **Description** This parameter sets the IPv4 precedence value, which allows priority queueing of IPv4 encapsulated packets.
Parameter Enable LU Capping? **Valid Values** Yes or No **Default Value** No **Description** This parameter allows you to determine how many TN3270 sessions each IP address is allowed to initiate. If the answer to this question is *yes*, you will be asked the following question.
Parameter Max number of LUs per IP address **Valid Values** 0 - 65 535 **Default Value** 0 **Description** This parameter sets the maximum number of TN3270 sessions each client IP address is allowed to initiate.

Syntax:

add implicit-pool

This command defines a pool of LUs as opposed to the **add lu** command which adds a single LU. 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 39. Configuration Parameter List - Add TN3270E Implicit

Parameter Information
Parameter Pool name **Valid Values** A string of 1 to 8 characters: • First character: A to Z, $, #, @, or < • Second to eighth characters: A to Z, 0 to 9, $, #, @, > or < **Default Value** PUBLIC **Description** This parameter specifies the name of the LU pool to be used when TN3270 clients connect.
Parameter Pool class **Valid Values** 1 or 2, where: 1. Implicit workstation 2. Implicit printer **Default Value** 1 **Description** This parameter specifies type of LU pool.
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 or the subarea link over which SNA data will flow.

Table 39. Configuration Parameter List - Add TN3270E Implicit (continued)

Parameter Information
Parameter LU Name Mask **Valid Values** A string of 1 to 5 characters: • First character: A to Z, @, $, and # • Second to eighth characters: A to Z, 0 to 9 **Default Value** @01LU **Description** This parameter specifies the mask to be used to ensure that the LU names will not duplicate other names in the network. LU names are generated by appending the NAU address to the end of the LU name mask. When not specifying an address range, NAU addresses from 2 - 253 will be checked to see if the address is unused. If the address is available, it will be used. Otherwise, the next NAU address will be tried. For example, if the LU name mask is FRED, the possible LU names are [FRED2, FRED3, ..., FRED253].
Parameter LU type **Valid Values** • 1 - 3270 Mod 2 display • 2 - 3270 Mod 3 display • 3 - 3270 Mod 4 display • 4 - 3270 Mod 5 display • 5 - 3270 printer • 6 - SCS printer **Default Value** 1 **Description** This parameter specifies the type of dependent LU for the LU being added.
Parameter Specify LU address range? **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether you want to define an LU address range.

Table 39. Configuration Parameter List - Add TN3270E Implicit (continued)

Parameter Information

Parameter
LU address range
Valid Values
Any range of values within 1 - 255
Default Value
none
Description
This parameter specifies LU address range.
 	
The LU address range can be specified by using the following format:
`lower_address_bound-upper_address_bound`
 	
If no hyphen follows the first value, that value is assumed to be a single LU address. Multiple ranges can be entered, separated by commas. For example, the following string specifies 2 address ranges and 2 specific LU addresses:
`2-40,56,58,100-250`

Parameter Number of implicit workstation definitions **Valid Values** 1 to 255 **Default Value** 1 **Description** This parameter specifies the number of dependent LUs to be added to the implicit pool.

add lu

This command adds a specific LU. 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 40. Configuration Parameter List - Add TN3270E LU

Parameter Information
Parameter LU name **Valid Values** A string of 1 to 8 characters: • First character: A to Z,@, $, and # • Second to eighth characters: A to Z, 0 to 9 **Default Value** None **Description** This parameter specifies the LU name of the dependent LU being defined.
Parameter NAU address **Valid Values** 1 to 255 **Default Value** None **Description** This parameter specifies the NAU address of the LU being defined.
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 either the link between the DLUR and the PU defined using the **add local-pu** command or the subarea link over which SNA data will flow.
Parameter Class **Valid Values** **1** Explicit Workstation **2** Implicit Workstation **3** Explicit Printer **4** Implicit Printer **Default Value** 1 **Description** This parameter specifies the LU class.

Table 40. Configuration Parameter List - Add TN3270E LU (continued)

Parameter Information

Parameter
LU type

Valid Values
- 1 — 3270 Mod 2 display
- 2— 3270 Mod 3 display
- 3 — 3270 Mod 4 display
- 4 — 3270 Mod 5 display
- 5 — 3270 printer
- 6 — SCS printer

Default Value
1

Description
This parameter specifies the type of dependent LU for the LU being added.

Parameter
Implicit pool 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
<DEFLT>

Description
This parameter specifies the name of the implicit pool to be used in the LU definition. This question is asked only if the *class* is an implicit workstation or implicit printer.

Parameter
Define an associated printer

Valid Values
Yes or No

Default Value
No

Description
This parameter specifies whether you want to define an associated printer.

Parameter
Associated printer name

Valid Values
A string of 1 to 8 characters:
- First character: A to Z,@, $, and #
- Second to eighth characters: A to Z, 0 to 9

Default Value
None

Description
This parameter specifies the name of the associated printer.

Table 40. Configuration Parameter List - Add TN3270E LU (continued)

Parameter Information
Parameter Associated printer NAU address **Valid Values** 1 to 255 **Default Value** None **Description** This parameter specifies the NAU address for the associated printer LU definition.

Syntax:

add map

This command adds a client IP address to LU name mapping. 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 [ ].

The following mapping rules apply:

- If a map definition contains a full subnet mask (255.255.255.255), indicating that the entry is for a specific client and a specific LU/pool is not requested by the client, any LU/pool in the map definition that matches the connection type may be tried.
- If a map definition does not contain a full subnet mask and a specific LU/pool is not requested, only pool entries in the map definition will be tried. You cannot create a definition that maps a subnet to a specific LU. You must map the subnet to a pool.
- If a connection request is received from a client and there are no map entries that match, the request will be rejected.
- A mixture of pool and LU types can be added to a particular map. The resource selected will be based on the type of connection request. The order in which the resources are defined in the map will be the order in which it is chosen for a particular connection request.
- If a map definition contains a non-zero destination port number, only clients that connect to that port will be checked against that mapping.

Note: When a client connects while mapping is enabled, the server will begin ANDing the client's IP address with the subnet mask of each sequential map. The longest match between the incoming client IP address and the map definition determines which map definition is tried first. If all eligible resources in the map definition are in use and **final LU mapping connection attempt** is *no*, the map definitions are again searched for the next most specific match.

Table 41. Configuration Parameter List - Add TN3270E Map

Parameter Information
Parameter Pool name/LU 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 an LU name or a Pool name to be mapped to the IP address. The LU name can only be mapped to a Host address. If the mask is a network mask, the name specified must be a pool name.
Parameter Client IP address or Network address **Valid Values** Any valid IP address **Default Value** 0.0.0.0 **Description** This parameter specifies the IP address of the client or network map definition to be added.
Parameter Address Mask **Valid Values** Any valid IP address mask **Default Value** 0.0.0.0 **Description** This parameter specifies the IP address mask the router applies to incoming client IP addresses and configured client IP or network addresses to determine whether they match.

Table 41. Configuration Parameter List - Add TN3270E Map (continued)

Parameter Information
Parameter Port number **Valid Values** 1 to 65535 If you want to specify a particular port, you should select either the global TN3270 server port value defined with the **set** command, or one of the port values defined with the **add port** command. **Default Value** 0 **Description** This parameter specifies the destination TCP port number a TN3270 client must connect to in order for this mapping entry to be checked. If the value is zero, the mapping entry applies to client connections to any defined TCP port number.
Parameter Final LU mapping connection attempt **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether the router should continue to try less specific mapping entries if a client match with this entry failed to yield a valid available LU.

Syntax:

add port

This command specifies additional port for the TN3270E Server to listen on. 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 42. Configuration Parameter List - Add TN3270E Port

Parameter Information
Parameter Port number **Valid Values** 1 to 65535 **Default Value** none **Description** This parameter specifies the port number to be added.

Table 42. Configuration Parameter List - Add TN3270E Port (continued)

Parameter Information
Parameter Support TN3270E? **Valid Values** Yes or No **Default Value** Yes **Description** This parameter specifies whether the added port will negotiate to be a TN3270E server. If it is not an “E” Server, it will not support printing or system requests.
Parameter Pool 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 of the pool associated with this port. Clients that connect to this port and do not specify an LU name or pool name will be assigned an LU from this pool.
Parameter Disable Client Filtering for this port? **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether incoming connections on this port should use the box-wide Client IP Address to LU Name Mapping function if it is enabled.

Syntax:

delete lu

This command removes a TN3270E LU. 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 - Delete TN3270E LU

Parameter Information
Parameter LU name **Valid Values** A string of 1 to 8 characters: • First character: A to Z,@, $, and # • Second to eighth characters: A to Z, 0 to 9 **Default Value** None **Description** This parameter specifies the LU name of the dependent LU to be removed.

Syntax:

delete implicit-pool

This command removes a TN3270E implicit pool. 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 44. Configuration Parameter List - Delete TN3270E Implicit

Parameter Information
Parameter Pool 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 of the LU pool to be deleted.
Parameter Delete entire pool **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether the entire pool or a specific entry is to be deleted.

Table 44. Configuration Parameter List - Delete TN3270E Implicit (continued)

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 of the station to be deleted.

Syntax:

delete map

This command removes a client IP address to LU name mapping. 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 45. Configuration Parameter List - Delete TN3270E Map

Parameter Information
Parameter Client IP address or Network address **Valid Values** Any valid IP address **Default Value** 0.0.0.0 **Description** This parameter specifies the IP address of the client or network map definition to be deleted.
Parameter Client IP address or Network address Mask **Valid Values** Any valid IP address mask **Default Value** 0.0.0.0 **Description** This parameter specifies the IP address mask of the client or network map definition to be deleted.

Table 45. Configuration Parameter List - Delete TN3270E Map (continued)

Parameter Information
Parameter Delete all entries for this client? **Valid Values** Yes or No **Default Value** No **Description** This parameter specifies whether the entire pool or a specific name is to be deleted.
Parameter Pool 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 LU name or pool name to be deleted.

Syntax:

delete port

This command deletes port definitions. 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 - Delete TN3270E Port

Parameter Information
Parameter Port number **Valid Values** 1 to 65536 **Default Value** none **Description** This parameter specifies the port number to be added.

Syntax:

list all

This command lists a TN3270E configuration.

Monitoring APPN

This section describes how to monitor APPN. It includes the following sections:
- "Accessing the APPN Monitoring Commands"
- "APPN Monitoring Commands"

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>
```

If typing **p appn** results in the message "Protocol APPN is available but not configured", you probably have one of the following errors:
- You have not enabled APPN globally in the active configuration (although you may have configured APPN parameters). Check the current configuration and if this is the case, enable APPN and restart or reload the router.
- The amount of memory required for APPN to initialize properly was not available in the router. Use **talk 2** to see if an error message to this effect has been logged. If so, reconfigure APPN to use less memory and restart or reload the router.

Once you have reached the APPN monitoring prompt, enter **tn3270** to reach the `TN3270E >` monitoring prompt.

APPN Monitoring Commands

This section describes the APPN monitoring commands for monitoring APPN interfaces. Enter the commands at the `APPN>` prompt, and TN3270 server commands at the `TN3270E>` prompt.

Table 47. APPN Monitoring Command Summary

Command	Function	See details on page:
? (Help)	Displays all the commands available for this command level or lists keyword options for specific commands.	--
activate link	Activates a configured link.	"Activate" on page 211
aping	Tests SNA/APPN connectivity to a target LU.	"Aping" on page 211
deactivate link	Deactivates a configured or dynamic link.	"Deactivate link" on page 212
dump	Writes an APPN dump to disk or to the network.	"Dump" on page 212

Table 47. APPN Monitoring Command Summary (continued)

list cp-cp_sessions	Displays a list of all adjacent CPs that may have CP-CP sessions with this router.	page 215
list dlur dlus	Displays a list of active DLUS's and the status of each session in the DLUS-DLUR pipe.	page 215
list dlur lu	Displays a list of downstream or internal PUs with LU statistics for each PU.	page 216
list dlur pu	Displays a list of downstream or internal PUs with their connection status.	page 217
list dlur status	Displays a summary of currently active global DLUR configuration information.	page 217
list ds incomplete_locates	Displays a list of APPN searches that are currently in progress.	page 218
list ds resource	Displays a complete or partial list of LU names in this router's APPN directory.	page 219
list ds status	Displays summary statistics for APPN Directory Services.	page 219
list dumps	Displays a list of dumps on disk.	page 220
list focal	Displays a list of network management focal points with their status.	page 220
list isr_sessions	Displays the number of active ISR LU-LU sessions that pass through this router, by link.	page 221
list link	Displays a list of configured and dynamic links from this router.	page 222
list link *link-name*	Displays detailed configuration and status about one particular link.	page 224
list local_link	Displays a list of logical links from DLUR to local PU2.0s in this router (which are used to contain TN3270 LUs).	page 224
list log	Now replaced by ″log view″ and ″log status″.	page 235
list port	Displays a list of configured physical and logical APPN router ports with their status.	page 225
list port *port-name*	Displays detailed configuration and status about one particular port.	page 226
list rtp	Displays a list of nodes in the RTP Partner Table, and summary information about all active RTP connections.	page 228
list rtp *tcid*	Displays detailed information about one or all RTP connection(s).	page 229

Table 47. APPN Monitoring Command Summary (continued)

list session	Displays a list of ISR sessions that flow through the router.	page 230
list status	Displays a summary of general APPN configuration and status information.	page 231
list topo node	Displays information in this router's topology database about a particular node in this topology subnet.	page 232
list topo status	Displays a summary of topology database statistics.	page 233
list topo tg	Displays a complete or partial list of active TGs in this topology subnet.	page 234
log status	Displays summary information about the APPN event log.	page 235
log view	Enters a submenu for navigating and viewing APPN event log entries.	page 237
memory	Displays summary and detailed information about APPN memory usage within the router.	"Memory" on page 237
restart	Stops and reactivates APPN and TN3270 disruptively.	"Restart" on page 241
rtp status	Displays currently in-use global RTP configuration information.	"Rtp status" on page 239
rtp switchpath	Causes an RTP connection to path switch to the best currently available path.	"Rtp switchpath" on page 240
rtp test	Does an HPR route test and displays the results.	"Rtp test" on page 240
stop	Stops APPN and TN3270 disruptively.	"Stop" on page 241
test rtp	Does an HPR route test and display the results (old form of ″rtp test″).	"Rtp test" on page 240
tn3270e	Accesses the TN3270 monitoring command menu.	"TN3270E Monitoring Commands" on page 242
transmit dump	Transmits an APPN dump from the router's hard disk (2216, Network Utility, 2212) to a workstation in the network using TFTP.	"Transmit" on page 242
exit	Returns you to the main Talk 5 monitoring menu.	--

Table 48. TN3270E Server Monitoring Command Summary

Command	Function	See details on page:
? (Help)	Displays all the commands available for this command level or lists keyword options for specific commands.	--
deactivate lu	Deactivates by force an LU in use by a TN3270 client, and disconnects the corresponding TCP connection to that client.	"Deactivate LU" on page 242

Table 48. TN3270E Server Monitoring Command Summary (continued)

list connections	Displays a complete or partial list of active client connections.	244
list lu *lu-name*	Displays detailed configuration and status information about a single internal LU.	245
list mapping	Displays a list of configured client IP address to LU/pool name mappings.	246
list pools	Displays a list of configured implicit LU pools.	246
list pools *pool-name*	Displays detailed information about a single LU pool.	247
list ports	Displays a list of configured TN3270 server target TCP ports.	248
list pu	Displays a list of all internal PUs (both DLUR and subarea) with summary status and configuration information.	249
list pu *pu-name*	Displays a list of all internal LUs under the specified PU, with summary status and configuration information for each LU.	250
list rejections	Displays a list of the most recent client connections rejected.	250
list status	Displays global TN3270 server configuration and statistical summary.	252
exit	Returns you to the APPN monitoring menu.	--

APPN Monitoring Command Details

This section describes the detailed syntax of the APPN monitoring commands. You enter these commands at the `APPN>` command prompt.

Activate

Use the **activate link** command to activate a configured link. Use the **list link** command to look up the name of the link you wish to activate and to view the status of the link after activating it.

Syntax:

activate link *link_name*

Aping

Syntax:

aping *flag-value-pairs lu_name*

where,

flag-value-pairs
Specifies one or more of the following flags followed by a value. Specify these flag values only if you want to override the default values.

Table 49. Flags

Flag	Meaning	Default value

Table 49. Flags (continued)

-m	Mode name for LU6.2 session	#INTER
-t	Destination TP (transaction program) name	APING
-i	Count of sends and receives to issue	1
-x	Count of LU6.2 conversations to run (serially)	1
-y	Count of TPs to run (serially)	1
-s	Size of packet	100 bytes
-q	Quiet	Status messages
-b	Output display goes to talk 2 (in background)	Display to Talk 5

lu_name

Specifies the fully-qualified LU name of the target of the APING.

Valid Values: Any valid fully-qualified LU name

Example:

```
APPN >aping stfnet.mvs8
Allocate duration: 536 msec
Iteration  Duration  Data Sent  Data Rate
  number    (msec)    (bytes)     (Kb/s)     LU name
------------------------------------------------------
     0       458       100          1       STFNET.MVS8
------------------------------------------------------
Avg.         458       100          1
```

Table 50. APING Output Description

Item	Description	Key values
Allocate duration	Time required to set up the LU6.2 session and conversation for the aping.	--
Iteration duration	Round-trip time required to send and receive acknowledgement for the data packet.	--
Iteration data rate	Calculated data rate (min 1Kb/s) based on duration and bytes sent.	--

Deactivate link

Use the **deactivate link** command to deactivate a configured link. Use the **list link** command to see link names and to view the status of the link after using this command. Configured links should have an inactive status and dynamic links should disappear.

Syntax:

deactivate link *link_name*

Dump

Use the **Dump** command to create APPN dump files to the hardfile, if there is a hardfile in the device. If the device does not have a hardfile, you configure the TFTP server destination using the `talk 6` **set dump target** and **enable dump-memory** commands at the `APPN>` prompt.

Syntax:

dump

Since this dump is non-disruptive to APPN functions, you can improve its integrity by minimizing traffic and APPN control commands while the dump is in progress.

List

Use the **List** command to display information about the APPN configuration. The command lists:

Syntax:

list

appc_sessions

cp-cp_sessions

dlur dlus

dlur lu

dlur pu

dlur status

ds incomplete_locates

ds resource

ds status

dumps

focal

isr_sessions

link

link *link-name*

local_link

log

port

port *port-name*

rtp

rtp *tcid*

session

status

topo node

topo status

topo tg

Command **Function**

list appc_sessions

Use the **list appc** command to display a list of all LU6.2 sessions that have an endpoint in this router. Examples of such sessions include: CP-CP sessions, sessions from DLUR to a DLUS, sessions to a network management focal point, and sessions started due to an ″aping″ command. This command lists all active sessions. If a pipe consists of two one-way sessions, both sessions in the pair are displayed.

Example:

```
APPN >li appc
LU Name            Mode  Type  FSM  FID  PCID
===============================================================
STFNET.CP3174BC   CPSVCMG  Pri  ACT  FID2 C4 9B 1F 3B 03 54 83 3D
STFNET.CP3174BC   CPSVCMG  Sec  ACT  FID2 CB 13 AF 4A 23 AC E5 06
STFNET.VL14       CPSVCMG  Pri  ACT  FID5 C4 9B 1F 3B 03 54 83 40
STFNET.VL14       CPSVCMG  Sec  ACT  FID5 CB 67 9F CA F8 27 B5 9F
STFNET.VLNN045    CPSVCMG  Sec  ACT  FID5 C8 8B 1F 3B 04 42 34 FA
STFNET.VLNN045    CPSVCMG  Pri  ACT  FID5 C4 9B 1F 3B 03 54 83 41
STFNET.MVS8       CPSVRMGR Pri  ACT  FID2 C4 9B 1F 3B 03 54 83 42
STFNET.MVS8       CPSVRMGR Sec  ACT  FID2 D3 B7 7C D5 57 35 0B C8
```

Table 51. List appc_sessions Output Description

Item	Description	Key values
LU name	Fully qualified partner LU name	--
Mode	Mode name for the session	• #CONNECT = standard medium priority • #INTER = standard high priority • CPSVCMG = CP-CP session • CPSVRMGR = DLUR-DLUS session • SNASVCMG = Focal point session • other mode names are architected and can also be user-defined
Type	Router session activation role	• Pri = Primary • Sec = Secondary
FSM	Current session status (Finite State Machine value)	• ACT = active • PBIR = pending BIND request • PCIN = pending CINIT (Session services is finding and activating the outbound TG) • RES = reset (initial)
FID	Format ID type	• FID2 = ISR • FID5 = HPR
PCID	Procedure correlator ID: session identifier	--

list cp-cp_sessions

Use the **list cp** command to display a list of all the adjacent nodes that may have CP-CP sessions with this router. The output list includes all CPs that have an active link that supports CP-CP sessions, as well as CPs that are no longer connected but had an active CP-CP capable link in the past (since APPN was last restarted). Unlike the **list appc** command, one line of output represents a conwinner/conloser session pair.

If the router is configured as a Branch Extender node, the list will indicate only one active CP-CP session pair to an adjacent NN. The is the BEX node's NN server.

Example:

```
APPN >li cp
          CP Name Type     Status    ConWinner ConLoser ConWinner ConLoser
                                        ID
     ID    Sense     Sense
```

```
=========================================================================
     STFNET.NN12  NN     Active   BAF92A69  BAF92A84 080F6051  00000000
 STFNET.CP3174BC  NN     Active   BAF927E3  BAF927E5 00000000  00000000
```

Table 52. Output Description

Item	Description	Key values
CP name	Fully qualified name of adjacent CP	--
Type	Node type of adjacent CP	NN = network node EN = end node Virt = virtual node
Status	CP-CP session-pair status	Active Inactive Pending
ConWinner/Loser ID	Router internal session id for the contention winner/loser session in the CP-CP session pair, 0 if session is not connected	--
ConWinner/Loser sense	SNA sense code for why the conwinner/loser session last disconnected	--

list dlur dlus Use the **list dlur dlus** command to display a list of active DLUSs and the status of each session in the DLUR-DLUS pipe. The DLUSs listed may come from one of these sources:

- Configured in the router as the global primary or backup DLUS
- Configured in the router as the primary or backup DLUS for a particular downstream link
- Dynamic DLUS (not configured) that connects to the router and drives call-out to dependent PUs

Example:

```
APPN >li dlur dlus
DLUS  NAME         CONWINNER    CONLOSER
                   STATE        STATE
---------------------------------------
STFNET.MVS8        UP           UP
```

Table 53. List dlur-dlus Output Description

Item	Description	Key values
DLUS name	Fully qualified CP name of DLUS	--
ConWinner/Loser state	Status of the contention winner/loser session in the DLUR-DLUS session pair	UP DOWN PENDING_UP PENDING_DOWN BLOCKED = waiting for SSCP takeover

list dlur lu Use the **list dlur lu** command to display a list of active downstream (or internal, for TN3270) PUs with LU statistics for each PU. Dependent PUs in this list either have an active link to the router, or the router is currently attempting to establish a link.

Example:

```
APPN >li dlur lu
CP NAME           LINK      TOTAL  ---NO SSCP LU STATE---   NO OF LUs
                  NAME      LUs    DOWN   PENDING  ACTIVE   LU_LU SESS
------------------------------------------------------------------------
STFNET.VLNN105    PUSUD1     253      0      0      253        0
STFNET.VLNN105    PUSUD21     10      0      0       10        0
STFNET.VLNN105    PUSUO2       9      0      0        9        0
STFNET.VLNN105    PUSUO1      10      0      0       10        0
```

Table 54. List dlur lu Output Description

Item	Description	Key values
CP name	Name of CP on which the LU resides. For TN3270 internal LUs, the router's CP name.	--
Link name	Configured or dynamically constructed link station name for the link to the dependent PU. This link can be external or internal to the router.	--
Total LUs	Sum of the number of LUs in all the SSCP-LU states. These LUs need not be defined at the router, but are defined at the host.	--
SSCP-LU state: down	Number of LUs that have no owning SSCP but still have LU-LU sessions (lost SSCP link but ANS=CONT).	--
SSCP-LU state: pending	Number of LUs that are waiting for ACTLU response.	--
SSCP-LU state: active	Number of LUs that have received ACTLU response. This number is not decremented when an LU is bound and enters LU-LU state.	--
LU-LU session	Number of LUs that currently have LU-LU sessions active	--

list dlur pu

Use the **list dlur pu** command to display a list of downstream (or internal, for TN3270) PUs with their connection status. Dependent PUs in this list either have an active link to the router, or the router is currently attempting to establish a link.

Example:

```
APPN >li dlur pu
CP NAME           STATUS      LOC LINK     SESS  ANS SSCP     ACT DLUS
                                  NAME     STAT
;  PUNAME   NAME
----------------------------------------------------------------------
STFNET.VLNN105    active      INT PUSUD1   act   CON PUSUD12  STFNET.MVS8
STFNET.VLNN105    active      INT PUSUD21  act   CON PUSUD1   STFNET.MVS8
STFNET.VLNN105    active      INT PUSUO2   act   CON PUSUO2   STFNET.MVS8
STFNET.VLNN105    active      INT PUSUO1   act   CON PUSUO1   STFNET.MVS8
```

Table 55. Output Description

Item	Description	Key values
CP name	CP name of the dependent PU. For external PUs, this is the CP name they send in their XID, or, if they do not send one, it is a name the router makes up using the format DLUR..@nnn. For internal PUs, this is the CP name of the router.	--

Table 55. Output Description (continued)

Status	SSCP-PU session status, from the perspective of the DLUR router. You can decode status values as follows: • pe = pending • Re = request • Rs = response • Actp, Actpu = ACTPU Dactpu = DACTPU • LnkAct = link activation • Inop = inoperative	active peReActpRs (e.g., pipe is down) reset (down) peActpu peActpuRs peLnkAct peDactpuRs peInop peInopActpu
Loc	Location of the PU relative to the DLUR router	INT = internal DON = downstream
Link name	Configured or dynamically constructed link station name for the link to the dependent PU. This link can be external or internal to the router.	--
Sess stat	Status of the DLUR-DLUS pipe that carries control flows for this dependent PU.	act = active res = reset (down) pAct = pending active pInac = pending inactive
ANS	Host sysdef value for Automatic Network Shutdown: whether LU-LU sessions should continue or stop when SSCP connectivity is lost.	CON = continue STP = stop
SSCP PU name	VTAM name for this dependent PU, received in ACTPU.	--
Act DLUS name	CP name of the DLUS that currently owns this PU (the ″active DLUS″).	--

list dlur status

Use the **list dlur status** command to display a summary of currently active global DLUR configuration information. Note that some of these values have optional link-level overrides.

Example:

```
APPN >li dlur st
Primary DLUS Name                    = STFNET.MVS8
Backup  DLUS Name                    =
Retry Time Limit                     = 15
Short Retry Timer                    = 15
Short Retry Count                    = 20
Long Retry Timer                     = 30
Drop Link when there are no sessions = NO
```

These are all configured data items. See page 106.

list ds incompletes

Use the **list ds inc** command to display a list of APPN search requests (″locates″) that are currently in progress. This router is waiting for replies from other nodes in the network.

The command prompts for several possible data filters. For a description of each, see the output description table below.

Example:

```
APPN >li ds inc
        PCID (0 if unknown) [00000000 00000000]?
        Locate origin CP      (NetID.CPname or *) [*]?
        Locate origin LU      (NetID.LUname or *) [*]?
        Locate destination LU (NetID.LUname or *) [*]?

PCID & Incomplete
 Child CP Name(s)     Origin CP         Origin LU      Destination LU
----------------- ----------------- ----------------- -----------------
c49b1f3b 03310d51 STFNET.VLNN105    STFNET.VLNN105    STFNET.VL12
STFNET.VL15


c49b1f3b 03310d50 STFNET.VLNN105    STFNET.VLNN105    STFNET.MVS8
STFNET.VL15
```

Table 56. Output Description

Item	Description	Key values
PCID	Procedure correlator ID: a network-level correlator for this particular search procedure.	--
Incomplete child CP names	CP names of nodes to which this router has sent locate requests, and from which it is still awaiting replies.	--
Origin CP	Name of the CP that started the search originally.	--
Origin LU	Name of the LU that started the search originally.	--
Destination LU	Name of the LU being searched for.	--

list ds resource *flag-value pair*

Use this command to display a list of resource (LU) names in this router's APPN directory.

To limit the data displayed, you can specify one of the following filter flags and a corresponding value:

Table 57. Output Description

Filter flag	Value
-c	CP name of LU owner, can be qualified with net id or not
-n	Net id of LU owner
-l	Fully-qualified LU name
-s	Fully-qualified server name

Example:

```
APPN >li ds res

 LU NAME          SERVER NAME       OWNER NAME        LOCATION TYPE
=================================================================
*                 STFNET.VLNN105    STFNET.TEMP       WILDCARD HOME
STFNET.MVS8       STFNET.MVS8       STFNET.MVS8       X-DOMAIN CACHE
STFNET.CNM08      STFNET.MVS8       STFNET.MVS8       X-DOMAIN CACHE
STFNET.SD1LO2     STFNET.VLNN105    STFNET.VLNN105    LOCAL    HOME
STFNET.SD1LO3     STFNET.VLNN105    STFNET.VLNN105    LOCAL    HOME
STFNET.SD1LO4     STFNET.VLNN105    STFNET.VLNN105    LOCAL    HOME
```

Table 58. Output Description

Item	Description	Key values
LU name	Name of the LU, or ″*″ to represent a full wildcard.	--
Server name	CP name of the NN server for that LU.	--
Owner name	CP name of the LU's owner. For instance, an EN might own an LU that resides in the EN.	--
Location	Where the LU is located.	REGISTER = registered by a served EN X-DOMAIN = in or served by another NN LOCAL = in the router, including LUs served by DLUR DOMAIN = served by the router as a NN, but not registered WILDCARD = owner has a full wild-card (non-explicit) definition
Type	Category of entry in the directory, reflecting how the entry is to be handled.	HOME = sysdef'd in the router CACHE = dynamically learned by the router, will age out REGISTER = registered by a served EN, can be deregistered by the same

list ds status

Use this command to display summary statistics about this router's APPN directory.

Example:

```
APPN >li ds s
Maximum Directory Entries   = 4000
Current Cache Entries       = 3
Current Home Entries        = 284
Registered Entries          = 0
Directed Locates Received   = 0
Broadcast Locates Received  = 1
Directed Locates Sent       = 2
Broadcast Locates Sent      = 2
Directed Locates Not Found  = 0
Broadcast Locates Not Found = 0
Outstanding Locates         = 0
```

list dumps

Use this command to list all APPN dump files on the router hard disk. This command is not available for routers that do not have a hard disk.

Example:

```
APPN >li du
 1     168084     Thu Jul 01 15:11:18 1999
```

Table 59. Output Description

Item	Description	Key values

Table 59. Output Description (continued)

Number	Dump number to use with the **transmit dump** command	--
Size	Size of the dump file, in bytes. This number grows while the dump is in progress.	--
Date/time	Date and time of the last file change. The time changes while the dump is in progress.	--

list focal

Use this command to display a list of configured and active dynamic network management focal points with their status.

Example:

```
APPN >li foc
CATEGORY         STATUS   TYPE    FOCAL POINT
----------------------------------------------
ALERT            NOTACT   IMP_PRI STFNET.CNM08
```

Table 60. Output Description

Item	Description	Key values
Category	Category of function performed by the focal point.	ALERT MS_CAPS ACCTNG OTH = other
Status	Status of LU6.2 sessions to this focal point.	NOTACT = not active ACT = active PENDING NEVERACT = was never active
Type	Nature of the focal point, using host-centric terms: Explicit = FP is not configured at the router, connects to the router Implicit = FP is configured at the router, router connects to FP Values at the right are listed in high-to-low priority order, where a higher priority FP can dynamically take over as FP.	EXP_PRI = explicit primary IMP_PRI = implicit primary BKUP_FP = backup foc. pt. DEF_PRI = default primary DEF_BKP = default backup DOMAIN HOST
Focal point	CP name of the node providing the focal point function.	--

list isr_sessions

Use this command to display the number of active ISR LU-LU sessions that pass through this router, by link. The counts include:

- Sessions that enter and exit the box using ISR (these sessions count once on each of the inbound and outbound TGs)
- Sessions that enter the box using ISR but exit on an RTP connection (these sessions count once only on the non-HPR TG)

- TN3270 LU sessions routed by DLUR that exit the box using ISR (these sessions are counted only on the real external ISR TG, not on the internal links between DLUR and the local PUs)

Use the **list session** command to display more information about the counted ISR sessions.

Example:

```
APPN >li isr
  Adjacent CP Name  TG Number   ISR Sessions
===============================================
    STFNET.CP3174BC      21            3
```

Table 61. Output Description

Item	Description	Key values
Adjacent CP name	CP name of the node adjacent to the router on this TG, either configured or received in an XID.	--
TG number	Negotiated TG number for this link.	--
ISR sessions	Number of active ISR sessions on this link.	--

list link_information

Use this command to display a list of all configured and all active dynamic links.

Example:

```
APPN > li l
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
 =========================================================================
  TO3174       TR005     5   STFNET.CP3174BC    NN  INACTIVE     ACT_LS
   TOLEN        TR00     0       STFNET.TEMP   LEN   ENABLED   RESET_LS
  TOLEN1        TR00     0       STFNET.ABCD   LEN   ENABLED   RESET_LS
     @@0       TR005     5       STFNET.NN12    NN    ACTIVE     ACT_LS
```

Table 62. Output Description

Item	Description	Key values
Name	For configured links, the link station name you configured. For dynamic links, the router constructs a name of the format ″@@nnnn″, where nnnn starts at zero and continues to increase until it wraps.	--
Port name	The configured APPN name for the port through which this link is connected.	--
Intf	The router’s logical interface number for the port through which this link is connected.	--
Adj CP name	CP name of the node adjacent to the router on this link, either configured or received in an XID.	--
Type	Configured or actual (if link is active) node type of the adjacent node.	LEN EN NN LEARN (configured only)

Table 62. Output Description (continued)

HPR	Configured or actual (if link is active) status of HPR on the link	ACTIVE INACTIVE ENABLED (configured only) DISABLED (configured only)
State	Current connection status of the logical link Some intermediate state definitions: SENT_REQ_OPNSTN = underlying port is active, DLC has been asked to contact the remote link station PEND_XID_EXCH = remote station contacted, exchanging XIDs	**Steady states** RESET_LS = reset (down) ACT_LS = active (up)**Going-up states** SENT_REQ_OPNSTN PEND_XID_EXCH SENT_ACT_AS SENT_SET_MODE SENT_CREATE_TG SENT_CONN_REQ PEND_RCV_CONN_IND PEND_SEND_CONN_RSP SENT_CONN_RSP**Going-down states** SENT_DEACT_AS_ORD SENT_DISC_ORD SENT_DESTROY_TG PEND_DEACT PEND_CLOSE_STN

list link_information *link-name*

Use this command to get detailed configuration and status information about a single logical link to an adjacent node.

Example:

```
APPN > li link vm30pu1

Link Station Information
===========================================
       ls_name = VM30PU1
       type = DEFINED
       act_at_startup = TRUE
       auto_act_supported = FALSE
       pan uplink = FALSE
       replace inbound CP name/node id = FALSE
       retry link act unconditionally = FALSE
       adjacent node subnet affiliation = NEGOTIABLE
       subnet visit count = 3
       remote mac_addr = 402222222222
       remote sap_value = 04
       hpr_sap_value = C8
       real_adj_cp_name = USIBMNR.NRMVM30
       node_id = 00000000
       cp_cp_sessions_supported = FALSE
       hpr_supp = FALSE
```

```
hpr link = FALSE
link station state = ACT_LS
direction = OUTBOUND
actual_max_send_btu_size = 2006
partner_node_type (actual) = EN
partner_node_type (defined) = LEARN
tg_isr_type = ENDPOINT_TG
tg_num (defined) = 0
tg_num (actual) = 0
Received CV22 Sense code = 0
```

Table 63. Output Description

Item	Description	Key values
Type	How the link is known to the router.	DEFINED = configured DYNAMIC TEMPORARY = not yet able to match against configured links
Act_at_startup	Whether link is configured to activate when APPN starts up.	TRUE FALSE
Auto_act_supported	Link is able to be activated only when needed	--
Pan_uplink	Whether link is configured as a Branch Extender (peripheral access node) uplink (EN appearance upstream to NN).	TRUE FALSE
Replace inbound CP name / node ID	Whether link is configured that these XID fields from an adjacent LEN node should be overridden by values configured in the router.	TRUE FALSE
Retry link act unconditionally	Whether link activation failure and link failure should always be retried regardless of the cause.	TRUE FALSE
Adjacent node subnet affiliation	Whether link is configured to be an EBN link to a different topology subnet.	NATIVE NON-NATIVE NEGOTIABLE
Real adj CP name	CP name received in XID from the adjacent node	--
CP-CP sessions supported	Configured value from router port or link definition	TRUE FALSE
Hpr_supp	Configured support for HPR	TRUE FALSE
Hpr link	Actual negotiated support for HPR on this link	TRUE FALSE
Link station state	Current connection status of the logical link	Same values as in ″list link″
Direction	Direction in which link activation occurred	INBOUND OUTBOUND

Table 63. Output Description (continued)

Tg_isr_type	Link/TG type	ENDPOINT_TG = adjacent node acts as an EN INTERMEDIATE_ROUTING_TG = router acts as NN or EBN and adjacent node is a NN
Received CV22 sense code	SNA error code for XID exchange failure, received from the adjacent node on this link.	--

list local_link_information

Use this command to display a list of logical links inside the router from DLUR to internal PU2.0s. These PUs are used to contain LUs for the TN3270 server function.

Example:

```
APPN > li loc
    Name     SSCP PU Name     Node ID    Auto Act    Sense  State
 ======================================================================
  PUSUD1      STFNET.PUSUD12   77DE711      TRUE        0  LOCAL_ACT_LS
 PUSUD21       STFNET.PUSUD1   77D7E11      TRUE        0  LOCAL_ACT_LS
  PUSU02       STFNET.PUSU02   77D7F12      TRUE        0  LOCAL_ACT_LS
  PUSU01       STFNET.PUSU01   77D7F11      TRUE        0  LOCAL_ACT_LS
```

Table 64. Output Description

Column title	Description	Key values
Name	Configured link station name for the internal link to the dependent PU.	--
SSCP PU name	VTAM's name for this PU, received in the ACTPU.	--
Node ID	Configured ID block and ID number for this internal dependent PU.	--
Auto act	Whether this link will automatically activate when APPN starts.	TRUE FALSE
Sense	Sense code for last link failure.	--
State	Current internal logical link status	**Steady states** LOCAL_RESET_LS = reset (down) LOCAL_ACT_LS = active (up)**Going-up states** LOCAL_SENT_CREATE_TG LOCAL_SENT_ACT_AS**Going-down states** LOCAL_SENT_DESTROY_TG LOCAL_PEND_DEACT

list port_information

Use this command to display a list of configured physical and logical APPN router ports and their status.

Example:

```
APPN > li port
  Intf        Name       DLC Type        HPR          State
 ============================================================
    5        TR005       IBMTRNET       TRUE       ACT_PORT
    0         TR00       IBMTRNET       TRUE       ACT_PORT
```

Table 65. Output Description

Item	Description	Key values
Intf	Router's logical interface number for this port.	--
Name	Configured APPN port name.	--
DLC type	Configured or physical interface type.	ETHERAND = ethernet FR = frame relay HPR_IP = enterprise extender IBMTRNET = token-ring PPP MPC+ = multi-path channel + SDLC X25 = X.25 QLLC
HPR	Default HPR status you configured for dynamic links on this port.	TRUE FALSE
State	State of the physical or logical interface as APPN perceives it.	**Steady states** RESET_PORT = reset (down) ACT_PORT = active (up) **Going-up** SENT_ENABLE SENT_ACT_SAP**Going-down** PEND_START_PORT_DEACT PEND_LS_DEACT_ORD_PORT PEND_LS_DEACT_IMM_PORT SENT_DEACT_SAP

list port_information *port-name*

Use this command to display detailed configuration and status information about one particular port.

Example:

```
APPN > li port t00004

Port Information
===================================
       port_name = T00004
       dlc_name = IBMTRNET
       port_num = 4
       max_rcv_btu_size = 2048
       ls_role = NEGOTIABLE
       sap_value = 04
       mac_addr = 401111111111
       hpr_sap_value = C8
       pan_uplink = FALSE
```

```
adjacent node subnet affiliation = NEGOTIABLE
subnet visit count = 3
hpr_supp = FALSE
port state = ACT_PORT
```

Table 66. Output Description

Item	Description	Key values
DLC name	Port type	Same values as DLC type field in ″list port″
Port num	Router logical interface number for this port	--
LS role	Initial local link station role on this interface.	PRIMARY SECONDARY NEGOTIABLE
Pan uplink	Whether dynamic links on this port are configured as Branch Extender (peripheral access node) uplinks (EN appearance upstream to NN).	TRUE FALSE
Adjacent node subnet affiliation	Whether dynamic links on this port are configured to be EBN links to a different topology subnet.	NATIVE NON-NATIVE NEGOTIABLE
HPR support	Configured support for HPR on dynamic links on this port	TRUE FALSE
Port state	State of the physical or logical interface as APPN perceives it	Same values as in **list port**

list rtp

Use this command to display a list of the entries in the RTP Partner Table, and summary information about all active RTP connections with an endpoint in the router (the RTP Connection Table).

The RTP Partner Table does not appear if there are no entries in it. An entry is created for each remote node for which all of the following are true:

- The router performed an RTP Route Setup to the node
- The node uses only one NCE for all its RTP connections
- The node has at least one active RTP connection with the router

Note that an RTP Route Setup is not performed during CP-CP or RSETUP RTP activation, so there will be no entry for an adjacent node if the only active RTP connections to it are for carrying CP-CP session or Route Setups. Also note that all levels of the IBM 3746-900/950, and recent levels of VTAM, use multiple NCEs.

Example:

```
APPN > li rtp
RTP PARTNER TABLE:
 Remote Partner Name  Remote Boundary Name  TG Number
======================================================
         STFNET.NN12           STFNET.NN12     -1
      STFNET.VLNN045       STFNET.CP3174BC     21
RTP CONNECTION TABLE:
   TCID             CP Name  ISR  APPC  Pathswitch    Alive    COS TPF TG Number
===============================================================================
31BE30E0       STFNET.NN12    0    1        180       180    CPSVCMG      21
```

```
31BE4428      STFNET.NN12    0    1        180       180    CPSVCMG      21
31BF4850      STFNET.NN12    0    0          0       180     RSETUP      21
31BF5B98      STFNET.NN12    0    1        180       180   SNASVCMG      21
31BF6EE0      STFNET.NN12    0    8        180       180   #CONNECT      21
```

Table 67. Partner Table

Item	Description	Key values
Remote partner name	CP name of the node in which an RTP connection terminates.	--
Remote boundary name	CP name of the next ISR node adjacent to the remote partner node, or LU name of the remote application using the RTP connection.	--
TG number	TG number of the TG to the next ISR node adjacent to the remote partner node. A value of “-1” indicates that the session which caused RTP activation ended in the remote partner node; in this case the ″Remote boundary name″ is the name of session’s destination LU in the remote partner node.	--

Table 68. Connection Table

Item	Description	Key values
TCID	Transport Connection ID, a unique identifier for this RTP connection shared by its two end-points.	--
CP name	CP name of the node in which this RTP connection terminates.	--
ISR	Number of ISR LU-LU sessions routed onto this RTP connection in the router. This number includes the following session types: • Sessions from LUs in external nodes that come in ISR and leave on HPR, whether routed using DLUR or not • Sessions from TN3270 LUs in this router that leave on HPR, but only if routed using DLUR (sessions on subarea links cannot use HPR)	--
APPC	Number of LU6.2 sessions with an endpoint in this router that are routed onto this RTP connection. This number can include the following session types: • CP-CP sessions to HPR CF-tower capable nodes • DLUR-DLUS pipe sessions • Focal point sessions • Aping sessions	--
Pathswitch	Maximum time in seconds to do a path switch, before failing the RTP connection	--

Table 68. Connection Table (continued)

Alive	Time in seconds between heartbeat messages when there is no user traffic	--
COS TPF	Class of Service name for all sessions on this RTP connection. Depending on connection setup timing conditions, it is normal to see parallel RTP pipes (same endpoints) with the same class of service.	CPSVCMG = CP-CP sessions SNASVCMG = DLUR-DLUS or FP sessions #BATCH = standard low-priority #CONNECT = standard medium-priority #INTER = standard high-priority other architected and user-defined names exist
TG number	Link/TG number for the first hop of the RTP connection out of the router.	--

list rtp *tcid*
Use this command to display detailed status and statisical information about one or all RTP connections.

Example:

```
APPN > li rtp 31CC5DA8
============================================================================
  TCID             CP Name  ISR  APPC  Pathswitch    Alive    COS TPF TG Number
31CC5DA8       STFNET.VL15    0    2         200       180    CPSVCMG      21
RemoteTCID: 00000000 31C680C8, Role: ACTIVE,  State: CONNECTED
FwdRSCV: 162B0100 12461080 150BE2E3 C6D5C5E3  *..........STFNET
         4BE5D3F1 F521                        *.VL15.
Xmit:  SentBytes SentFrames  FramesQd FramesWAck AllowdRate ActualRate Tokens?
      0x00003009 0x00000057         0          0    311Kbps      0Kbps  AVAIL
Recv:  RcvdBytes RcvdFrames OutOfSeqQ FramesDiscarded ARBmode
      0x0000349B 0x00000055         0          0       GREEN
Misc: SmoothedRoundTrip  SR_timeouts FramesResent Pathswitches
              654ms              2           0
;        0
FwdMinLinkCapacity:    15974Kb/s,     ReverseMinLinkCapacity:    15974Kb/s

Each set of data below is taken over 5 min intervals - New(top), Old(bottom)
Allwdsndrate  Actlsendrate  SmRoundTrip  FramesResent  PacketsDisc  GapsReptd
       0KB/s         0KB/s          0ms            0           0          0
       0KB/s         0KB/s          0ms            0           0          0
       0KB/s         0KB/s          0ms            0           0          0
       0KB/s         0KB/s          0ms            0           0          0
       0KB/s         0KB/s          0ms            0           0          0
       0KB/s         0KB/s          0ms            0           0          0
```

Table 69. Output Description

Item	Description	Key values
Role	Router’s role in establishing this RTP connection	ACTIVE PASSIVE
State	Current state of the connection. If the RTP connection is currently undergoing a path switch, the string ″in path switch″ is appended to the state value (e.g., ″CONNECTED, in path switch″).	CONNECTED CONNECTING DISCONNECTING OPENED CALLING LISTENING

Table 69. Output Description (continued)

Tokens?	Whether the router has permission to send at this instant in time. It is normal for Tokens to be NOT AVAIL whenever FramesQd is nonzero, as long as subsequent displays show SentBytes and SentFrames increasing.	AVAIL NOT AVAIL
ARB mode	Status the router is reporting as a receiver to its partner, based on network congestion detected through ARB calculations.	GREEN YELLOW RED
SR timeouts	Number of times the Short Request timer expired. This timer starts when the router sends a control message to its RTP partner. Timer expiration indicates that the reply did not come within the expected time.	--
MinLinkCapacity	Capacity of the slowest TG along this RTP's route.	--
Allowed send rate	Maximum data send rate permitted by the receiver. This is an average value over the 5-minute interval.	--
Actual send rate	Calculated data send rate based on actual bytes transmitted between the last two rate requests. If there is no data to send, this rate drops. This is an average value over the 5-minute interval.	--
Smoothed round trip	Average time to send data to and get reply from the other end of the connection, over the 5-minute interval..	
Frames resent	Number of frames this router resent in this 5-minute interval due to gaps reported by the receiving partner node (a single gap can result in multiple frames resent).	--
Packets disc	Number of received packets that this router discarded in this 5-minute interval, due to a shortage of APPN buffers in this router or a protocol violation detected.	--
Gaps reptd	Number of data gaps this router reported as a receiver during this 5-minute interval, to the sending partner node.	--

list session_information

Use this command to display a list of ISR sessions that flow through the router. These sessions are the same ones counted by link with the command **list isr** and include:

- Sessions that enter and exit the box using ISR
- Sessions that enter the box using ISR but exit on an RTP connection

- TN3270 LU sessions routed by DLUR that exit the box using ISR

This command does not list LU6.2 control sessions with an end-point in the router; use **list appc** to see these sessions. In order to see the full output of this command, you must have configured APPN Node Management parameters to save RSCV information for intermediate sessions.

Example:

```
APPN > li sess
     Origin CP Name         Primary LU       Secondary LU  Mode Name
=========================================================================
        STFNET.VL15        STFNET.VL15        STFNET.MVS8     #INTER
        STFNET.VL15        STFNET.VL15        STFNET.MVS8   SNASVCMG
        STFNET.MVS8        STFNET.MVS8        STFNET.VL15   CPSVRMGR
        STFNET.VL15        STFNET.VL15        STFNET.MVS8   CPSVRMGR
```

Table 70. Output Description

Item	Description	Key values
Origin CP name	CP name of the node that owns the primary LU for this session.	--
Primary LU	LU name of the primary LU.	--
Secondary LU	LU name of the secondary LU.	--
Mode name	Mode name used to set up this session. Note that mode names for LU6.2 control sessions (e.g., DLUR-DLUS pipe) do not mean that these sessions terminate in the router. Rather, they are passing through the router via ISR. Use **list appc** to see the sessions that terminate in the router.	#CONNECT = standard medium priority #INTER = standard high priority CPSVCMG = CP-CP session CPSVRMGR = DLUR-DLUS session SNASVCMG = Focal point session other mode names are architected and can also be user-defined

list status

Use this command to display a summary of general APPN configuration and status information. The output provides an “at a glance” view of current status.

Example:

```
APPN > li stat
Fully Qualified CP  NAME : STFNET.NETU24
Node up Time             : 6 hrs 50 min 21 Sec
Extended Border Node     : Not Supp    Branch Extender : Not Supp
DLUR                     : ACTIVE      TN3270E         : ACTIVE
Main Mem Stat            : OK          Buffer Mem Stat : OK
```

Table 71. Output Description

Item	Description	Key values
FQ CP name	Configured network ID and CP name of this router.	--
Node up time	Amount of time since APPN last restarted.	--
Extended border node	Whether the router is configured to be an EBN.	Supp = configured Not Supp = not configured
Branch Extender	Whether the router is configured to be a branch extender node.	Supp = configured Not Supp = not configured

Table 71. Output Description (continued)

DLUR	Whether DLUR function is configured and active.	ACTIVE = configured and running NOT ACT = not configured or not running
TN3270E	Whether TN3270 server function is configured and active.	ACTIVE = configured and running NOT ACT = not configured or not running
Main mem stat	The current state of the main part of APPN memory.	OK CONSTRED = constrained CRITICAL
Buffer mem stat	The current state of the buffer part of APPN memory.	OK SLOWDOWN CONSTRED = constrained CRITICAL

list topo node

Use this command to display topology information about a particular node in this router's topology subnet.

Example:

```
APPN > li topo node
NODE NAME []? stfnet.rbkim
 CP NAME           NODE  ROUTE  CON  TIME   RSN    BN  HPR   ICN  CDS NAT
                   TYPE  RES    GES  LEFT              SUP
;         IVE
=========================================================================
STFNET.RBKIM       NN    128    N    15     23     Y   CF     N   N   Y
ACTIVE TGs ORIGINATING FROM THIS NODE

DESTINATION CP    CP_CP     HPR  TG_TYPE  TG NUM
================================================
NETIDA.RB61        ACT       Y    APPN      21
STFNET.MVS3        ACT       Y    APPN      21
STFNET.RBBOB       NOTSUP    Y    APPN      21
STFNET.RBBRUNO     ACT       Y    APPN      21
```

Table 72. Output Description

Item	Description	Key values
CP name	Control point name of the node, which you input	--
Node type	Architected type of the node	NN EN VN = virtual node (e.g., connection network)
Route res	Route addition resistance (higher is more resistant to adding new routes through the node). This value is usually configured at the node and is not dynamic.	--
Conges	Congested or not, as dynamically reported by the node.	Y = yes N = no

Table 72. Output Description (continued)

Time left	Days remaining for this topology database entry to age out. If you need to force the entry out sooner, VTAM provides topology delete functions that can cause the router to remove entries.	--
RSN	Resource sequence number for this node, used to determine whether an received update contains new information not previously seen.	--
BN	Whether the node performs a Border Node function	Y = yes N = no
HPR sup	Level of HPR support the node can perform	BASE = ANR forwarding only TRAN = transport - can have RTP endpoints for data sessions only CF = control flow - can have RTP endpoints for data and control sessions
ICN	Interchange node - whether the node is a VTAM performing both SNA subarea and APPN function	Y = yes N = no
CDS	Central directory server	Y = yes N = no
Native	Whether the node is in the router's topology subnet. Note that a node could have the same net id yet be in a different topology subnet.	Y = yes N = no

For a description of the fields in the list "Active TGs originating from this node", see **list topo tg**.

list topo status

Use this command to display a summary of topology database statistics.

```
APPN > li topo st
Max num of Nodes allowed in Topo( 0 = limit is memory ) : 5400
Current number of Nodes in Topology                     : 25
Number of Node records purged from this node            : 0
Number of TG records purged from this node              : 0
The last flow reduction seq num sent out by this node   : 259
Topology safe store frequency ( 0 = not saved)          : 0
```

Table 73. Output Description

Item	Description	Key values
Max nodes allowed	Calculated value for the maximum number of nodes allowed in the database, based on the amount of APPN memory, the product type, and various min and max limits.	--
Number of node records purged	Number of node records deleted because they aged out or because of VTAM-initiated network topology operations.	--

Table 73. Output Description (continued)

Number of TG records purged	Number of node records deleted because they aged out or because of VTAM-initiated network topology operations	--
Last FRSN sent out	Latest flow reduction sequence number sent out by this node to any other node.	--
Topology safe store frequency	Configured time in minutes between backups of topology data base to the router's hard disk.	0 = topology safe store is not enabled

list topo tg *flag-value pairs*

Use this command to display information in the router's topology database about active TGs (links, or transmission groups) in this topology subnet.

To limit the data displayed, you can specify one or more of the following filter flags and corresponding values.

Table 74. Output Description

Filter flag	Value
-c	CP name of TG owner, can be qualified with net id or not
-n	Net id of TG owner
-p	Fully qualified name of TG partner

Example:

```
APPN > li topo tg -c c20015
 ACTIVE TG's
 TG OWNER         TG DESTINATION     CP_CP     HPR  TG_TYPE  TG       RSN

                   NUM
==========================================================================
STFNET.C20015      STFNET.VLNN045     ACT       Y    APPN      23      444
STFNET.C20015      STFNET.PDLUR2      ACT       N    APPN       1      436
```

Table 75. Output Description

Item	Description	Key values
TG owner	CP name of the node that reported this TG. Both endpoints of a TG report the TG, each as the owner with the other as the destination.	--
TG destination	CP name of the other end of the TG relative to the owner.	--
CP-CP	CP-CP session support on this TG	ACT = active NOTSUP = not supported SUPINACT = supported but inactive (e.g., parallel TGs where only one carries CP-CP sessions) UNK = unknown
HPR	HPR support on this TG	Y = yes N = no

Table 75. Output Description (continued)

TG type	Architected type of this TG	APPN INTER = interchange, a Subarea to APPN link VIRT = virtual, e.g., a link to a connection network virtual node

Log

Use this command to display APPN's internal event log.

Syntax:

log

status

view

log status

APPN keeps its own internal event log, in addition to the router's ELS event logging. Use this command to display current summary statistics about the APPN event log.

Example:

```
APPN > log st
Entries: 32, Discarded: 0, Filtered: 25959, Memory: 9348 of 273400
Filters enabled:
   none
Display direction: Descending
Top Entry:
   32|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
Bottom Entry:
    1|Jul 23 08:55:45 2F104-14 (E) NOF unable to monitor EGPE environment
Current Time:
  Fri Jul 23 15:47:35 1999
```

Table 76. Output Description

Item	Description	Key values
Entry numbers	The total number of entries, the number discarded due to the log being full, and the number filtered out as duplicates.	--
Memory size	Error log current size and maximum size in bytes. The maximum size is fixed at about 1% of APPN memory.	--
Filters enabled	A list of log output viewing filters that you currently have set.	none Severity: *severity level* Message: *message ID*
Display direction	The time order of output viewing that you currently have set.	Descending (newest at top) Ascending
Top/bottom entries	Summary line for each of these entries (order is dependent on display direction). This lets you see the time scope of the entries currently in the log.	--

Table 76. Output Description (continued)

Current time	Current day and time with same basis as log entries.	--

log view

Use the **log view** command to enter a submenu of commands for navigating and viewing the APPN event log.

When you enter log viewing mode, you can use the commands **bottom**, **top**, **goto**, **next**, and **prev** to move around and display log entries in summary mode (a page of 1 or 2-line entries at a time). You use the commands **det next**, **det prev**, and **det entry** to move around and display the details of individual log entries.

The log viewing submenu also contains commands to control settings for log viewing. You can use the **filter** command to select the minimum severity level you wish to see, or to only look for a single message type. Each use of the **filter** command overrides all previous settings; it does not combine with previous commands. You can use the **set** command to establish log viewing preferences.

Submenu syntax and functions are as follows:

Table 77. **Log view** *Submenu Syntax*

Command	Keywords and Parameters	Function
bottom		Move to bottom, show summary page
current		Redisplay current summary page
detail	next_entry	Display the next entry in detail
	prev_entry	Display the previous entry in detail
	entry_id *seq_num*	Display the specified entry in detail
filter	all	Clear output filters (show all)
	only severity action_required	Show entries with this severity or greater.
	critical	
	error	
	warning	
	informational	
	message *message-id*	Show only entries with this msg
goto_entry	sequence_num	Move to entry, show summary page
next_page		Display next summary page
prev_page		Display previous summary page
set	lines_in_page	Show this many lines in page
	direction ascending	Show newest entry last
	descending	Show newest entry last

*Table 77. **Log view** Submenu Syntax (continued)*

top		Move to top, display summary page
exit		Return to main APPN t 5 menu

Example:

```
APPN > log v
LOG VIEW
LOG VIEW >?
BOTTOM
CURRENT
DETAIL
FILTER
GOTO_ENTRY
NEXT_PAGE
PREV_PAGE
SET
TOP
EXIT
LOG VIEW > top
 32|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
 31|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
 30|Jul 23 15:08:15 2F10A-1A (I) Request Route
 29|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
 28|Jul 23 15:08:15 2F10A-1A (I) Request Route
 27|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
 26|Jul 23 15:08:15 2F10A-1A (I) Request Route
 25|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
 24|Jul 23 11:41:06 2F120-18 (C) Correlation table entry was not found.
 23|Jul 23 11:37:46 2F120-18 (C) Correlation table entry was not found.
 22|Jul 23 11:07:27 2F120-18 (C) Correlation table entry was not found.
 21|Jul 23 11:07:27 2F126-0D (E) TNS0013I %1: Keepalive processing detected error
 ; the connection between IP addr %2 and LU %3 has been ended.
LOG VIEW > det e 21
------------
Sequence Number: 210
APPN Lifetime: 7206.950 seconds
Fri Jul 23 11:07:27 1999
ProbeID 226066B3
Message 2F126000-0000000D
Severity: Error

TNS0013I %1: Keepalive processing detected error ; the connection between IP addr
 %2 and LU %3 has been ended.
(Sn)  e124102
(Sn)  15.170.99.210
(Sn)  STAT1
```

Table 78. Output Description (Summary Page, left to right)

Item	Description	Key values
Sequence number	Unique number assigned to this event when it is written to the log (not when displayed). This is the number you use with the ″goto″ and ″detail″ commands.	--
Date / time	When the event occurred, per this router's clock.	--

Table 78. Output Description (Summary Page, left to right) (continued)

Message ID	Major-minor message identifier for the condition that occurred. See the “APPN Log Event Reference Guide” for a description of every possible message. Append three zeros to the major and prepend six zeros to the minor part of the ID to map to the values in the Reference Guide.	--
Severity	APPN classification of how serious the event is. Key values are listed in the order of decreasing severity.	A = action required C = critical E = error W = warning I = informational
Event name	Brief description of the event. Use the ″detail″ command and the Reference Guide for more information.	--

Table 79. Output Description (Event Details)

Item	**Description**	**Key values**
Sequence number	Same number described above for the summary page.	--
APPN lifetime	Time in seconds from when APPN last started.	--
Date / time	Same as on summary page.	--
Probe ID	ID for the exact software location that logged this error.	
Message ID	Same as on summary page, but expanded with leading and trailing zeros to match the “APPN Log Event Reference Guide”.	--
Severity	Same values as on summary page, but expanded in words.	See above
Event name	Brief description of the event, enhanced by the data items listed below it. Use the Reference Guide for more information.	--
Data type labels	Identifiers for the different types of data logged with each message. See the Reference Guide for a description of the data items with each message.	(Ix) (Se) (X) others ...

Memory

Use the **Memory** command to display APPN memory usage information.

Syntax:

memory

Example:

```
APPN > mem
APPN memory status:
             Size (MB)   Percent in-use   State
   Main       152           17           OK
   Buffer      19            0           OK
   Total      171           14

APPN total shared memory size= 179200000, special use= 800
APPN main part: size = 159487200 crit_thresh= 151512840 cons_thresh= 143538480
APPN main part: inuse= 26516176 (incl: Trace tbl=65536, Error log= 1447)
APPN main part: peak memory usage= 26518048
APPN main part: event counts: crit= 0 cons= 0 OK  = 1
APPN main part: OK for last 278211 seconds
APPN bufr part: size = 19712000 crit= 18726400 cons= 17740800 slow= 13404160
APPN bufr part: inuse= 1232 reserved (< slow)= 24992
APPN bufr part: peak memory usage= 26360
APPN bufr part: event counts: crit= 0 cons= 0 slow= 0 OK  = 1
APPN bufr part: OK for last 278211 seconds
```

Table 80. Output Description

Item	Description	Key values
Total shared memory	Configured size of APPN and TN3270 server data memory, in bytes. You set this when you configure APPN. It does not include the APPN or router code space, or the data/buffer memory needed by other router components. The ″special use″ part of this is not counted in the main or buffer parts, and is for APPN system control structures.	--
Main part	Part of APPN shared memory that is used for control blocks, trace tables, internal messages, and other general fixed and dynamic data. This part includes two special data areas: - a trace table (Trace tbl) fixed at 2% of total shared memory or 64KB, whichever is larger. For Network Utility, it is fixed at 20MB. This table is allocated at APPN startup. - an event log (Error log) that grows up to 1% of total shared memory	--
Buffer part	Part of APPN shared memory that is used for packet/frame buffering. The ″reserved″ part of this is a dynamic number of committed buffer space that statistically backs a larger logical buffer space. ″(< slow)″ indicates that this value must remain below the slow threshold for normal functioning.	--

Table 80. Output Description (continued)

Main states	State of the main part of APPN memory relative to calculated threshold values. When the main state becomes progressively more congested, APPN takes some of these actions to help ease congestion: put links into local busy, and reject incoming broadcast searches.	OK Constrained Critical
Buffer states	State of the buffer part of APPN memory relative to calculated threshold values. Note that the buffer state is considered critical any time the main part is critical, regardless of the level of buffer memory usage. When the buffer state becomes progressively more congested, APPN takes some of these actions to help ease congestion: reject new sessions, pace session data flow more slowly, report the node as congested in topology updates, slow down RTP senders, put links into local busy, and even disconnect current lowest-priority sessions.	OK Slowdown Constrained Critical
Inuse, peak usage	Current number of bytes in use, and the high water mark that the in-use value ever reached.	--
Event counts	Number of times a given state occurred since APPN last restarted.	--
<state> for last nn seconds	Length of time that the memory part has been in the current state. If the node has ever entered a depletion state, additional information is provided about how long that state lasted, how long ago it was, etc.	--

Rtp status

Use the **rtp status** to display currently in-use global RTP configuration information.

Syntax:

rtp status

Example:

```
APPN > rtp stat
                    Network       High      Medium       &
nbsp; Low
Liveness timer          180        180         180         180
Path Switch Timer       180        180         180         180
Retries                   6          6           6         6
```

Table 81. Output Description

Item	Description
Network, etc.	SNA transmission priority

Table 81. Output Description (continued)

Liveness timer	Time in seconds between heartbeat messages when there is no user traffic.
Path switch timer	Maximum time in seconds to do a path switch, before failing the RTP connection.
Retries	Number of short request retries to do before attempting a path switch.

Rtp switchpath

Use the **rtp switchpath** to force an HPR path switch for an RTP connection that has an endpoint in this router. The path switch operation selects the best currently available path, which may in fact be the current path. In any case, the path switch causes a temporary suspension of user traffic flow on the specified RTP connection.

To use this command, use **list rtp** first to determine the TCID of the RTP connection you wish to force a path switch on. Type ″rtp switch″ and provide that TCID when prompted. To see the results of the path switch, use **list rtp** *tcid*, and look at the status of the connection to determine when path switch is complete (status reverts to ″active″). You can see the new path either in the RSCV or by using **rtp test**.

Syntax:

rtp switchpath

Rtp test

Use the **rtp test** command to perform an HPR route test and display information about each link hop along the path of the RTP connection. Use the **list rtp** command first to determine the TCID of the RTP connection you wish to test. This command performs the same action as the older command **test rtp**

Syntax:

rtp test

Example:

```
APPN > rtp test
Enter TCID of the route to be tested [0]? 31B96928
Route Test issued
Waiting for 10 Seconds.....
Information
============
Result     : SUCCESS
Detailed Information
====================
TG OWNER            TG DEST NAME        TGNUM  RT    DELTA    RESULT
                                               TIME  TIME
======================================================================
STFNET.VLNN105      STFNET.VL16          21       8      8    SUCCESS
STFNET.VL16         STFNET.VL15          21      68     60    SUCCESS
```

Table 82. Output Description

Item	Description	Key values

Table 82. Output Description (continued)

Result (overall)	Status or failure reason for the route test operation.	SUCCESS IN PROGRESS NO RESPONSE INVALID NCE ID INVALID TCID NO ROUTE
TG owner	CP name of the nearest node on this route hop.	--
TG dest name	CP name of the far node on this route hop.	--
TG num	Number for this link as negotiated between the owner and destination.	--
RT time	Round-trip time in milliseconds from the router to the TG destination.	--
Delta time	Round-trip time in milliseonds from the TG owner to the destination, i.e., the portion of RT time that is just for this hop.	--
Result (detailed)	Status of reaching the destination of this hop.	SUCCESS NO REPONSE

Restart

Use the **restart** command to restart APPN and TN3270 disruptively, without restarting or reloading the rest of the router software. If APPN is not already stopped, this command stops APPN before restarting.

When APPN restarts, it uses the current in-memory configuration information, whether or not that information has been written to disk using the `talk 6` **write** command (only for router models with a hard disk).

Syntax:

restart

Stop

Use the **stop** command to stop APPN and TN3270 disruptively without affecting the rest of the route.

Syntax:

stop

TN3270E

Use the **tn3270e** command to access the `TN3270E>` command prompt from which you can display information about the TN3270E configuration.

See Table 83 on page 242 for a description of these commands.

Syntax:

tn3270e

Transmit

Use the **transmit dump** command to transmit an APPN memory dump file from the router's hard disk to a TFTP server over a network interface. Use the **list dump** command to find the number of the file to transmit. You configure the TFTP server destination using the APPN `talk 6` commands **set dump target** and **enable dump-memory.**

This command is not available for routers that do not have a hard disk.

Syntax:

transmit dump-number

TN3270E Monitoring Commands

Table 83. TN3270E 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 xxviii.
Deactivate *lu_name*	Deactivates an LU in use by a TN3270 client, and to disconnect the corresponding TCP connection to that client.
List	Lists the following from configuration memory: • Connections • Connections *LU name* • Connections *IP address* • Maps • Pools • Pools *pool name* • Ports • Status
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Deactivate LU

Use the **deactivate LU** command to deactivate an LU in use by a TN3270 client, and to disconnect the corresponding TCP connection to that client. Use the **list conn** command first to determine the local LU name based on IP address, VTAM LU name, or pool name.

This command provides success/failure completion status, and you can also use list commands to check status. After deactivation, the client should no longer appear under **list conn**, and **list lu** or **list pu** *puname* should reflect the change in LU status.

Syntax:

deactivate lu *local lu_name*

List

Use the **list** command to display information about TN32870 connections.

Syntax:

list

connections

lu *internal_LU_name*

mapping

pools

pools *pool_name*

ports

pu

pu *pu_name*

rejections

status

Command **Function**

list connections *flag-value pair*

Use this command to display a complete or subset list of active TN3270 client connections.

To limit the data displayed, you can specify one or more of the following filter flags and corresponding values:

Table 84. Flag Description

Filter flag	Value
-l (flag not required, you can just type the value)	Router LU name or pool name
-i (flag not required, you can just type the value)	Client IP address, or a leading substring of that address. For example, 9.67 will satisfy all IP addresses of format 9.67.*.*
-p	VTAM primary LU name
-s	VTAM secondary LU name (normally does not match router LU name)

Example:

```
TN3270E > li conn
Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle Min
-----------------------------------------------------------------------------
PU1LU207   IW              9.37.182.187      LU-LU  NRAVM30   LU22207   8
PU1LU60    IW              9.37.176.39       LU-LU  NRAVM30   LU2260    52
PU1LU89    IW              9.37.178.49       LU-LU  NRAVM30   LU2289    288
```

Table 85. Output Description

Column title	Description	Key values
Local LU	LU name configured or host-defined in the router.	--

Table 85. Output Description (continued)

Class	Type of LU	IW = implicit workstation EW = explicit workstation IP = implicit printer EP = explicit printer
Assoc LU	For a workstation LU, the name of any associated printer LU	--
Client addr	IP address of the client. Note that a single client IP address may have multiple LUs in use, by varying its TCP source port.	--
Status	Connected state of the LU	SSCP-LU state LU-LU state blank = TCP connection exists but LU is not connected yet
Prim LU	Primary LU name as known to VTAM	--
Sec LU	Secondary LU name as known to VTAM	--
Idle min	Number of minutes since this connection carried any user data	--

list lu *internal LU name*

Use this command to display detailed configuration and status information about a single internal LU. Use the **list conn** or **list pu** *name* commands to help determine the router LU name for a particular LU.

Example:

```
TN3270E > li lu pu1lu207
LUNAME    : PU1LU207        NAU : 207              LINK NAME : VM30PU1
POOL NAME : PUBLIC          MODEL : 3270002
SSCP_LU ST:  NOT PCHSCON  ,     LUENABLE , NOT ACTLURSP , NOT TRMNOTFY
             NOT NOTIFIED ,     ACTIVATD , NOT DEACTTNG , NOT ACTIVTNG
             NOT NMVTSNT  , NOT NMVTRCV  ,     COUNTED  , NOT DACPUPEN
             NOT TERMPEND , NOT NMVTOFF
LU_LU ST  :  NOT SNTUNBND ,     BOUND    , NOT UNBNDING , NOT BINDING
FLAGS     :  NOT SEGFOR   ,     FAPBP    ,     GETPCID  , NOT BINDFRT
             NOT SESSTOP  , NOT DETCHRCV ,     LSACON   ,     HSACON
FLAGS1    :  NOT MUEXPD   , NOT PENDSF   ,     WRAPNORM , NOT INOPST
             NOT SLI      , NOT EXIT     ,     OWNED    ,     INITCOMP
VERB FLAGS:  NOT EXIT, NOT SF  , NOT TERM, NOT INIT, NOT PURG, NOT RD1
             NOT RD2 , NOT RD3 , NOT RD4 ,     BID , NOT WR1 , NOT WR2
ACTLU     :     4915        DACTLU :        0            BIND  :    0
UNBIND    :        0        NOTIFY :        1
MINI TRACE    WRAPPED : NO  NUMBER OF ENTRIES : 7
OTHERS :  14  : INIT ,NEW     : INIT ,GETPCID : INIT ,PCIDREPY: INIT ,PCHSCOND
INIT ,SENNOTFY: INIT ,NOTFYRSP
```

Table 86. Output Description

Column title	Description	Key values
LU name	LU name configured or host-defined in the router, which you input.	--
NAU	SNA 1-byte NAU address of this LU on its PU (2-254). This value is now displayed in decimal.	--

Table 86. Output Description (continued)

Link name	For subarea host links, the link station name of the external link associated with this PU. For DLUR host links, the PU/station name of the internal link to DLUR.	--
Pool name	Name of the pool through which this LU can be selected by a client.	--
Model	3270 display or printer model this LU supports.	--
SSCP_LU state	Value decodings of individual bits of SSCP-LU session status for this LU, for engineering use	--
LU_LU state	Value decodings of individual bits of LU-LU session status for this LU, for engineering use	--
Flags, Flags1, Verb flags	Other state flags for engineering use	--
Other output	Other state information for engineering use	--

list mapping Use this command to see the currently active configured mappings between client IP address and TN3270 LUs in the router. You can also test which mapping entries apply to a particular client IP address.

To limit the data displayed to the entries the server will use for a particular IP address, just specify that IP address when you invoke this command.

Example:

```
TN3270E > li map
TN3270E Client IP Address to LU Name Maps
Client IP         Address          Resource         Last
Address           Mask             Name      Port   Map  Type  Resource
---------------------------------------------------------------------------
8.1.1.99          255.255.255.255  <DEFLT>   23     Y  POOL  WORKSTATION
9.9.9.9           255.255.255.255  LU45      0      Y  LU    WORKSTATION
9.1.1.1           255.255.255.255  LU47      0      Y  LU    PRINTER
4.4.4.4           255.255.255.255  LU46      0      Y  LU    WORKSTATION
7.7.7.7           255.255.255.255  LU48      0      Y  LU    PRINTER
2.2.2.2           255.255.0.0      POOL2     0      N  POOL  PRINTER
1.1.1.1           1.1.1.1          POOL1     0      N  POOL  WORKSTATION
0.0.0.0           0.0.0.0          <DEFLT>   0      N  POOL  WORKSTATION
```

Table 87. Output Description

Item	Description	Key values
Client IP address	IP address seed for matching client IP addresses	--
Address mask	Bit mask to be applied to the address seed and incoming client addresses to determine whether this mapping applies to this client. Only bit positions where the mask bit is 1 are compared.	255.255.255.255 = compare the entire incoming client IP address
Resource name	LU name or pool name configured in the router	<DEFLT> = the globally configured default pool

Table 87. Output Description (continued)

Port	Server destination TCP port for incoming connections to be matched against this entry.	0 = entry applies to all destination ports
Last map	If a match is found on this entry but cannot be satisfied by the pool/LU, whether the server should go on to try and match the connection against less specific entries.	Y = yes N = no
Type	Whether the resource name is an LU or pool	LU POOL
Resource	Type of LU or type of LUs in pool	WORKSTATION PRINTER

list pools
Use this command to list configured named pools of implicit LUs. Clients can request any LU in a pool by passing the pool name on their connection request.

Example:

```
TN3270E > li pool

TN3270E Implicit pools
Default pool name : PUBLIC
Name         Class
----------------------------
PUBLIC       WORKSTATION
POOL2        PRINTER
POOL1        WORKSTATION
POOL3        WORKSTATION
POOL4        WORKSTATION
```

Table 88. Output Description

Item	Description	Key values
Default pool name	Name of the global default pool into which all implicit LUs not placed into another pool fall. This is the pool referenced by the string <DEFLT> in various commands and displays.	--
Name	Configured name of the pool	--
Class	Configured type of LUs in the pool	WORKSTATION PRINTER

list pools *poolname*
Use this command to show detailed configuration information about a single LU pool. This command allows you to see how the LUs in a pool are distributed among dependent PUs, how they are named, and what type they have. For full information about the LUs under a particular PU, use the **list pu** *name* command.

Example:

```
TN3270E >li pools pool1
TN3270E Implicit Pool
----------------------------------------------------------------------------
Pool Name : POOL1                                Pool Class  : WORKSTATION
        Station Name  : PU1
                LU Name Mask : @02LU
                Number of lus :200
                Model Type : 3270 mod 2
```

Example:

```
TN3270E >li pools pool2
TN3270E Implicit Pool
----------------------------------------------------------------------------
Pool Name : POOL2                                Pool Class  : PRINTER
        Station Name  : PU1
                LU Name Mask : @03LU
                LU Address Range : 5-10,78-99
                Model Type : SCS

        Station Name  : PU1
                LU Name: LU48
                NAU Address :  48
                Model Type : 3270
```

Table 89. Output Description

Item	Description	Key values
Station name	For subarea host links, the link station name associated with the dependent PU. For DLUR host attachment, the local PU name.	--
LU name mask	For implicit LUs only, the configured name seed the router uses to generate LU names in the given address range or number.	--
LU address range	For implicit LUs only, the NAU address range the router uses to generate LUs in this pool under this PU.	--
Number of LUs	For implicit LUs only, the number of LUs the router generates under this PU.	--
LU name	For an individual explicit LU only, the configured LU name.	--
NAU address	For an individual explicit LU only, the 1-byte NAU address for the LU.	--
Model type	Configured type of the single LU or group of LUs.	**For displays:** 3270 mod 2 3270 mod 3 3270 mod 4 3270 mod 5 **For printers:** 3270 SCS

list ports
Use this command to display all the TCP ports that TN3270 clients can connect to, and the configured characteristics of each port.

Example:

```
TN3270E > li ports
TN3270E Server Ports
Port Number   TN3270E   Resource Name    Disable Filtering
--------------------------------------------------------
23             Y        <DEFLT>            N
45             Y        <DEFLT>            N
66             Y        <DEFLT>            Y
88             Y        POOL1              N
99             Y        <DEFLT>            N
```

Table 90. Output Description

Item	Description	Key values
Port number	Destination TCP port number in the router that clients connect to.	--
TN3270E	Whether this port is configured to support ″E″ clients or not.	Y = yes N = no
Resource name	Configured pool name for clients connecting to this port.	<DEFLT> = the global default implicit pool other names are user-configured
Disable filtering	Whether client IP address maps should be checked for clients connecting to this port.	Y = yes N = no

list pu Use this command to display all internal dependent PUs configured for TN3270 LUs, including those that use DLUR and those that use subarea host links.

Example:

```
TN3270E > li pu
PU NAME    STATUS        NODE ID   TOTAL  DDDLU    -------LUs  IN------
                                   LUs    ENABLED  ACTIV OW
NED AVAILABL
-----------------------------------------------------------------------
VM30PU1    ACTPU_RCVD    07711111  249    N        249      5    244
VM30PU2    ACTPU_RCVD    07722222  249    N        249      5    244
```

Table 91. Output Description

Column title	Description	Key values
PU name	For PUs associated with subarea links, the configured link station name of the host link. For PUs associated with DLUR, the configured local PU name.	--
Status	Current status of the SSCP-PU session	ACTPU_RCVD NOT ACTIVE
Node ID	The internal configured node id that represents this dependent PU to VTAM.	--
Total LUs	The current number of LUs defined in the router under this PU. This includes both configured LUs and active host-initiated dynamic LUs.	--
DDDLU enabled	Whether this PU is configured for dynamic LU definition.	Y = yes N = n
LUs active	Number of LUs that have been ACTLU'd from the host. This number can include both configured and host-initiated DDDLU LUs.	--
LUs owned	Number of LUs that are associated with client TCP connections.	--

Table 91. Output Description (continued)

LUs available	Number of LUs that are active or DDDLU-capable and are not owned, so are available for use by TN3270 clients. This number can include configured LUs whose PU is active and supports DDDLU, but does not include host-initiated DDDLU LUs unless they are active.	--

list pu *pu-name*

Use this command to display configuration and status information for all LUs under a particular dependent PU in the router. These LUs include:

- configured implicit LUs, whose names the router generates based on configured name seeds, and whose NAU addresses the router assigns based on configured numbers of LUs or address ranges
- configured explicit LUs, whose names and NAU addresses are completely configured
- host-initiated dynamic LUs, whose names and NAU addresses are set by the host

Example:

```
TN3270E > li pu vm30pu1
PU NAME    STATUS        NODE ID   TOTAL  DDDLU    -------LUs  IN------
                                   LUs    ENABLED  ACTIV OW
NED AVAILABL
-------------------------------------------------------------------------
VM30PU1    ACTPU_RCVD     07711111  249    N        249      5    249
-----------------------------------------------------------------------
LU NAME   NAU  STATUS   OWN  POOL     SSCP_LU   LU_LU   FLAGS  FLAGS1
          ADD                NAME     STATUS    STATUS
----------------------------------------------------------------------
PU1LU2     02  ACTIV    NO   PUBLIC   (04,20)   00        02    00
PU1LU3     03  ACTIV    NO   PUBLIC   (04,20)   00        02    00
PU1LU4     04  ACTIV    NO   PUBLIC   (04,20)   00        02    00
PU1LU5     05  ACTIV    NO   PUBLIC   (04,20)   00        02    00
PU1LU6     06  ACTIV    NO   PUBLIC   (04,20)   00        02    00
PU1LU7     07  ACTIV    NO   PUBLIC   (04,20)   00        02    00
```

Table 92. Output Description

Item	Description	Key values
LU Name	Name of the LU as it is known to the router. This name is either fully configured at the router, generated by the router based on a configured seed value, or passed from the host for a host-initiated dynamic LU.	--
NAU add	The 1-byte SNA address for this LU under this PU. This value is either configured at the router, selected by the router, or passed from the host. The value is now displayed in decimal.	--
Status	Current status of this single LU	ACTIV NOT ACT
Own	Whether this LU is associated with a TN3270 client TCP connection	YES NO

Table 92. Output Description (continued)

Pool name	Pool name through which a client may be assigned this LU.	Blank for explicit LUs
SSCP_LU status, LU_LU status, Flags, flags1	Hex values of status fields for engineering use. To see these values decoded, use the **list lu** *name* command.	--

list rejections Use this command to display a list of up to 99 of the most recently rejected TN3270 client connections. This can help you see and correct the reason for the rejections. The list is sorted with the most recent rejection at the top, and shows all rejections including multiple attempts by the same client.

Example:

```
TN3270E > li rej
Connection Rejection Table
-----------------------------------------------------------------
  1 Time   : 7/23/1999 11:09:00
    Client : 15.170.99.210
    Reason : Client is not authorized by Filter entries
  2 Time   : 7/23/1999 11:08:59
    Client : 15.170.99.210
    Reason : Client is not authorized by Filter entries
  3 Time   : 7/23/1999 11:08:59
    Client : 15.170.99.32
    Reason : Client is not authorized by Filter entries
```

Table 93. Output Description

Item	Description	Key values
Time	Day and time the rejection occurred.	--
Client	IP address of the client.	--
Reason	Text describing why the server rejected the client connection. There are currently over 40 reasons defined.	Example reasons include: Node is terminating Couldn’t get memory No LUs available Requested LU not found/available LU type validation failed LU capping value reached LU Pool depleted APPN memory constrained

list status Use this command to display a summary of configuration and current status information for the TN3270 server function.

Example:

```
TN3270E > li st
TN3270E Server Status Summary

TN3270E IP Address: 9.37.179.142
NetDisp Advisor Port Number: 10008
Keepalive type: NOP          Frequency: 60
Automatic Logoff: N
Client IP Address mapping : N
Number of connections                : 10
Number of available LUA LU's         : 498
Number of LUA LU's pending termination : 0
```

```
Number of defined LU's                 : 498
Number of connections in SSCP-LU state : 0
Number of connections in LU-LU state   : 10
```

Table 94. Output Description

Item	Description	Key values
IP address	IP address within the router to which the TN3270 clients connect	--
NetDisp advisor port number	TCP port number to which the Network Dispatcher load balancing function can connect to poll for load information on this server.	--
Keepalive type	Whether and how the server polls clients to see if they are still active.	None = server does not poll clients, and will discover client absence only when trying to send data NOP = server polls clients at the TCP level Timing mark = server polls clients at the TN3270 level
Frequency	Interval in seconds between keepalive polls	--
Automatic logoff	Whether or not the server disconnects clients after a period of inactivity (no data flowing in either direction).	Y = yes N = no
Client IP address mapping	Whether the server is globally enabled to map incoming IP addresses to LU/pool names	Y = yes N = no
Number of connections	Current number of active TCP connections to TN3270 clients	--
Number of available LUA LUs	Number of LUs that are currently activated from the host, or are dynamically capable of activation. This includes LUs that are in currently in use by TN3270 clients.	--
Number of LUA LU's pending termination	Number of LUs that are going down, and the router is waiting for host confirmation. These LUs are no longer associated with TN3270 client connections.	--
Number of defined LU's	Number of LUs that are either configured in the router or active host-initiated dynamic LUs.	--
Number of connections in SSCP-LU state	Number of active TCP connections associated with an LU in SSCP-LU state. When the LU associated with a connection is bound by an application and enters LU-LU state, this number is decremented (even though the SSCP-LU connection is still active).	--
Number of connections in LU-LU state	Number of active TCP connections associated with an LU in LU-LU state.	--

APPN Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

APPN supports the CONFIG (Talk 6) **delete interface** command with the following considerations:

- When an interface is deleted, the ports and links defined over this interface are deleted when APPN is restarted.
- If an **activate_new_config** from Talk 6 or a **restart** from Talk 5 is issued before a device reload, any of the interfaces greater than the interface deleted will not be redefined successfully.

GWCON (Talk 5) Activate Interface

APPN supports the GWCON (Talk 5) **activate interface** command with the following consideration:

When an interface is activated, the ports and links in APPN SRAM for this interface are defined to the APPN node and activated.

All APPN interface-specific commands are supported by the GWCON (Talk 5) **activate interface** command.

GWCON (Talk 5) Reset Interface

APPN supports the GWCON (Talk 5) **reset interface** command with the following consideration:

- When an interface is reset, the ports and links defined over this interface are taken down. If the link is a subarea TN3270E link, the APPN node will be restarted. For a normal port, the port and link definitions are deleted. After the interface becomes active, the port definitions and link definitions are redefined and activated.

All APPN interface-specific commands are supported by the GWCON (Talk 5) **reset interface** command.

GWCON (Talk 5) Component Reset Commands

APPN supports the following APPN-specific GWCON (Talk 5) **reset** commands:

GWCON, Protocol Appn, Restart Command

Description:
This command restarts the APPN node.

Network Effect:
The APPN data flowing through this node will be disrupted. APPN is stopped and restarted.

Limitations:
The changes made to the APPN configuration (Talk 6) will also be reflected.

All APPN commands are supported by the **GWCON, protocol appn, restart** command.

CONFIG (Talk 6) Activate Commands

APPN supports the following CONFIG (Talk 6) **activate** commands:

CONFIG, Protocol APPN, Activate_new_config Command (OR) CONFIG, Protocol APPN, TN3270E, Activate_new_config Command

Description:
This command activates any changes made to APPN config.

Network Effect:
If the change cannot be activated dynamically, APPN is restarted.

Limitations:

- If the change cannot be activated dynamically, APPN is restarted. Examples of this are changes to any of the node parameters, the default DLUR parameters, or the global tn3270e parameters. Some of the deletion commands also restart the APPN node. Deletion of link stations or ports does not restart the APPN node except if the link stations are subarea tn3270e links.
- If the changes are made to the tuning parameters, a device reload or restart is required.

All APPN commands are supported by the **CONFIG, protocol appn, activate_new_config (OR) CONFIG, protocol appn, tn3270e, activate_new_config** command.

Chapter 4. Using AppleTalk Phase 2

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

- "Basic Configuration Procedures"
- "AppleTalk 2 Zone Filters" on page 256
- "Sample Configuration Procedures" on page 257

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.
- 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 over PPP

There are two modes for AppleTalk over PPP, full-router and half-router. In full-router mode, the point-to-point network is visible to other AppleTalk routers. In half-router mode, the point-to-point network is invisible to other routers, but it still transmits AppleTalk routing information and data packets.

To set up your network for full-router mode, give each router on the PPP link a common network number, a common zone name, and a unique node number. If you configure one end of the PPP link with a non-zero network number, you must also configure that end to have a non-zero node number and to have a zone name. In this case, the other end of the link must have either:

- The same network number and zone name and a different node number.
- Network and node numbers set to zero. The router will learn network and node numbers from the configured router.

To set up your network for half-router mode, configure both routers on the PPP link so that network and node numbers are set to zero and no zone name is used.

AppleTalk 2 Zone Filters

Zone name 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 zone names. These zone name 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 zone names of the new network. Note that the net range is repeated in every new RTMP update but that the zone names 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 AARPed 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 Zone Name 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 zone list 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 263. 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.

Note: Do not set a network range or a node number for half routers.

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 11.

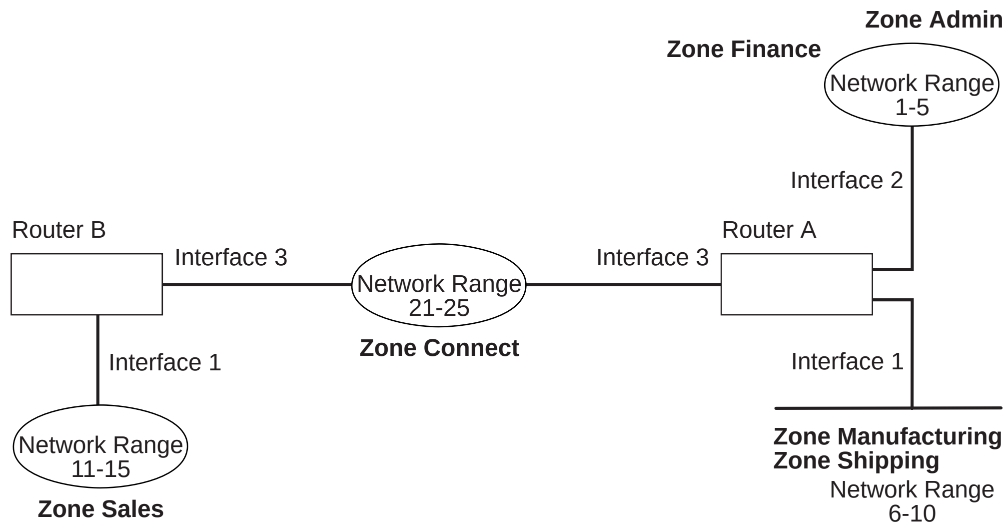


Figure 11. Example of Zone Filtering

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 12 on page 261.

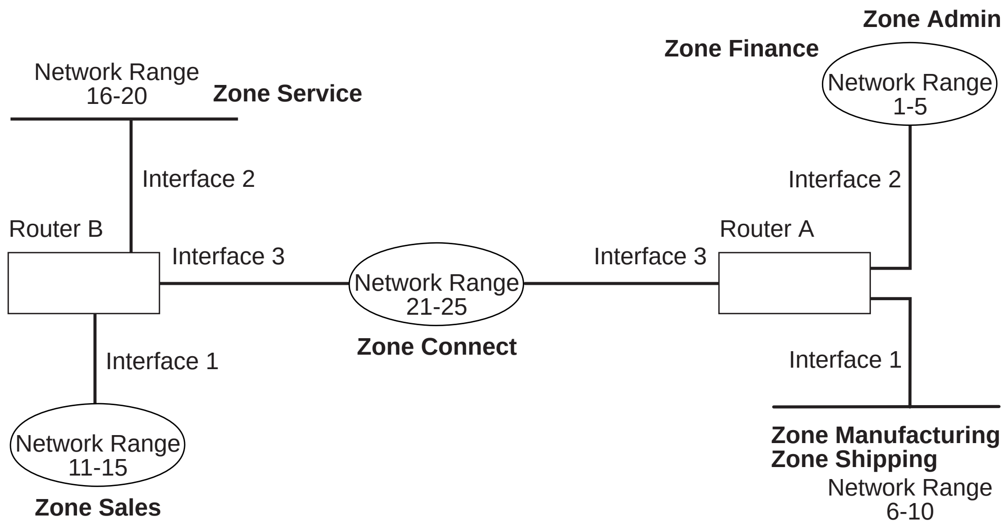


Figure 12. Example of Network Filtering.

The following steps show how to filter Network 6-10 so that it is not visible to Network 16-20 as shown in Figure 12.

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.

Chapter 5. 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"
- "AppleTalk Phase 2 Configuration Commands"
- "Accessing the AppleTalk Phase 2 Monitoring Environment" on page 270
- "AppleTalk Phase 2 Monitoring Commands" on page 270

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 95 shows the commands.

Table 95. 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 xxviii.
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 xxviii.

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 interfaces 0 and 1

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
0               1000-1000        /  1       "SerialLine"(Def)
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing enabled
1               10-19            /  52  "EtherTalk", "Sales"(Def)
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing enabled
2               unseeded net     /  0
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing disabled
```

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.

Setting the first value to zero on a Point-to-Point (PPP) interface allows that interface to operate in ″half-router″ mode. In half-router mode, neither of the two ends of a PPP network is configured with a network range or a zone list which reduces the amount of configuration needed. Both routers on a PPP network must operate in the same mode.

Note: When connecting a 2212 to an IBM 6611 using a PPP interface, set the 2212 for “half-router” mode which is the *only* mode of operation supported by the IBM 6611 for AppleTalk communications over a PPP interface.

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 96 shows the commands.

Table 96. 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 xxviii.
Atecho	Sends echo requests and watches for responses.
Cache	Displays the cache table entries.

Table 96. AppleTalk Phase 2 Monitoring Command Summary (continued)

Command	Function
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 xxviii.

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. If the outgoing interface is an unnumbered half-router PPP interface, the router uses any one of its LAN interface network nodes.

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. If the outgoing interface is an unnumbered half-router PPP interface, the router uses any one of its LAN interface network nodes.

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
FR/0             0
Eth/0            4
PPP/0           22
```

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.

Zones Specifies the human-understandable name for that network. The zone names are 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
  PPP/0       0/1 on net 1000-1000  default zone "SerialL ine"
  Eth/0       10/52 on net 10-19    default zone  "Sales"
  PPP/1       0/0 in startup range
  TKR/0       0/0 on net 20-29 default zone "Backbone"
```

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 6. 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

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 2212 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 277. Distributes topological information to support the routing services provided by VINES IP.
- "Internet Control Protocol (ICP)" on page 280. 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 280. 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 97 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 97. 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.

Table 97. Vines IP Header Fields Summary (continued)

VINES IP Header Field	# of Bytes	Description
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 13 on page 278 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 13. 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 14 on page 279 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 14. Sample Neighbor Table

Neighbor Table Field
Description

Nbr Address
The address of the neighbor node. In Figure 14, 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 98 summarizes the states the service and client nodes enter during VINES ARP implementation.

Table 98. 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.

Table 98. Client and Service Node VINES ARP States (continued)

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 **restart** or **reload** after the OPCON prompt (*) and answer **yes** to the following prompt:

```
Are you sure you want to restart (or 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.

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 7. 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 99. 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 xxviii.
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 xxviii.

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 2212s 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 2212s 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 100. 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 xxviii.
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 xxviii.

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 1/2 minutes. 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-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 8. Using DNA IV

This chapter describes IBM’s implementation of Digital Network Architecture Phase IV (DNA IV) and includes the following sections:

DNA IV Overview

DNA IV is a collection of software components that transfer information between networks connected by physical media. By transferring information, DNA IV software facilitates communication between network devices, such as personal computers, file servers, and printers.

DNA IV protocol is the underlying protocol for Digital Equipment Corporation’s DECnet software products as well as DNA-compatible products. DNA IV protocol includes the following:

- Routing software for DNA IV protocol networks.
- NCP, an implementation of the DNA IV Network Control Program. For more information, refer to the appropriate DECnet-VAX documentation, published by Digital Equipment Corporation.
- Support for DNA IV Maintenance Operations Protocol (MOP).

DNA IV performs two major functions:

- Maintains a complete routing database on all nodes in its area. (If the router is operating as a level 2 router, it maintains the database for all areas as well.)
- Routes incoming DECnet data packets to the appropriate destinations based on its own routing database. It ignores packets that are addressed to the router that are not hello packets or routing packets.

DNA IV supports the following:

- Multiple areas on an Ethernet or Token-ring network.
- Basic MOP operations. DNA IV responds to a MOP Request ID message with a MOP System ID message. DNA IV also sends a MOP system ID Message when a circuit comes up. You can monitor MOP messages using the Ethernet configuration module under DECnet-VAX NCP. The router NCP does not include an Ethernet configuration module.
- LAT Protocol. LAT protocol is not part of the DNA IV protocol family. It is an Ethernet-only protocol intended only for short-distance (limited round-trip time) communications. (CTERM protocol provides wide-area terminal support using DNA IV protocols across routers. The **set host** command in DECnet-VAX provides the CTERM protocol.)

Special consideration should be given to the following DNA IV restrictions:

- DNA IV does not support the NSP, Session, or NICE protocols.
- DNA IV does not support the DDCMP line protocol on its directly connected synchronous lines.
- DNA IV does not provide any Phase III compatibility features because it does not support the DDCMP data link protocols used by all Phase III nodes.

- NCP (the router's implementation of the DECnet Network Control Program) implements a subset of the original NCP commands and functions.

DNA IV Terminology and Concepts

This section contains a brief description of DNA IV terminology.

Addressing

Each node has a 16-bit node address, which is the same for all interfaces on that node. An address consists of 2 fields: 6 bits of area number and 10 bits of node number. Addresses are printed in decimal with a period separating the area and the node, such as 1.7 is node 7 in area 1. If no area is given, area 1 is assumed. Any address in the range 1.1 to 63.1023 is legal. Both nodes and areas should be numbered starting from 1, with few, if any, gaps. This is because the maximum node number and the maximum area numbers are configuration options and control the size of many of the routing data structures.

There is no direct correlation between addresses and physical cabling. Routes are computed to nodes, not wires.

Ethernet Data Link Addressing

Each Ethernet interface is set to the same 48-bit physical address, which is the concatenation of a 32-bit prefix (AA-00-04-00) and the 16-bit DNA IV node address. The node address is byte-swapped (to convert from PDP11 to Ethernet byte order). Thus, DNA IV node 1.1 has Ethernet Address AA-00-04-00-01-04.

Multicast (not broadcast) is also used in routing. The three multicast addresses used by DNA IV are AB-00-00-02-00-00, AB-00-00-03-00-00, and AB-00-00-04-00-00.

802.5 Token-Ring Data Link Addressing

The implementation of DNA over IEEE 802.5 Token Ring conforms to the *DECnet Digital Networking Architecture (Phase IV) Token-Ring Data Link and Node Product Functional Specification* , Version 1.0.0, that includes support for Arbitrary MAC Addresses (AMA).

There are two types of MAC addressing, conventional DNA IV addressing, which is the concatenation of a 32-bit prefix (AA-00-04-00) and the 16-bit DNA IV area/node address or AMA that allows the DNA protocol to run on IEEE 802.5 nodes without their MAC addresses being changed by the DNA protocol. This is necessary if you follow certain IBM protocol conventions. You can select the type of addressing that you are using through the DNA configuration process (`NCP>`).

Another type of addressing representation is native bit-order. This type of address is byte-flopped when sent over the physical layer. For example, the canonical 32-bit prefix shown above (using dashes) is expressed as 55:00:20:00 in native bit-order with colons separating each byte.

X.25 Data Link Addressing

The router supports DECnet Phase IV over X.25 and can interoperate with routers running Digital's implementation of DECnet Phase IV over X.25.

You set up the local and the remote DTE address with the **set/define circuit** command when you set up a DECnet circuit. In the *call-userdata* parameter you specify the local DTE address in hexadecimal octets (characters). In the *DTE-address* parameter you specify the remote address in hexadecimal octets.

Both the local and remote DTE addresses can be up to 14 hexadecimal octets in length with two ASCII characters representing one hexadecimal octet.

Routing

DNA IV handles both forwarding of DNA IV data packets and automatic routing with other DNA IV nodes. The router performs the following DNA IV functions:

- Announces its presence by sending hello messages on each network that has DNA IV enabled.
- Maintains a list of adjacent DNA IV nodes from the hello packets it receives from other DNA IV nodes.
- Exchanges routing information with other routers.
- Forwards packets between nodes.

All end and routing nodes periodically broadcast hello messages to the all-routers multicast address. This allows each router to locate other nodes in its area.

On each broadcast network (for example, Ethernet, Token-Ring), one router declares itself the designated router for that wire. The designated router broadcasts its presence so that the end-nodes know to use it as their default gateway. Any end-node sending a packet to a node not on that wire automatically sends it to the designated router for forwarding.

In a multi-area DNA, assign priorities to routers in such a way that the designated router is a level 2 router, or is likely to be the best next hop to commonly-used destinations. This reduces the possibility of traffic from end-nodes having to take an extra hop.

Routing decisions are based on a least-cost algorithm. Each link (e.g., point-to-point, broadcast network, hop) has a cost. Every router broadcasts (to other routers only) its cost and the number of hops to get to every node in its area. In this way, each router finds the cheapest path, subject to a maximum hop count.

Routing Tables

A router forwards any DNA IV data packet it receives to the proper node based on its routing table. To maintain its routing table, a router listens to and sends level 1 updates to every node in its area. If the router’s type is set to AREA, it also exchanges level 2 routing updates.

Each router maintains a routing table with an entry for every node (up to the maximum address) and every possible next hop (all circuits and up to the maximum broadcast routers). Each entry in this table contains the cost and hop to reach a node via one circuit or next hop node. Once a second the routing table sends out a broadcast routing timer.

Area Routers

If the router is configured as an area router, it maintains a similar database for all of the areas up to the maximum area, and can exchange area routing information with other area routers. Areas are handled almost exactly the same as nodes, except messages give costs to areas, but not nodes.

The areas concept results in two types of routing nodes:

- A level 1 router only knows about one area, so it keeps track of nodes in its area. Also, it ignores adjacencies across areas.

- A level 2 router keeps an area routing database, and can have cross-area adjacencies. Level 2 routers advertise routes to all other areas, so level 1 routers send all foreign-area traffic to the level 2 routers.

End-nodes simply pass packets on to a router.

A level 2 router that can reach other areas advertises a route to node 0 within its area. When level 1 routers need to send a packet to another area, they route it toward the closest node 0. This is not necessarily the best route to that area. From there, the level 2 routing algorithm sends the packet to its destination area.

Configuring Routing Parameters

In each system you can set the following routing parameters:

- Maximum number of nodes in the area
- Maximum number of routers adjacent to this router
- Maximum number of networks on any given node
- Maximum number of end-nodes one hop away from this end-node
- Cost of a hop on each network to which this node is attached
- Values of several timers involved in sending hello messages and expecting them from other nodes

IBM's Implementation of DNA IV

The main user interface program for the router's implementation of DNA IV is called NCP. The router's NCP is a limited subset of the DECnet Network Control Program (NCP) commands. The router's NCP enables you to view and modify the various operating arguments of DNA IV and to read various DNA-specific counters.

Some of the features of the router's NCP include the following:

- NCP implements new entities: module access-control and module routing-filter.
- NCP has no **set executor buffer size** command because the router does not originate any DECnet traffic. The router can forward the largest packet any DECnet implementer can generate. It honors the buffer size restrictions of all adjacent nodes.
- NCP allows an **all** qualifier on the **node**, **area**, and **circuit** subcommands.

The router NCP is similar to NCP on DECnet-VAX, with the following differences:

- Router NCP does not include the **set node name command**, and therefore cannot assign names to nodes, or display node names with addresses.
- Router NCP does not include the **clear** or **purge** commands, nor do the **set** commands have an **all** argument. The permanent database is always copied to the volatile database when the router starts, restarts, or boots.
- A router NCP command can have only one argument.
- NCP does not have the concept of lines. To see the data that a DECnet-VAX NCP **show line** command displays, use the GWCON **interface** and **network** commands.
- Router NCP does not support cross-network commands:
  - Router NCP does not include the **tell** command, which requests NCP commands on other nodes.
  - Similarly, router NCP does not support protocol requests from other DNA routers to execute NCP commands at the router on their behalf.

Important

Before configuring DNA IV, you need to be aware of the optional security features discussed in:

- "Managing Traffic Using Access Control"
  - Provides additional security by limiting access within routers in the network.
- "Managing Traffic Using Area Routing Filters" on page 298
  - Limits access to group of areas from other areas
  - Allows blending of two DECnet address spaces

If you already are familiar with these topics, skip these two sections and begin reading at "Configuring DNA IV" on page 303.

Managing Traffic Using Access Control

Access control protects one group of nodes from other nodes on the network. Routers make all nodes on a network accessible to each other. Usually, the main forms of security are passwords and conservative use of DNA IV proxy access at the host level.

However, due to differences in the security level of machines, you might need to provide additional security by limiting access within the routers in the network. The DNA forwarder enables you to do this using access controls.

Generally, access controls are not recommended due to the following liabilities:

- Access controls affect performance of the router because every packet is tested. The more complicated the access control configuration, the greater the performance impact.
- Access controls are difficult to configure and errors in configuration are difficult to diagnose.
- Access controls cannot hide a node from the routing protocols. The node remains visible from all routers in its area.

Note: Access controls do not guarantee security; they only make intrusion more difficult. The DNA IV routing protocols used on Ethernet and other broadcast media do not have built-in security features.

Access control prevents the forwarding of DNA IV (Long Format) data packets on the basis of source address, destination address, and interface. Access control does not affect routing packets, because they use a different packet format. This makes configuring access control safer, because you cannot break the routing protocol.

To implement access control, addresses are masked and compared. That is, the address in question is masked with 1s in the bit positions to be tested, and 0s in the free area. The address is then compared to a fixed value. For example, you could use a mask of 63.1023 (all 1s), and compare it to a result of 6.23 which would be true only for node 6.23. You could use a mask of 63.0 and a result of 9.0 which would be true for any node in area 9.

These mask and compare values come in pairs for source and destination address. They are then formed into lists for an interface. Each interface can have one access control list, which is applied to packets received on that interface. This list may be inclusive or exclusive. An inclusive list is a set of address pairs that designates a corridor for traffic flow. An exclusive list is a set of address pairs that does not allow traffic flow.

In an inclusive list, the source and destination addresses are tested using the mask and compare values. If any entry's source and destination matches, the packet is forwarded. In an exclusive list, the source and destination addresses are tested using the mask and compare values. If any entry's source and destination matches, the packet is dropped. The choice between exclusive and inclusive should be made on the basis of which list will be shorter. However, exclusive access control is usually easier to configure.

When packets are dropped due to access controls, the Return to Sender Request (RQR) bit is set in the Long Format Data Packet header and the packet is returned. Then, the connect request immediately fails, because NSP Connect Initiate packets are normally sent with the RQR bit set.

Configuring Access Control

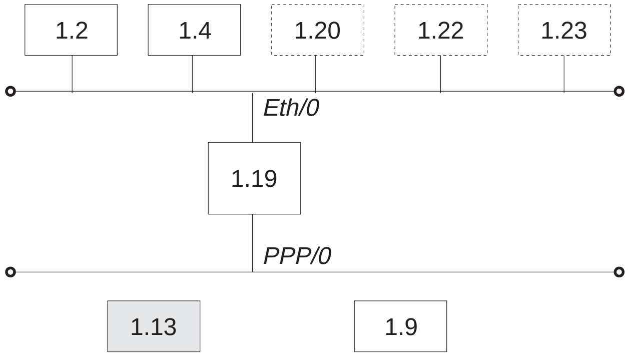
Access control limits access to a particular host or group of hosts. You must assign access control to all routes to that host, not just the preferred route. Otherwise, access control functions when the primary route is up, but fails when the secondary route is in use.

On your network map, draw a line to isolate the secure region from the rest of the network. Ideally the line should cross the minimum possible set of adjacencies so that the least number of interfaces are running with access control. For broadcast networks (Ethernet and Token-Ring), draw the line through the drop cable to the node, to identify the interface to filter. For each interface crossed by the access control line, use NCP to define the same access control list.

Note: Because all DECnet applications use the NSP protocol, which requires bidirectional connectivity, you do not need to define access controls in both directions.

Inclusive Access Control

In Figure 15 on page 297, node 1.13 wants to communicate with nodes 1.2 and 1.4 only. Access control allows you to secure nodes from all nodes connected by routers. Therefore, in Figure 15 on page 297 you can protect node 1.13 from all nodes except node 1.9 because these two nodes share the same physical network. To configure the desired access control for this example, build an inclusive filter on interface Eth/0 of router 1.19 as shown in the bottom of Figure 15 on page 297



Inclusive Filter Information

Source Result	Source Mask	Destination Result	Destination Mask
1.2	63.1023	1.13	63.1023
1.4	63.1023	1.13	63.1023
0.0	0.0	1.9	63.1023

Figure 15. Example of Inclusive Access Control

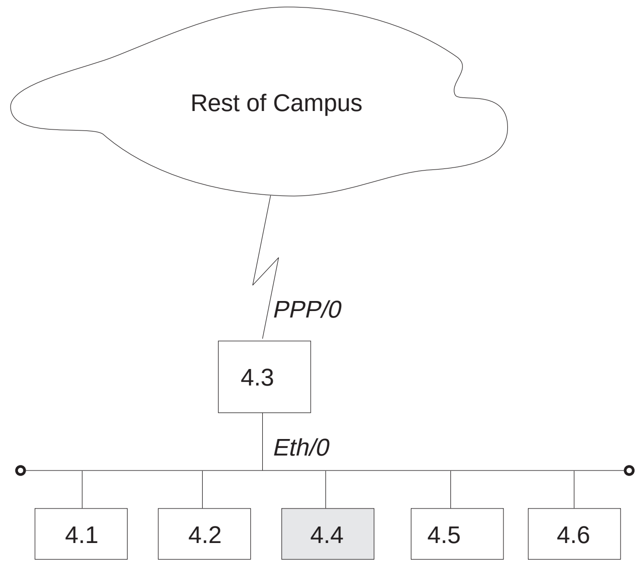
The first and second entries of the inclusive filter information shown in Figure 15 allow nodes 1.2 and 1.4 to send packets to node 1.13. The third entry allows any node to send to node 1.9 (you are not trying to secure node 1.9).

To configure the example given for router 1.19, enter the following NCP commands and parameters:

```
NCP> def mod access-cont circ eth/0 type inclusive
NCP> def mod access-cont circ eth/0 filter 1.2 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 1.4 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 0.0 0.0 1.9 63.1023
NCP> def mod access-cont circ eth/0 state on
```

Exclusive Access Control

Figure 16 on page 298 shows how exclusive access control isolates node 4.4 from the rest of the campus.



Exclusive Filter Information

Source Result	Source Mask	Destination Result	Destination Mask
0.0	0.0	4.4	63.1023

Figure 16. Example of Exclusive Access Control

Configure the desired access control for this example by building an exclusive filter on the PPP/0 interface of router 4.3 as shown in Figure 16. To configure the example given for router 4.3 in Figure 16, enter the following NCP commands and parameters:

```
NCP> def mod access-cont circ ppp/0 type exclusive
NCP> def mod access-cont circ ppp/0 filter 0.0 0.0 4.4 63.1023
NCP> def mod access-cont circ ppp/0 state on
```

Managing Traffic Using Area Routing Filters

Area routing filters allow special configurations of your DNA network. Because this is an advanced topic, very few DNA IV networks need routing filters. There are two primary applications for area filtering in DNA IV:

- Security, limiting access to some group of areas from other areas.
- Allowing the blending of two DECnet address spaces.

Note: Area Routing Filters are very tricky and subtle to configure. It is very easy to completely break your area routing. If you do not understand how DECnet routing works, especially at the area level, do not try to use routing filters. Documentation on the DECnet routing protocol can be found in *DECnet Digital Network Architecture Phase-IV Routing Layer Functional Description* , Order Number AAX435ATK, December 1983, Digital Equipment Corporation, Maynard, Massachusetts.

Area routing filters allow you to configure a router to control the information about DECnet areas that are sent or accepted in level 2 routing messages. You may configure separate incoming and outgoing filters for each interface. Each filter specifies which areas routing information will be passed to or accepted from.

When a network sends a level 2 routing update and there is a routing filter, the entry (RTGINFO) for any area not in the filter has the cost of 1023 and a hop count of 63. Any area in the filter has the correct cost and hops placed in the entry.

When the network receives a level 2 routing message and there is a routing filter, any entry for an area not in the filter is treated as if the cost is 1023 and the hop count is 63 (unreachable). Any routing entry from the packet that is in the filter is processed normally.

The routing filters affect the processing of level 2 routing messages only. There are no filters for level 1 routing messages. Routing filters have no effect on router hello processing, and do not prevent area routers from developing adjacencies. They affect the area routing database. If the filters prevent an area router from learning about another area, they would prevent the router from becoming attached, and then the router could not advertise as an area router.

Security by Area Filtering

Like access controls, routing filters provide security. However, routing filters have some disadvantages compared to access controls:

- Area filtering is less flexible than access controls because it requires the assignment of areas to correspond to the desired security architecture.
- Area filtering is more difficult to understand and configure.
- The level of security is lower because a host that ignores the lack of routing information can send the packets to the correct router anyway.

However, area filtering is more efficient because there is no need to check every packet. In the following example area filtering occurs in an area that contains workstations that are part of a large network that contains machines with confidential information. There might be one machine outside the area that the confidential machines need to reach for information.

In Figure 17 on page 300, area 13 contains workstations that need to be able to reach area 7. Node 13.1 is the router, and the other nodes are the workstations. Node 13.1 has a filter to accept only routes to area 7. Therefore, if node 13.1 receives a packet from any node in area 13 not destined for area 7, node 13.1 cannot forward the packet and sends the sending node an error message.

To configure router 13.1 in Figure 17 on page 300, enter the following NCP commands and parameters:

```
NCP> def mod routing-filter circ eth/1 incoming area 7
NCP> def mod routing-filter circ eth/1 incoming state on
```

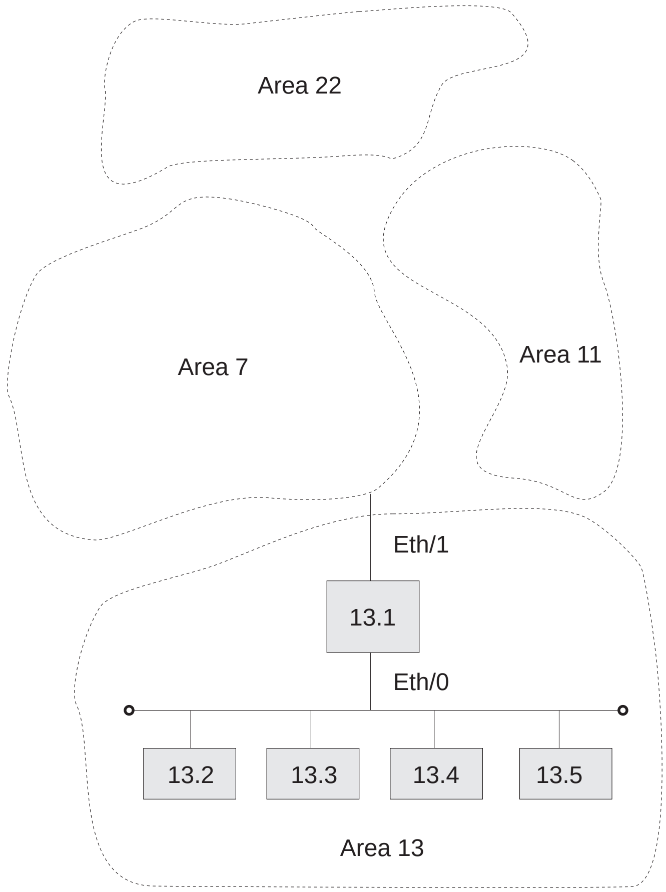


Figure 17. Example of Area Routing Filter for Security

Blending DECnet Domains

DECnet has a 16-bit node address space with a fixed hierarchy of 6 bits of area and 10 bits of node. By comparison, IP has a 32-bit node address space with a flexible multilevel hierarchy. Many established networks have now grown to the point where they use all 63 areas. The problem is that as different facilities connect to each other, they want to connect their DECnet networks but cannot due to area number conflicts.

The only solution is to redesign the DECnet architecture. (This is addressed by DECnet Phase V.) However, by using area routing filters, it is possible to allow some overlap between two DECnet domains.

Domain is not a standard DECnet term; it is used here as a name for a DECnet wide-area network, presumably one with many areas. The goal is to blend two of these domains, so that there is a common area that can reach parts of both domains. However, there are more than 63 areas in the union of the two domains. Because area filtering is not simple to administer and is restrictive, you should not consider using it if there are enough area numbers available for the union of the domains.

To configure the overlap of two domains, first you must decide which areas to intersect. These areas are the ones that will be able to participate in both domains. These area numbers must not be used elsewhere in the two domains.

Figure 18 on page 302 shows the areas that intersect are areas 1 and 2. The remainder of the areas can be duplicated between the two domains. In the example, there are two areas 3, 4, and 5, one in each domain. Note that it is never possible to allow direct connection between a node in area 3 in domain A and area 3 in domain B. The best that you can do is give the areas in the intersection the ability to talk to portions of each domain.

In designing the intersection, be careful that neither domain relies on routes through the intersection to maintain connectivity between areas that are not in the intersection. Because the routes in and out of the intersection are filtered, they probably do not offer normal reachability between all areas in the domain.

To decide how to configure the routing filters, draw a concise map of the configuration. On this map, locate all of the areas and outline the two domains. Then decide upon the filtering fence that you need to establish. Carefully go around the intersection of the two domains and locate all level 2 adjacencies that cross the filtering fence. These are one hop communications paths between level 2 routers that cross between areas.

In the example, there are six adjacencies that cross the fence, 1.18 to 5.7, 1.18 to 5.8, 1.18 to 8.3, 2.17 to 3.12, 2.21 to 4.7, and 2.21 to 4.9.

The first step in designing the area filters is to set up filters that keep the areas in one domain from being propagated into the other domain. The only area routes that should leave the intersection are those for areas in the intersection. In the example, these are areas 1 and 2. Therefore, only routes for areas 1 and 2 should be sent from nodes such as 2.17 and 3.12.

On point-to-point links such as 2.17 and 3.12, it does not matter which end filters, but it is probably safer to filter on the sending end. Therefore there would be a filter on the interface of 2.17, allowing forwarding only routes from areas 1 and 2. The same would occur on the two interfaces of 2.21 and the link from 1.18 and 8.3.

When the hop between two areas is an Ethernet or other broadcast media, such as 1.18 to 5.7 and 5.8, you should make the decision on another basis. Most Ethernets have most of the level 2 routing nodes in one area, and a few in the second area. Here, the filtering should be on the few, rather than the many. In the example, node 1.18 is the interloper on the Ethernet in area 5, so it should filter. Mode 1.18 would send routers only for areas 1 and 2 on the Ethernet.

You can filter on both ends of an adjacency. This adds an extra layer of security against accidental reconfiguration. However, if you set up only one end for filtering, then only that end filters.

Given these filters, the two domains cannot contaminate each other. However, for a node in the intersection, it is not clear which area 3 will be reached when a connection is attempted to node 3.4. It depends on the current route and the circuit costs. Clearly, this is not ideal. It does not matter that there might only be a node 3.4 in domain A and not in domain B. Routing between areas is done solely on the basis of area; only the routers inside an area know the routes to nodes in that area.

Thus, you must establish a second set of filters to decide which instance of an area (domain A or B) is reachable from the intersection for each area not in the intersection. Therefore, you could decide that nodes in the intersection could reach areas 3 and 4 in domain A and area 5 in domain B. In the example, this would be done by configuring routers 1.18 and 2.21 to only accept routes to areas 3, 4, 6, and 8 from domain A. Routers 2.17 and 2.21 would only accept routes for areas 5 and 9 from domain B.

Therefore, nodes in the intersection see a universe that contains areas 1 and 2 from the intersection, areas 3, 4, 6, and 8 from domain A, and areas 5 and 9 from domain B.

To configure router 1.18 in Figure 18, enter the following NCP commands and parameters:

```
NCP> def mod routing-filter circ eth/0 outgoing area 1,2
NCP> def mod routing-filter circ eth/0 outgoing state on
NCP> def mod routing-filter circ eth/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ eth/0 incoming state on
NCP> def mod routing-filter circ ppp/0 outgoing area 1,2
NCP> def mod routing-filter circ ppp/0 outgoing state on
NCP> def mod routing-filter circ ppp/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ ppp/0 incoming state on
```

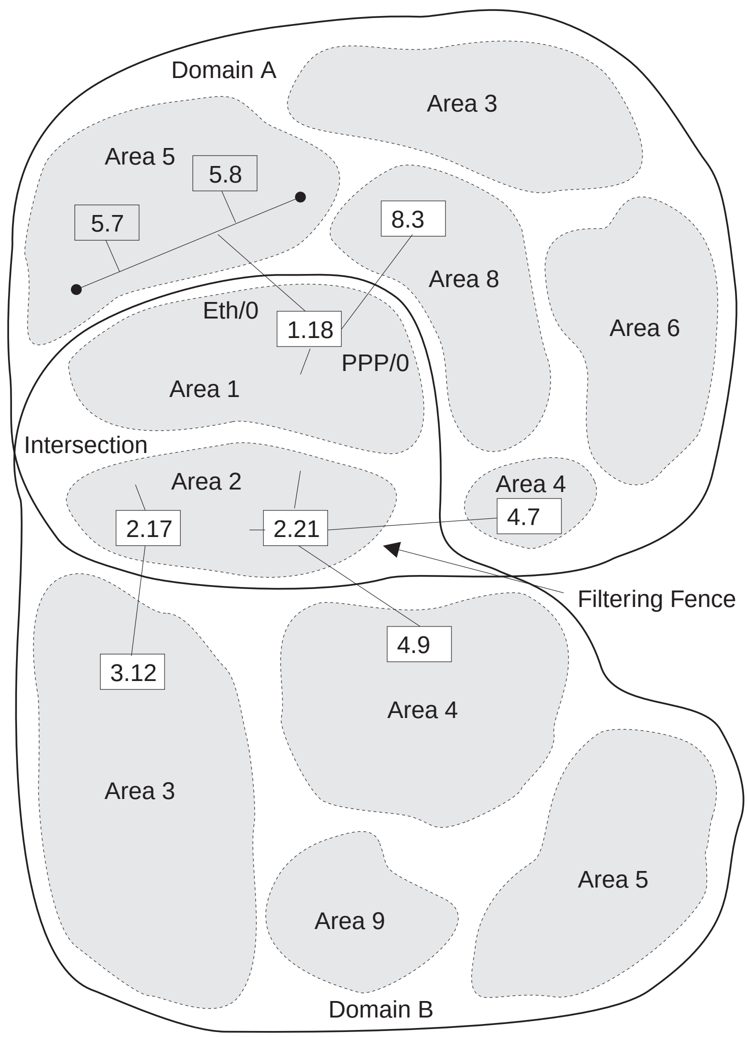


Figure 18. Example of Blending DECnet Domains

There is still no way that a node in domain A area 5 can communicate directly to a node in domain B area 5. For nodes in these two areas to communicate, you must do a series of application-level relays using the **set host** command. For example:

- Run the set host command to remotely login from a node in the domain A area 5 to a node in domain A area 8.
- Run the set host command to remotely login from a node in domain A area 8 to a node in area 1 or 2.
- Run the set host command to remotely login from a node in area 1 or 2 to a node in domain B area 5.

Configuring DNA IV

The DNA IV protocol runs over Token-Ring, Frame Relay, Ethernet, PPP, and X.25 interfaces. The following sections describe the procedures for configuring the DNA IV protocol to work over Token-Ring and X.25 interfaces.

Note: When operating in mixed DNA IV and DNA V networks, all DNA IV configuring and monitoring must be done from the process described in this chapter.

DNA IV and DNA V Algorithm Considerations

DNA IV uses a distance-vector routing algorithm. DNA V can use either a distance-vector or a link-state routing algorithm. The algorithm that the bridging router selects is according to what protocol is enabled and disabled, and any combinations that can result from these two protocols. See Table 101 for details.

Table 101. DNA IV and DNA V Algorithm Considerations

DECnet IV Status	OSI/DNA V Status	Algorithm Selected
Enabled	Disabled	Distance-vector (automatically)
Disabled	Enabled	Link-state (automatically)
Enabled	Enabled	Use the **set algorithm** command to configure this information into SRAM.

Configuring DNA IV For Token Ring

The procedure to run the DNA IV protocol over 802.5 Token Ring (TR) involves commands from the DNA IV and Token-Ring configuration processes.

1. From the OPCON prompt (*) enter the configuration process.

   ```
   * talk 6
   Config>
   ```

2. Enter **list device** to see the interface numbers for the Token-Ring interfaces. Note the interface number of each Token-Ring interface.

   ```
   Config> list device
   ```

3. Use the **network** command with the interface number of the Token-Ring interface you want to configure. This places you in the Token-Ring configuration process.

   ```
   Config> network 0
   TKR config>
   ```

4. Use the **list** command to verify the Token Ring configuration information.

   ```
   TKR config> list

   Token-Ring configuration:

   Packet size (INFO field):    2052
   Speed:                       4 Mb/sec
   Media:                       Shielded
   ```

```
RIF Aging Timer:             120
Source Routing:              Enabled
Mac Address    000000000000
```

5. Exit the Token-Ring configuration process and enter the DNA NCP configuration process.

```
TKR config> exit
Config> protocol DN
NCP>
```

6. Use the **define** command to define a DNA circuit on the Token-Ring interface:

```
NCP> define circuit tkr/0 state on
```

7. Optionally use the **define** command to set the routing type for the circuit. For bilingual or Phase IV support, you need to change the routing type from the default (standard) to either bilingual or AMA.

```
NCP> define circuit tkr/0 router type bilingual

                   or-

NCP> define circuit tkr/0 router type AMA
```

8. Use the **list** command to check the parameters.

```
NCP> list circuit tkr/0 characteristics
Circuit Permanent Characteristics
Circuit             = TKR/0
State               = On
Cost                = 4
Router priority     = 64
Hello timer         = 15
Max routers         = 16
Router type         = Standard
```

9. Restart the router, so that all configured parameters take effect.

Note: If you want to disable source-routing or set the RIF-timer to a value other than the default value, use the **source-routing** command and the **set RIF-timer** command in the Token-Ring configuration process.

Configuring DNA IV for X.25

The procedure to run the DNA IV protocol over X.25 circuits involves commands from the X.25 and DNA IV configuration processes.

1. From the OPCON prompt (*) enter the configuration process. Go to "t 6" and enter X.25 config (net #). If this is the first time X.25 is being configured then do the following:
   a. DEFINE the router's DTE address.

      ```
      X.25 Config> set address
      ```

   b. DEFINE each protocol that will be supported over X.25:

      ```
      X.25 Config> add protocol
      ```

      IP It is usually a good idea to add this protocol so that you can verify the general X.25 configure is OK

      DN

      Note: Allow protocol parameters to default.

   c. DEFINE protocol remote address to the remote X.25 address mapping for the protocols that require this:

      ```
      X.25 Config> add address
      ```

      for IP:
      - IP address = 128.185.247.22

- X.25 address = 22

for DN:
- DN address = 5.22
- X.25 address = 22

d. VERIFY that one end of the X.25 circuit is a DTE and the other end is a DCE.

```
X.25 Config> list all
```

Check the National Personality field for device type. For a national personality type of GTE-Telenet you see:

```
National Personality: GTE Telenet (DTE)

                   -or-

National Personality: GTE Telenet (DCE)
```

To change the device type to DCE, enter:

```
X.25 Config> set equipment-type dce
```

Lists all parameters configured for X.25

National Personality: GTE Telenet (DTE) National Personality: GTE Telenet (DCE)

If not, then chose one router to act as a DCE and modify as such,

```
X.25 Config> set national-personality dce
```

e. RESTART the router, so that all configured parameters take effect.

f. To VERIFY that the configuration is valid after a restart, go to the monitor side and observe if the link is coming up.

```
* t 5
+ c
```

This gives you the state of the link at that time. If you see the state of the X.25 link transitions from “testing” to “down”, go to ELS messages and see if there is an obvious error. If the state of the X.25 link transitions from “testing” to “up”, then chances are the x.25 configuration is valid.

2. To VERIFY that the X.25 link is operational:

a. TRY to PING each end of the X.25 link from the IP monitor:

```
IP> interface
```

Verify that the correct X.25 addresses had been configured in the IP protocol.

IP> **ping** *IP address of remote X.25 link*

3. To CONFIGURE DECnet PhaseIV on the Router:

a. DEFINE DECnet Executor parameters:

NCP> define exec address *area.node*
: Router’s DECnet address

NCP> define exec type DEC-ROUTING-IV
: Configures the router as a LEVEL 1 DEC type router

Note: This example is for configuring a router to interoperate with other routers supporting the DEC-routing standard over X.25 networks. A router supporting the standard must be defined as type DEC-ROUTING-IV (level 1) or DEC-AREA (level 2). The default routing type is ROUTING-IV and AREA which allows interoperation with many existing IBM 2212 and other compatible routers.

```
NCP> define exec state on
```

Restart the router so that when you configure the X.25 circuit, all DEC specific parameters are visible. To verify executor configuration, NCP> **show executor characteristics**

b. DEFINE PhaseIV X.25 circuits.

   You must configure the X.25 circuit as either a PVC or SVC. If this circuit is configured as a PVC then the other end must also be a PVC. If this circuit is configured as an IN-SVC, then the other end must be configured as an OUT-SVC

```
NCP> define cir x25/0 usage IN-SVC
NCP> define cir x25/0 DTE-address "remote X.25 DTE"
NCP> define cir x25/0 call-data
NCP> define cir x25/0 verification enabled
```

   Enabling verification is optional.

c. DEFINE circuits to the active state:

   - for Token-Ring

     NCP> **define cir TKR/0 router type bilingual**

   - for ALL circuits

     NCP> **define cir** *xxx* **state on**

   Restart the router so that all of the DECnet parameters become effective, VERIFY the X.25 configuration within the DECnet protocol is as you want it.

```
NCP> list circuit x25/0 characteristics
```

Chapter 9. Configuring and Monitoring DNA IV

DNA IV Configuration and Monitoring Commands

This section describes the NCP configuration and monitoring commands. Enter the commands at the `NCP>` prompt. ***All*** NCP commands can be accessed from either the configuration or monitoring environments.

Table 102. NCP Configuration and Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page xxviii.
define	Defines items in the nonvolatile (permanent) database, including: • Access control lists and routing filters • Circuit items • Arguments global to DNA • Configuration data from the nodes
purge module	Removes access control lists and routing filters from the permanent database.
set	Sets or changes items in the volatile database, including: • Circuit items • Arguments global to DNA • Configuration data from the nodes
show	Displays the status of the volatile database and volatile nodes in the routing database.
show/list	Displays items in the volatile (show) or permanent (list) database, including: • The current state of the specified circuits • The current state of the volatile/permanent database for DNA • DECnet access control lists that have been defined in the permanent database for the router • DECnet area routing filters that have been defined in the permanent database for the router
zero	Clears circuit counters in the volatile database, global counters in the volatile database, and counters in the access control list module. Does *not* clear the argument settings made with **set** or **define** commands.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxviii.

Note the following information about the commands:

1. The **define** commands do not take effect until the next time the router is started.
2. The **list, define,** and **purge** commands modify or display data in the permanent (router’s Static RAM) database. The permanent database is stored in the configuration, and remains in effect across restarts, software loads, and power cycles.
3. The **show** and **list** commands are the most useful for monitoring the DNA IV protocol.
4. Use **set, show**, and **zero** to modify, display, or clear data in the volatile database.
5. The **zero** command clears statistics saved in the volatile database, but does ***not*** clear the argument settings made with set or define commands.

Define/Set

This section explains both the **define** and the **set** commands.

Use the **define** command to define access control lists and routing filters, and to define circuit, executor, and node parameters. **Define** is used to set SRAM (needs reboot).

Syntax:

define	circuit-specifier . . .
	executor . . .
	module access-control . . .
	module routing-filter . . .
	node . . .

Set can be used for volatile RAM (immediate change, no reboot).

Syntax:

set	circuit-specifier . . .
	executor . . .
	node . . .

circuit-specifier *argument*

The *circuit-specifier* options include the following:

active circuits
Specifies all circuits who are up and whose state is on (set only).

all circuits
Specifies all circuits on the router.

circuit name
The name of the circuit. For example: Eth/0, TKR/0, PPP/1.

known circuits
(**set** only) Specifies all circuits on the router.

The *arguments* include the following:

call-userdata
Used during circuit initialization of static X.25 circuits. When a circuit is defined as an outgoing SVC, the initial and all subsequent call requests contain the defined call-userdata when the circuit is enabled. When a circuit is defined as an incoming SVC, one of the criteria for accepting an incoming call request is a match of the defined call-userdata.

Currently the call-userdata must be set to the DTE of your local router for both incoming and outgoing SVCs.

Enter an even number of hexadecimal characters (octets) up to a maximum of 14 characters.

cost [range]
Sets the cost to receive a packet on this circuit. This is used by the

routing algorithm to determine the cost of a circuit in choosing routes (cost is not the same as an IP metric). Range: 1 to 25. Default: 4.

The following values are suggested starting points:

Circuit type	*Cost*
Ethernet	4
Token-Ring 4/16	4
Sync 56 Kb	6
Sync T1	5
X.25	25

Example:

```
define circuit tkr/0 cost 5
```

DTE Address
Specifies the address of the remote DTE on the X.25 circuit. This is always the address of the remote system. This is a decimal number of up to 14 characters.

hello timer [range]
Specifies how often (in seconds) router hellos are sent on this circuit. Range: 1 to 8191 seconds. Default: 15 seconds (recommended).

maximum recalls
(**define** only) Specifies how many attempts the router makes to reestablish an outgoing static SVC call after an initial call failure. After the maximum number of recalls, the router makes no further attempts to establish the SVC without your intervention. Valid values are in the range of 1 to 20, the default is 1. See also the recall timer argument.

maximum routers [range]
(**define** only) Specifies how many other routers there may be on this circuit. Range: 1 to 33. Default: 16.

Note: This parameter is not user-configurable on an X.25 circuit when the executor *type* is set to DEC-routing-IV or DEC-area. In this case the maximum number of routers is 1.

If this is a level 1 router, only routers on this circuit in the same area count. If this is a level 2 router, all routers on this circuit count. The local router does not count against the limit.

The router's efficiency and memory requirements are improved by keeping this number low. Set this argument to equal a few more than the total number of adjacent routers on the circuit. Do not set this argument to less than the number of routers on the circuit; this can result in anomalies in routing.

Note: For a point-to-point (synchronous line) circuit, set this argument to 1. The result is significant memory savings on a router with multiple point-to-point lines.

The sum of maximum routers over all circuits should be less than the executor maximum broadcast routers argument, although this limit is not strongly enforced.

recall timer
Determines the delay in seconds between call attempts to establish an X.25 outgoing static circuit.

For **define**, valid values are in the range 1 to 60 seconds. The default is 1 second. See also the argument maximum recalls.

For **set**, valid values are in the range 0 to 65595 seconds. The default is 60 seconds.

router priority [range]
Specifies the router's priority in bidding to become the designated router for the end-nodes on this circuit. Range: 1 to 127, where 127 is the highest priority. Default: 64.

If two routers have the same priority, the one with the higher node address wins. The router priority has no effect on area routing decisions, or in reaching the closest attached level 2 router.

Use the router priority to choose the designated router to be the one that is most likely to be the best next hop for the end-nodes on the circuit. If there are two routers on a circuit, one with 500 nodes behind it, the other with 20 nodes behind it, the one with 500 nodes should have the higher router priority. This is not required, however, because once a packet from an end-node packet reaches a router, it will be forwarded toward its destination.

This argument is irrelevant on point-to-point lines, where there will be no end-nodes. (A designated router is selected anyway.)

router type
Specifies the kind of routing that the router needs to perform, standard, AMA, or bilingual.

- *Standard*. Specifies that the router is using conventional phase IV addressing where the MAC address is built from the area and node number. The router defaults to this type.

- *AMA*. Specifies that the router can route packets that use phase IV addressing where the MAC address is arbitrary and learned from the data link layer.

- *Bilingual*. Specifies that the router can route packets that use both conventional and phase IV with AMA addressing.

state When set to **on** specifies that the circuit is enabled for use by DNA. When set to **off** specifies that the circuit is disabled for use by DNA. **off** is the default.

usage Specifies whether an X.25 circuit is:

- PVC: A permanent virtual circuit
- OUT-SVC: An outgoing static circuit
- IN-SVC: An incoming static circuit

  This parameter applies when the executor type is set to *DEC-routing-IV* or *DEC-area*. (See **circuit executor type** for more information.)

verification
Specifies whether the router compares a verification string on the router to verification data in an incoming initialization message. If they do not match, the X.25 circuit must be reinitialized. Specify enabled or disabled.

executor *argument*
Defines or sets arguments (that is, the executor) global to DNA in the permanent (**define**) or volatile (**set**) database.

Most of these arguments reduce the efficiency of the router, and increase the load on the circuits, as they are made larger. They can also increase memory requirements. They should not be used unnecessarily in excess of the values required for the actual network configuration.

For **set**, the executor must be in the off state to modify numeric arguments or type in the volatile database. (Unlike DECnet-VMS, the **set executor state on** command is valid when the executor state is off.) These changes take place immediately without rebooting the router.

address [area.node]
Sets the executor's node address, the node ID of this router. Area range: 1 to 63. The area and the node must be less than executor maximum area. Node range is 1 to 1023. The default 0.0 is illegal.

Note: DNA will not be enabled if the executor address is not set to a legal value.

area maximum cost [number]
Maximum cost allowed between this level 2 router and any other level 2 router. If the best route to an area is more costly than this, that area will be considered unreachable. Maximum: 1022. Default: 1022. This argument does not apply to level 1 routers. It should be greater than the maximum legal cost to the most distant area. A suggested value is 25 times “area maximum hops”.

area maximum hops [number]
Maximum number of hops allowed between this level 2 router and any other level 2 router. If the best route to an area requires more hops than this, that area will be considered unreachable. Maximum: 30. Default: 30. This argument does not apply to level 1 routers. It should be about twice the longest path length (in hops) that is expected.

The hop count is used by routing only to speed the decay of routes to unreachable areas. The area maximum hops may be reduced to cause unreachable areas to become unreachable more quickly.

broadcast routing timer [range]
Specifies how often level 1 (and 2 in a level 2 router) routing messages are sent, in seconds. This is how often they will be sent in the absence of any cost or adjacency changes. This protects the routing database from corruption. At least partial routing updates are sent automatically if any cost or adjacency changes. Range: 1 to 65535. Default: 180. Lower values increase the overhead for this and all adjacent routers. Larger values increase the time required to correct the routing database if a partial routing update message is lost.

maximum address number [range]
(**define** only) Is the highest node address (within this area) for which routes will be kept by this router. The routing database will not include routes to nodes in this area with a higher node part of their address. Range: 1 to 1023. Default: 32. It should be higher than the highest node address in the router's area. Setting it excessively large will affect the efficiency of the router, and will use excess memory. This argument does not take effect until the router is restarted.

maximum area number [number]
(**define** only) Is the highest area for which routes will be kept, if this is a level 2 router. The routing database will not include routes to areas higher than this. Maximum: 63. Default: 63. It should be higher than the highest area number in the overall network. This argument does not take effect until the router is restarted.

maximum broadcast nonrouters [number]
(**define** only) Maximum number of end-nodes that can be adjacent (one hop away) to this router. This is the sum over all broadcast circuits. If there are more end-nodes, some of those end-nodes will not be reachable by this router, which may cause unpredictable routing problems. This argument does not take effect until the router is restarted. Range: 1 to 1023. Default: 63.

maximum broadcast routers [number]
(**define** only) Maximum number of routers than can be adjacent (one hop away) to this router. This is the sum over all broadcast circuits. If there are more routers, routes will not be accepted from the excess routers. This may cause unpredictable routing problems. This argument does not take effect until the router is restarted. Default: 32. Maximum: 33 times the number of circuits. This value should be greater than or equal to the sum of “circuit maximum routers” over all circuits, although this is not strongly enforced. This parameter has a strong effect on memory utilization, and should not be set much larger than required. Because the default is rather high, you may need to reduce the value if you have set a large “maximum address.”

maximum cost [number]
Maximum cost allowed between this router and any other node in the area. If the best route to a node is more costly than this, that node will be considered unreachable. Maximum: 1022. Default: 1022. It should be greater than the maximum legal cost to the most distant node. A suggested value is 25 times “maximum hops”.

maximum hops [number]
Maximum number of hops allowed between this router and any node in the area. If the best route to a node requires more hops than this, that node will be considered unreachable. Maximum: 30. Default: 30. It should be about twice the longest path length (in hops) that is expected. The hop count is used by routing only to speed the decay of routes to unreachable nodes. The maximum number of hops may be reduced to cause unreachable nodes to become unreachable more quickly.

maximum visits [number]
Specifies that any packet forwarded by this router that has been forwarded by more than maximum visits routers will be dropped.

This is used to detect packets which are in routing loops, which occur when routes decay. The maximum visits is 63. This is the default. This argument should be larger, by a factor of two, than both maximum hops and area maximum hops.

state on
Enables DNA. May be issued at any time, providing the router has a valid node address.

state off
Disables DNA. May be issued at any time. The default state is off.

For **set**, **set executor** will be inhibited if the DNA initialization failed for lack of available memory for the routing tables.

type (**define** only) On X.25 circuits, causes the router to act in one of four ways, depending on the value selected. The options are:

DEC-routing-iv
configures the router as a DEC-compatible Level 1 router.

DEC-area
configures the router as a DEC-compatible Level 2 (area) router.

Routing-iv
configures the router as a Level 1 router without DEC compatibility on X.25 circuits. This is the default.

Area configures the router as a Level 2 (area) router without DEC compatibility on X.25 circuits.

A Level 2 router accepts adjacencies with routers in other areas, and maintains routes to all areas. If it can reach other areas, it also advertises itself to Level 1 routers as a route to other areas.

For Level 1 routers, adjacencies are accepted only to routers in the same area.

Example:

```
define executor state on

define executor type DEC-area

define executor maximum broadcast routers 10
```

type area
(**set** only) Causes the router to act as a level 2 router. It will accept adjacencies with routers in other areas, and will keep routes to all areas. If it can reach other areas, it will also advertise itself as a route to other areas to level 1 routers.

The DNA state must be set to *off* before changing the *type*.

type routing-IV
(**set** only) Causes the router to act as a level 1 router, which is the default. Adjacencies will be accepted only to routers in the same area.

The DNA state must be set to *off* before changing the *type*.

Example:

```
set executor state on
```

```
set executor maximum broadcast routers 10
```

module access-control *circuit-specifier argument*

(**define** only) Defines access control lists, which are used to restrict the forwarding of packets between certain origins and destinations. Each access list is associated with one circuit, and applies to DECnet Long Format Data Packets received on that circuit. Access control does not apply to any routing or hello packets.

The arguments for the circuit-specifiers include the following:

all circuits
Specifies all circuits on the router.

circuit name
Specifies the named circuit.

known circuits
Specifies all circuits on the router.

The following items are the arguments you select from after you enter the **define module access-control** command and the circuit-specifier:

state on
Enables the access control list on this circuit.

state off
Disables the access control list on this circuit.

type exclusive
Specifies that any packets matching one or more of the filters in the access control list for this interface will be dropped.

type inclusive
Specifies that only packets matching one or more of the filters in the access control list for this interface will be forwarded.

filter [source-result source-mask dest-result dest-mask]
Adds a filter to the list for the specified circuit. The filter is added to the end of the existing list.

The source address is masked with the source-mask, and compared to the source-result. The same is done with the dest-mask and dest-result. The action depends on what type of access control is in use on the circuit.

The following items are the options you select from after you enter the **define module access-control** command and the **filter** circuit-specifier:

source-result
Address that the source address is compared to after masking.

source-mask
Mask used for the source address.

dest-result
Address that the destination address is compared to after masking.

dest-mask
Mask used for the destination address.

Example: `define module access-control circuit eth/0 state on`

module routing-filter *circuit-specifier argument*

(**define** only) Defines routing filters, which are used to restrict the sending of Area routes by level 2 (Executor Type Area) routers.

all circuits
Specifies all circuits on the router.

circuit name
Specifies the named circuit.

known circuits
Specifies all circuits on the router.

The following items are the direction options you select from after you enter the **define module routing-filter** command and the circuit-specifier:

incoming
Affects the filter on routing information received on this circuit.

outgoing
Affects the filter on routing information sent on this circuit.

The following items are the arguments you select from after you enter the **define module routing-filter** command and the circuit-specifier:

area [area-list]
Specifies that the filter allows routing information to pass for the set of areas in the area-list. The area-list is a comma-separated list of areas or ranges of areas. A range is specified by two area numbers separated by a dash. The area-list can also be none, specifying that information will be passed on no areas. The following are area-list examples:

1,4,9,60
Areas 1, 4, 9, and 60

1-7,9-13,23
Areas 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, and 23

state on
Specifies that the filter is active.

state off
Specifies that the filter is disabled, but continues to be stored in the permanent database. The only way to remove the filter is by using the **purge** command.

Example: `define module routing-filter circuit eth/0 state on`

node *argument*

Allows defining or setting configuring information on nodes into the volatile (**set**) or permanent (**define**) database. The only node for which any information is kept is the executor node, because node names are not stored. The node specifies the router's (executor's) node address. See the **define executor** command description.

Example: `define node state on`

Example: `set node state on`

Purge

Use the purge command to remove access control lists and routing filters from the permanent database.

Syntax:

purge	module access-control . . .
	module routing-filter . .

module access-control *circuit-specifier*
Removes access control lists from the permanent database. You can delete an entire access control list; you cannot delete one filter.

all circuits
Specifies all circuits on the router.

circuit name
Specifies the named circuit.

Example: `purge module access-control all circuits`

module routing-filter *circuit-specifier*
Removes routing filters from the permanent database. You can purge a specified filter or you can purge them all.

The options for the circuit-specifiers include the following:

all Specifies all routing filters in the configuration memory.

circuit name
Specifies the routing filter for the named circuit.

Example: `purge module routing-filter all`

Set

Use the **set** command to add, set, or modify circuit specifiers, global arguments, data link modules, or nodes in the volatile DNA database.

Syntax:

set	circuit . . .
	executor . . .
	node . . .

For a description of the options for these arguments, see “Define/Set” on page 308.

Show

Use the show command to show the status of the volatile database and volatile nodes in the routing database.

Syntax:

show	area-specifier . . .
	node-specifier . . .

area-specifier *argument*
Examines the status of the volatile area routing database. This lets you find out what areas are reachable, and what the routes are to various areas.

The options for the area-specifiers include the following:

active areas
Provides information on those areas which are currently reachable.

all areas
Provides information on all areas (up to the executor maximum area).

area Provides information on the specified area. If the area is not provided, you will be prompted for it.

known areas
Provides information on those areas which are currently reachable.

The following items are the subcommand options you select from after you enter the **show** command and the area specifier:

characteristics
Shows the current state of the specified area. (The same as summary.)

status Provides detailed information on the specified areas, including cost and hops.

summary
Shows the current state of the specified areas. This is the default.

Example.:

show active areas

```
Active Area Volatile Summary
Area State       Circuit Next
                         Node
1    reachable    Eth/0  1.22
2    reachable           2.26
3    reachable    X25/0  2.30
```

Example:

show active areas status

```
Active Area Volatile Status
Area State       Cost Hops Circuit Next
                                   Node
1    reachable   3    1     Eth/0  1.22
2    reachable   0    0            2.26
3    reachable   2    1     PPP/0  3.9
6    reachable   12   3     PPP/0  3.9
3    reachable   11   1     X25/0  2.30

Area Volatile Status
Area State       Cost Hops Circuit Next
                                   Node
5    unreachable 1023  31
```

The following items define the information displayed when you use the **show** command.

area Indicates the area for this line of the display.

circuit Indicates which circuit the next hop to this node will go over. No circuit is given for the router’s own area.

cost Indicates the cost to this area.

hops Indicates the hops to this area.

next node
Indicates the router that will be the next hop (intermediate destination) to the specified area.

state Indicates that this will be reachable or unreachable.

node-specifier *argument*
Shows the status of the volatile node routing database; this includes information on the reachable nodes and the routes to them.

The node-specifiers can be any of the following:

active nodes
Provides information on all nodes that are currently reachable.

all nodes
Provides information on all nodes (up to the executor maximum address). An all nodes display includes information on the "pseudo-mode" area.0. A route to node area.0 is advertised by any level two router which reaches other areas. Level one routers use these routes to forward all packets to the nearest level one router that knows how to get that packet to the correct area. There is no other way to examine node 0, because it is not a legal node address.

node node
Provides information on the specified node. If the node is not provided, you will be prompted.

known nodes
Provides information on those nodes which are currently reachable.

The arguments include the following:

characteristics/ summary
Both subcommand options show the current state of the specified nodes.

status Provides detailed information on the specified nodes, including cost and hops.

Example:
show node status

This example shows the detailed status of a specific node.

```
Which node [1.9]? 2.26
Node Volatile Status
Executor node            = 2.26 (gato)
State                    = on
Physical address         = AA-00-04-00-1A-08
Type                     = DEC-area
```

Example:
show active nodes

This example shows the reachable nodes.

```
Active Node Volatile Summary
Executor node            = 2.26 (gato)
State                    = on
Identification           = DECnet-MC68360 V1 R2.0 NP00523 [P10]

Node    State       Circuit Next
Address                     Node
2.14   reachable    Eth/0  2.14
2.34   reachable    PPP/0  2.34
2.37   reachable    PPP/0  2.34
1.22   reachable    Eth/0  1.22
```

Example:
show adjacent nodes status

This example shows the detailed routing information on all adjacent nodes. Only nodes with one hop will be shown. The node type is known and displayed for adjacent nodes only since this information is contained in hello messages only.

```
Adjacent Node Volatile Status

Executor node            = 2.26 (gato)
State                    = on
Physical address         = AA-00-04-00-1A-08
Type                     = DEC-area
Node    State       Type       Cost  Hops Circuit  Next
Addr                                                Node
2.14  reachable  routing IV     3    1    Eth/0   2.14
2.34  reachable  routing IV     2    1    PPP/0   2.34
2.42  reachable  nonrouting IV  2    1    PPP/0   2.42
1.22  reachable  area           3    1    Eth/0   1.22
```

Show/List

Use the **show circuit** command to retrieve information on the current state of the specified circuits from the volatile database. The **list circuit** command retrieves the data that is stored in the permanent data base for circuits.

Syntax:

show
- all
- area
- circuit . . .
- executor . . .
- known *argument*
- module *argument*
- node *argument*

Syntax:

list
- all
- area
- circuit *argument*
- executor *argument*
- module
- node *argument*

circuit-specifier *argument*
Where the circuit-specifiers options are the following:

active circuits
Specifies all circuits that are currently on (per the volatile database).

all circuits
Specifies all circuits on the router.

circuit name
Specifies the named circuit.

known circuits
Specifies all circuits on the router.

The following items are the subcommand options you select from after you enter the command and the circuit specifier:

characteristics
Provides detailed information on all of the argument settings for the circuit.

counters
Shows counters for the circuit.

status Shows detailed information on the circuit from the volatile database.

summary
Shows summary information on the circuit from the volatile database. This is the default if no argument is supplied.

Example:
show all circuits

```
Circuit Volatile Summary

Circuit State       Adjacent
                      Node

X25/0   on           5.25
Eth/0   on           1.22
Eth/0                2.14
Eth/0                1.13
PPP/0   off
```

Example:
list circuit eth/0 characteristics

```
Circuit Permanent Characteristics

Circuit           = Eth/0

State             = On
Cost              = 4
Router priority   = 64
Hello timer       = 15
Maximum routers   = 16
Router type       = Standard
```

Example:
show active circuits status

```
Active Circuit Volatile Status

Circuit State      Adjacent   Block
                     Node     Size

Eth/0   on           1.22     1498
Eth/0                2.14     1498
Eth/0                1.13     1498
X25/0   on           5.25     1498
```

Example:
show all circuits characteristics

This example shows the current characteristics of the circuits on this machine. This includes all of the configuration arguments, as well as the current adjacencies, and the Listen timer (three times the adjacency's hello timer).

```
Circuit Volatile Characteristics

Circuit           = Eth/0

State             = on
Designated router  = 2.26
Cost              = 4
Router priority   = 64
Hello timer       = 15
Maximum routers   = 16
Adjacent node     = 1.22
  Listen timer    = 45
Adjacent node     = 2.14
  Listen timer    = 45
Adjacent node     = 2.39
  Listen timer    = 90

Circuit           = PPP/0

State             = off
Designated router  =
Cost              = 4
Router priority   = 64
Hello timer       = 15
Maximum routers   = 8
```

Example:

```
show circuit eth/0 counters
```

This example shows the counters that are kept for the circuits. Note that some counters kept by DECnet-VAX are not kept here, but are instead read through the **network** command of GWCON.

```
Circuit Volatile Counters

Circuit = Eth/0

525249  Seconds since last zeroed
     0  Terminating packets received
     0  Originating packets sent
  3693  Transit packets received
  4723  Transit packets sent
     0  Transit congestion loss
     0  Circuit down
     0  Initialization failure
     0  Packet corruption loss
```

adjacent node
Node ID of a node that has an adjacency with this node on the circuit being displayed. While adjacencies with end-nodes automatically make that node reachable, a router adjacency does not automatically make that node reachable. A router is not considered reachable unless a routing message has been received over an active adjacency from that router. Thus, nodes may show as adjacent in the circuit database, but will not be in the reachable nodes database (show active nodes).

block size
Maximum data block size that the associated adjacent node is willing to receive. This is typically 1498 bytes, which is the standard 1500 bytes of an Ethernet packet, less the 2-byte length field used with DECnet.

circuit Circuits to which this data applies.

designated router
Displays what this node believes to be the designated router for this area on this circuit. (There may be some transient disagreements when a new router starts up.) This normally will be the same for all routers on the circuit. End-nodes send all packets for destinations not on the local circuit to their designated router.

hello timer
Hello timer for this circuit. Router hello messages are sent this often on the circuit.

listen timer
Amount of time designating how often router or end-node hellos must be received from this adjacency on this circuit. It is three times the hello timer set for this circuit on the adjacent machine.

router priority
Router priority for this circuit, used in vying for designated router status.

router type
Router type for this circuit - standard, phase IV with AMA, or Bilingual.

maximum routers
Maximum number of routers allowed on this circuit.

state Either ON or OFF. In the volatile database, the state will be ON if the circuit is enabled, and is passing self-test. If the circuit has failed self-test, or the device is not present, the state will be OFF.

In the permanent database, this tells if DNA will try to enable the circuit.

executor *argument*

Retrieves information on the current state of the volatile database for DNA with the show executor command. The **list executor** command retrieves the data which is stored in the permanent data base for DNA.

The following lists the subcommand options or arguments you select from after you enter the show/list executor command:

characteristics

The detailed information on the settings of all of the adjustable arguments of the routing database.

counters

Gives the global event and error counters for DNA. There are no permanent counters, so the **list executor counters** command is irrelevant.

status Gives key information on the state of DNA.

summary

Gives a brief summary on the state of DNA. This is the default.

Example:

show executor

```
Node Volatile Summary
Executor node            = 2.26 (gato)
State                    = on
Identification           = DECnet-MC68360 V1 R2.0 NP00523 [P10]
```

Example:

show executor characteristics

This example shows the full configuration of the router's database. The **list executor characteristics** command produces essentially the same display.

```
Node Volatile Characteristics
Executor node            = 2.26 (gato)
State                    = on
Identification           = DECnet-MC68360 V1 R2.0 NP00523 [P10]
Physical address         = AA-00-04-00-1A-08
Type                     = DEC-area
Routing version          = V2.0.0
Broadcast routing timer  = 180
Maximum address          = 64
Maximum cost             = 1022
Maximum hops             = 30
Maximum visits           = 63
Maximum area             = 63
Max broadcast nonrouters = 64
Max broadcast routers    = 32
Area maximum cost        = 1022
Area maximum hops        = 30
Maximum buffers          = 103
Buffer size              = 2038
```

Example:

list executor status

This example shows the status of the router in the permanent database:

```
Node Permanent Status
Executor node            = 2.26 (gato)
State                    = on
Type                     = DEC-area
```

Example:

show executor counters

This example shows the counters that DNA keeps.

```
Node Volatile Counters
Executor node           = 2.26 (gato)
525948  Seconds since last zeroed
     0  Aged packet loss
     0  Node unreachable packet loss
     0  Node out-of-range packet loss
     0  Oversized packet loss
     0  Packet format error
     0  Partial routing update loss
     0  Verification reject
```

The following items define the fields that are displayed when you use the **show/list executor** command.

area maximum cost
Maximum allowed cost to an area.

area maximum hops
Maximum allowed hops to an area.

broadcast routing timer
Frequency of sending routing messages in the absence of any changes.

buffer size
Buffer size for the router.

executor node
Node address and node name. The node name is the name set by the CONFIG **set hostname** command.

identification
Identification of the router software, as sent in MOP System ID messages.

maximum area
Highest area to which routes are kept.

maximum broadcast nonrouters
Maximum number of end-nodes that can be adjacent to this router.

maximum broadcast routers
Maximum number of routers that can be adjacent to this router.

maximum buffers
Number of packet buffers in the router.

maximum cost
Maximum allowed cost to a node.

maximum hops
Maximum allowed hops to a node.

maximum visits
Maximum number of routers a packet may be routed through between source and destination.

physical address
Physical Ethernet address set on all Ethernet circuits when DNA starts. Derived from the node ID.

routing version
Version is always Version 2.0.0.

state The state of DNA, on or off.

type Either ROUTING IV or AREA, corresponding to level 1 and level 2.

module access-control circuit-specifier *argument*

Lists the DECnet access control lists that have been defined in the permanent database for the router, as well as the counters of their use. The options for the circuit-specifiers include the following:

all circuits
Specifies all circuits on the router.

circuit [name]
Specifies the named circuit.

known circuits
Specifies all circuits on the router.

The following items are the arguments you select from after you enter the **show/list module access-control** command and the circuit-specifier:

counters
Gives counters on the use of the access control lists.

status Shows detailed information on the access control lists, including the filters in the access control list.

summary
Shows summary information on the state of the access control lists. This is the default.

Example:
`show module access-control circuit eth/0 counters`

Example:
`list module access-control circuit eth/0 counters`

```
Module Access-Control Volatile Counters

Circuit = Eth/0

6337         Seconds since last zeroed
   0         Packets processed
   0         Packets rejected
   0         Access control loop iterations
```

module routing-filter circuit-specifier *argument*

Lists the DECnet area routing filters that have been defined in the permanent database for the router.

all circuits
Specifies all circuits on the router.

circuit [name]
Specifies the named circuit.

known circuits
Specifies all circuits on the router.

The following items are the arguments you select from after you enter the **show/list module routing-filter** command and the circuit-specifier:

status Shows detailed information on the routing filters, including the area list.

summary
Shows summary information on the state of the routing filters. This is the default.

Example: **`show module routing-filter circuit eth/0 status`**

Example: `list module routing-filter circuit eth/0 status`

Zero

Use the **zero** command to clear circuit counters in the volatile database, global counters in the volatile database, and counters in the access control list module.

Syntax:

zero	circuit-specifier
	executor
	module access-control circuit-specifier

circuit-specifier

all circuits
Specifies all circuits on the router.

circuit [name]
Specifies the named circuit.

known circuits
Specifies all circuits on the router.

Example: `zero all circuits`

executor
Sets all global counters in the volatile database to a zero value. There are no options.

Example: `zero executor`

module access-control circuit-specifier

all circuits
Specifies all circuits on the router.

circuit [name]
Specifies the named circuit.

Example: `zero module access-control all circuits`

Chapter 10. Using OSI/DECnet V

This chapter describes the router's implementation of the International Standards Organization's (ISO) Open Systems Interconnection (OSI) Connectionless Network Layer. DECnet Phase V supports OSI (hereafter called DECnet V/OSI) and users of DNA V networks can use this chapter for information about the ISO OSI protocols.

This chapter contains the following sections:

OSI Overview

An OSI network consists of interconnected subnetworks. A subnetwork consists of connected hosts referred to as end systems (ESs) and routers referred to as intermediate systems (ISs), as shown in Figure 19.

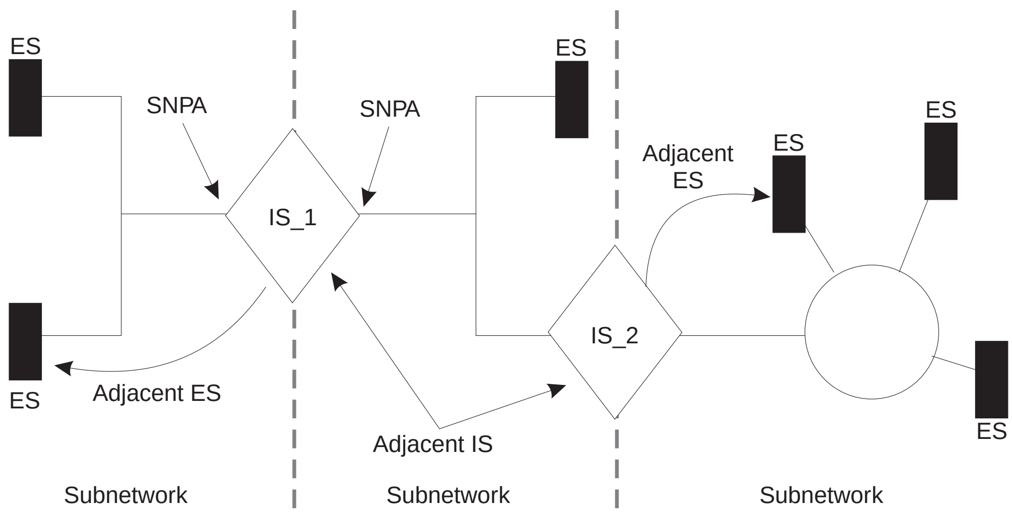


Figure 19. OSI Network

ESs contain all the layers of the OSI reference model and contain the host applications. ISs perform the functions of the lower three layers of the OSI reference model and handle the routing of the network protocol data units (NPDUs) between subnetworks. ISs logically attach to the subnetwork at the subnetwork point of attachment (SNPA). The SNPA is the access point into the data link layer.

Depending on the IS configuration, each IS can run three protocols: ES-IS, IS-IS, and Connectionless-Mode Network Protocol (CLNP).

The ES-IS protocol enables the ESs and ISs attached to the same subnetwork to dynamically discover each other's existence. An ES connected to the same subnetwork as an IS is adjacent to the IS. The IS-IS routing protocol enables the ISs to do the following:

- Dynamically discover the existence and availability of adjacent ISs.
- Exchange routing information with other ISs.
- Use the exchanged routing information to calculate routes based on the shortest path.

The CLNP protocol is a datagram protocol that transports packets between ISs.

NSAP Addressing

The NPDU contains OSI network addresses (also called NSAPs). The NSAP refers to a point at the network layer where the user accesses the network layer. NSAPs are unique points within a system that represent addressable endpoints of communication through the network layer. The number of NSAPs may vary from system to system.

An addressing authority, such as the United States government's National Institute of Standards and Technology (NIST), administers NSAP addresses and determines how the addresses are assigned and interpreted within their domain. If desirable, these authorities may further partition the domain into subdomains and designate corresponding authorities to administer them.

There are two NSAP addresses within the NPDU, a destination address and a source address. Each address can vary in length from 2 octets to 20 octets and is usually represented in hexadecimal notation. The following is an example of a 6-octet NSAP that can be entered in the OSI configuration of the router.

```
AA000400080C
```

Because the address length is variable, portions of the PDU header called Destination Address Length Indicator and Source Address Length Indicator are used to indicate the length, in octets, of each address.

An NSAP address consists of two parts, an Initial Domain Part (IDP) and a Domain Specific Part (DSP) as shown in Figure 20.

<table>
<tr><td colspan="2">IDP</td><td rowspan="2">DSP</td></tr>
<tr><td>AFI</td><td>IDI</td></tr>
</table>

Figure 20. NSAP Address Structure

IDP

The IDP consists of two parts, the Authority and Format Identifier (AFI) and the Initial Domain Identifier (IDI).

The AFI specifies the type of IDI and the network addressing authority responsible for allocating the values of the IDI.

The IDI specifies both the network addressing domain from which the values of the DSP are allocated and the network addressing authority responsible for allocating values of the DSP from that domain.

DSP

The network addressing authority identified by the IDI determines the DSP. However, what is important is that the DSP includes specific addressing information for the domain.

IS-IS Addressing Format

The IS-IS protocol divides the NSAP address into three portions; area address, system ID, and selector (see Figure 21). The area address and system ID, together with a selector of 0, are referred to as the Network Entity Title (NET). A NET is the address of the network layer itself and is assigned when you configure an IS into the OSI network.

<table>
<tr><td>IDP</td><td colspan="3">DSP</td></tr>
<tr><td colspan="2">Area Address</td><td>System ID</td><td>Selector</td></tr>
</table>

Figure 21. IS-IS NSAP Addressing Interpretation

Area Address

In the IS-IS protocol, the area address is that portion of the NSAP that includes all or a portion of the IDP and the portion of the DSP up to the system ID.

The area address is that portion of the NSAP that identifies a specific area within a domain. This address must be at least 1 octet long and all ESs and ISs in the same area must have the same area address.

System ID

The system ID is that portion of the NSAP that identifies a specific system within an area. System IDs must have the following attributes:

- 1 octet to 8 octets in length.
- Equal length throughout the domain. The routers use a default configuration length of 6 octets.
- Unique for each system throughout the domain.

Selector

The selector is a 1-octet field that acts as a selector for the entity that is to receive the PDU, for example, the transport layer or the IS network layer itself. The router sets this field to 0.

GOSIP Version 2 NSAPs

Government Open Systems Interconnection Profile (GOSIP) Version 2 provides for government use the NSAP addressing format illustrated in Figure 22 on page 330. The authorities responsible for the address have clearly defined the fields and specified the addressing format under the DSP set by the National Institute of Standards and Technology (NIST).

IDP		DSP						
AFI 47	IDI 0005	Ver 80	Auth.	Reserved	Domain (2)	Area (2)	Sys. ID (6)	Selector (1)

Figure 22. GOSIP Address Format

AFI This 1-octet field has a 47 (hexadecimal) designation. This value signifies that the address is based on the ICD format and that the DSP uses a binary syntax.

IDI This 2-octet field has a 0005 (hexadecimal) designation. This value is assigned to the U.S. Government and the format has been established by NIST.

VER This 1-octet field has designation of 80 (hexadecimal). This value identifies the DSP format.

Auth. (Authority)
This 3-octet field identifies the authority that controls the distribution of the NSAP addresses.

Reserved
This 2-octet field is provided to accommodate future growth.

Domain
This 2-octet field contains the routing domain identifier.

Area This 2-octet field contains the area ID.

Sys. ID
This 6-octet field identifies the system.

Selector
This 1-octet field selects the entity to receive the NPDU.

Multicast Addresses

Multicast addressing is the method that level 1 (L1) and level 2 (L2) ISs use to distribute link-state updates (LSUs) and hello messages to other systems or LANs. When an LSU or a hello message is multicast, a group of destination stations receive the packet. For example, an L1 LSU is multicast only to other L1 ISs. An Intermediate System Hello (ISH) is multicast only to ESs on the same subnetwork.

You can configure multicast addresses for each subnet with the **set subnet** command. Table 103 lists the multicast addresses for Ethernet, and Token-Ring.

Table 103. IS-IS Multicast Addresses

Destination	Ethernet 802.3	Token-Ring 802.5	Address Description	
All ESs	09002B000004	C00000004000	9000D4000020	For all end systems on the subnetwork.
All ISs	09002B000005	C00000008000	9000D40000A0	For all intermediate systems on the subnetwork.
All L2 ISs	0180C2000015	C00000008000	800143000028	For all L2 intermediate systems on the subnetwork.

Table 103. IS-IS Multicast Addresses (continued)

Destination	Ethernet 802.3	Token-Ring 802.5	Address	Description
All L1 ISs	0180C2000014	C00000008000	8001430000A8	For all L1 intermediate systems on the subnetwork.

OSI Routing

OSI routes packets using the IS-IS protocol. Routing with the IS-IS protocol is based on:
- A system ID for routing within an area
- An area address for routing within a domain
- The reachable address prefix for routing outside the domain

The IS-IS protocol uses routing tables to forward packets to their correct destinations. The routing table entries are built from information in the link state database or from user-configured reachable addresses. The link state database is built from information received in the link state update (LSU). Refer to the “Link State Databases” on page 335.

IS-IS Protocol

The IS-IS protocol is a link state dynamic routing protocol that detects and learns the best routes to reachable destinations. IS-IS can quickly perceive changes in the topology of a domain, and after a short convergence period, calculate new routes. To accomplish this, the IS uses the following packets:
- Link State Updates (LSU) that the IS uses to keep the link state database information current.
- Sequence Number PDU (SNP) to keep the database synchronized and to ensure that each adjacent IS knows what the most recent Link State Packet (LSP) from each other router was.
- Hello messages that ISs use to discover, initialize, and maintain adjacencies with neighboring ISs.

IS-IS Areas

An IS-IS area is a collection of systems on contiguous subnetworks. Each area’s topology is hidden from those of the other areas to reduce routing traffic. A level 1 (L1) IS is used to route within an area. A level 2 (L2) IS is used to route between areas or over the backbone. An IS that routes within an area and over the backbone is considered an L1/L2 IS.

IS-IS Domain

An IS-IS domain is a set of rules, administered by the same authority, that all ESs and ISs must follow to ensure compatibility. There are two types of domains that require discussion, administrative domain and routing domain.

Administrative Domain

An administrative domain controls the organization of ISs into routing domains as well as the NSAP and subnetwork addresses that those routing domains use.

Routing Domain

A routing domain is a set of ISs and ESs governed by the following rules:
- All devices use the same type of routing metric.
- All devices use the same routing protocol, such as IS-IS.

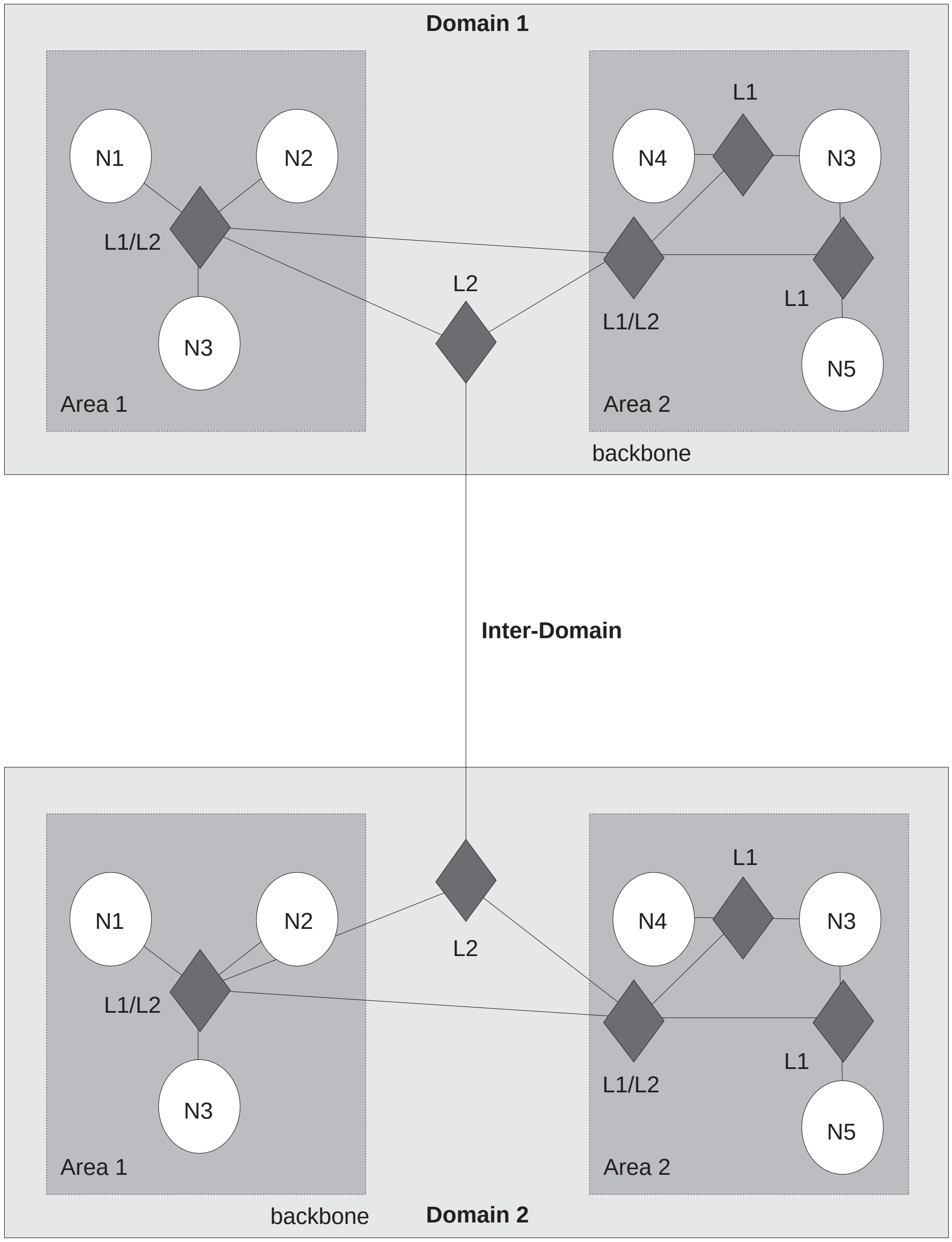


Figure 23. OSI Domain

Synonymous Areas

When an L1 IS services more than one area, these additional areas are called synonymous areas. A router can support any number of synonymous areas, as long as there is an overlap of at least one area address between adjacent routers. For example, in Figure 24 on page 333, Area 1 and Area 2 are synonymous areas to each other and Areas 3 and 4 are also synonymous to each other.

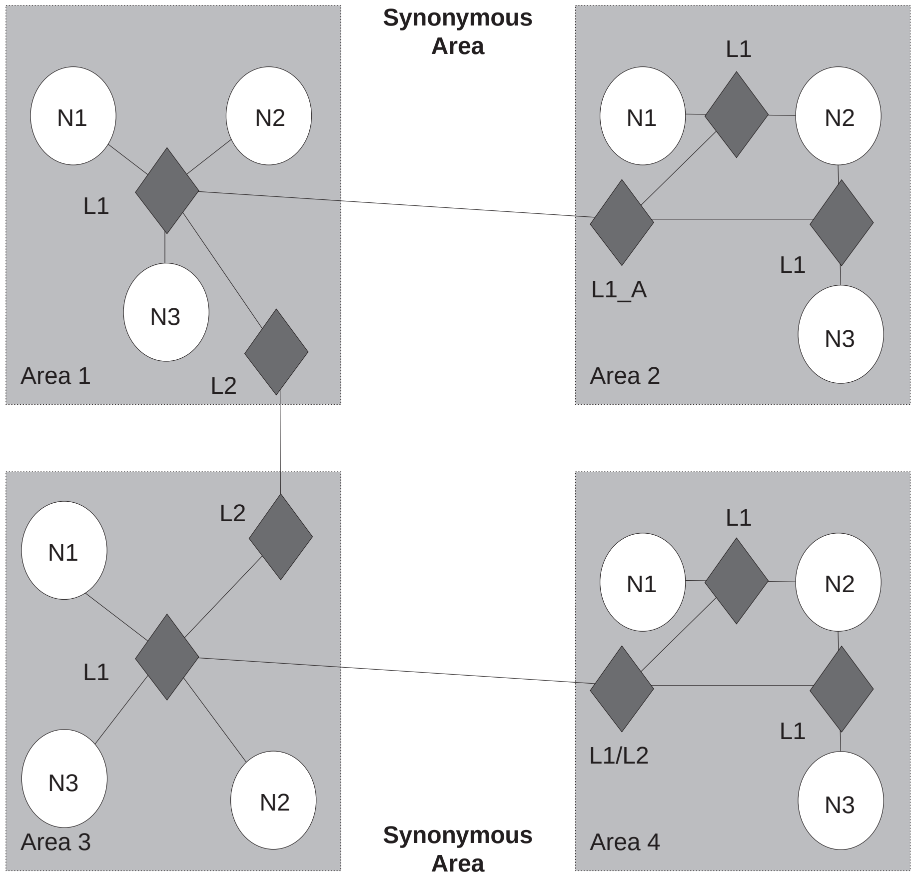


Figure 24. Synonymous Areas

L1_A IS in area 2 must have area 1's address added to its configuration and the L1 IS in area 1 must have area 2's address added to its configuration. For areas 3 and 4 to be synonymous, each area's address must be added to the others L1 IS.

IS to IS Hello (IIH) Message

The IIH message enables an IS to determine the existence of other ISs and to establish adjacencies. There are three types of IIH messages: L1, L2, and point-to-point.

Each IS contains a local hello timer and holding timer. Each time the hello timer expires, an IIH is multicast over the IS's interface to any adjacent ISs. When the hello message is received, the recipient establishes or updates (refreshes) the adjacency information. This information remains current for amount of time (seconds) specified by the holding timer. If the holding timer expires, the adjacency is brought down.

L1 IIH Message

The L1 IIH message is multicast over the interface when its local hello timer expires. The L1 IS places the following information in its IIH:
- Source ID
- Any manual area addresses that it services
- IS type (L1 only, or L1/L2)
- Priority
- LAN ID

- If applicable, the system ID of the L1 designated IS (pseudonode)

Upon receiving this message, the adjacent L1 IS extracts the source ID of the sending IS. This IS then constructs its own IIH message and places its source ID into the source ID field. The sender's source ID is placed into the IS neighbors field. Returning the sender's ID verifies to the sender that the adjacent IS is aware that it exists (2-way adjacency).

When the first IS receives the IIH, it too extracts the source ID and looks at the IS neighbor field. Upon discovering its own source ID in the IS neighbor field, this IS establishes an adjacency with the other IS.

Note: Before the adjacent L1 IS can accept the packet, the packet must have a common area address and the same system ID length as the adjacent IS.

L2 IIH Message

The L2 IIH is multicast over its interfaces for purpose of identifying itself to other L2 ISs. The L2 IS has the same function as an L1 IIH. The L2 IS places the following information in its IIH:

- Source ID
- Any manual area addresses that it services
- IS type (L2 only or L1/L2)
- Priority
- LAN ID
- If applicable, the system ID of the L2 designated IS

Note: Before the adjacent L2 IS can accept the packet, the packet must have the same system ID length as the adjacent IS.

Point-to-Point IIH Message

A point-to-point IIH message is sent out over an IS's non-broadcast interface (Frame Relay or X.25) to identify itself to other ISs. This IS gives the IIH to contain the following information:

- Source ID
- Any manual area addresses that it services
- IS type (L1 only, L2 only, or L1/L2)
- Local circuit ID

Designated IS

A designated IS is selected among all ISs connected to the same LAN to perform additional duties. In particular it generates link state updates on behalf of the LAN, treating the LAN as a pseudonode. A pseudonode is a method of modeling the entire LAN as a node on the network with fewer logical links. Minimizing logical links throughout the domain lessens the computational complexity of the link-state algorithm.

When more than one IS exists on a LAN, each IS compares the following to determine which IS will become the designated IS:

- All ISs compare their priorities. The IS with the highest priority becomes the designated IS.
- If the ISs have the same priority, they compare their source MAC addresses. The IS with the numerically highest MAC address becomes the designated IS for that LAN and is indicated through the LAN ID.

Link State Databases

Each L1 and L2 IS contains a link state database. The primary element of the database is the link state update (LSU). The router is responsible for building its own LSU and processing other ISs' LSUs to maintain the database. The L1 database contains information on ESs. Each L1 database is identical for all L1 ISs in the same area. The L2 database contains information on areas and reachable addresses. Each L2 database is identical for all L2 ISs configured in the IS-IS domain. With information from the databases, the Dijkstra routing algorithm calculates the shortest paths to all destinations and builds the routing tables.

Link State Flooding

To ensure that each L1 and L2 IS maintains an identical database, LSUs are flooded throughout an area or a backbone. Flooding is a mechanism that an L1 or L2 IS uses to propagate an LSU to all L1 or L2 ISs. An L1 IS floods LSUs to L1 ISs only. An L2 IS floods LSUs to L2 ISs only. An L1/L2 IS accepts both L1 and L2 LSUs.

L1 Link State Update (non-pseudonode)

The L1 LSU is flooded to all L1 ISs. The L1 IS gives the LSU the following information:

- Source ID
- Any manual area addresses that it services
- IS type (L1)
- System IDs and costs of reaching IS adjacencies
- If applicable, the system IDs adjacent pseudonodes
- System IDs for any manual ES adjacencies

L1 Link State Update (pseudonode)

The L1 pseudonode LSU is flooded to all L1 ISs located in the area. Any L1 IS located on the same LAN that receives the LSU propagates the LSU to all L1 ISs adjacent on all of its other subnetworks. The L1 IS places the following information in its LSU:

- Source ID
- IS type (L1)
- System IDs and cost of reaching all non-pseudonode ISs located on the LAN
- System IDs for any ES adjacencies learned through the ES-IS protocol

L2 Link State Update (non-pseudonode)

The L2 LSU is flooded to all L2 ISs. The L2 IS places the following information in its LSU:

- Source ID
- Set of area addresses that it services
- IS type (L2)
- System IDs and the cost of reaching IS adjacencies
- If applicable, the system ID of the pseudonode
- Address prefixes for ISs located in an external domain

L2 Link State Update (pseudonode)

The L2 pseudonode LSU is multicast over the interface and propagated to all L2 ISs located outside the subnetwork. Any L2 non-pseudonode IS located on the same subnetwork that receives the LSU relays the LSU to all L2s located outside the subnetwork. The L2 IS places the following information in its LSU:

- Source ID
- IS type (L2)
- System IDs and metrics for non-pseudonode ISs located on the same subnetwork

Attached and Unattached L2 IS

An attached L2 IS is a router that knows of other areas. An unattached L2 IS is a router that does not know of any areas other than its own.

When routing, an unattached L2 IS routes packets to the closest attached L2 IS.

Routing Tables

An L1-only IS uses one routing table, the level 1 routing table. An L2-only IS contains three routing tables: an L2 area-address routing table, an L2 internal-metric reachable-address-prefix routing table, and an L2 external-metric reachable-address-prefix routing table. An L1/L2 IS contains the L1 routing table and all L2 routing tables. The routing table entries are built from information in the link state database.

L1 Routing

The following summarizes L1 routing:

1. An L1 IS receives a packet and compares the area address portion of the destination address in the header of the packet to the set of area addresses in the router.
2. If the packet is destined for the router’s area, the router extracts the system ID from the address. Searching for a match, the router compares the system ID to the system IDs in the L1 routing table.
3. If a match occurs, the IS routes the packet to the ES or the next hop IS. If no match occurs, the packet is dropped.
4. If the packet is not destined for this area, the L1 forwards the packet to the nearest L2 IS or if this router is an L1/L2 IS, it checks its L2 routing tables as described in the next section. If the L1 cannot determine where to route the packet, the packet is dropped.

L2 Routing

An L2 IS contains three routing tables: an L2 area-address routing table, an internal-metric reachable-address-prefix table (internal), and an external-metric reachable-address-prefix table (external).

The following summarizes L2 routing:

1. An L2 IS receives a packet and compares the destination address in the header of the packet to the set of area addresses in the area address routing table. If a match exists, the packet is forwarded to the next hop backbone router. If no match exists, the router checks the internal routing table.
2. The internal routing table contains entries of reachable address prefixes that lead to other domains. If the internal routing table contains a match, the packet is forwarded along the backbone to the appropriate domain. If no match exists, the router checks the external routing table.
3. The external routing table contains entries to reachable address prefixes that also lead to other domains. If the external routing table contains a match, the packet is forwarded along the path to the appropriate domain. If no match exists, the packet is dropped.

Refer to “Internal and External Routing” on page 337 for a detailed explanation of the internal and external routing tables.

Routing Metric

A routing metric is a value associated with a function of the circuit to indicate the cost of routing over that circuit. For example, the routing metric based on the monetary expense of a circuit would use a low number to indicate a low monetary expense and high number to indicate a high monetary expense of routing a packet over that circuit.

The IS-IS routing protocol uses four routing metrics: default metric, delay metric, expense metric, and an error metric.

The current implementation of the OSI protocol uses the IS-IS default metric only. The default metric, by convention, is intended to measure the circuit's capacity to handle traffic. All ISs in the routing domain must be capable of calculating routes based on the default metric. The other routing metrics are optional. Though they are not used by this implementation of the OSI protocol, they are described below for informational purposes only.

- The delay metric measures the transit delay of the associated circuit.
- The expense metric measures the monetary cost of utilizing the associated circuit.
- The error metric measures the residual error probability of the associated circuit.

Internal and External Routing

Internal or external routing involves an L2 IS routing a packet between two separate domains. When a packet needs to be routed to another domain, the L2 IS tries to match the address to a reachable address prefix in the internal or external routing table. Internal and external routes are based on the cost (routing metric) to the destination. An internal route's cost considers the cost of routing within the domain and the cost of routing to the destination. An external route's cost is based only on the cost of routing to the destination outside the routing domain. The IS chooses the path with the lowest cost.

For example, a packet is destined to go from node A in domain 1 to node D in domain 2 (Figure 25 on page 338). Node A can choose two paths to send the packet, to node B and then on to D or to node C and then on to D. How nodes B and C advertise the cost of their routes to D determines how node A decides to route the packet, internally or externally. There are three possible options:

- Nodes B and C advertise the cost of their routes to D as internal. The internal cost of the route A-B-D is 35 which is the cost of routing from A to B, plus the cost of routing from B to D. The internal cost of the route A-C-D is 40, which is the cost of routing from A to C, plus the cost of routing form C to D. Node A in this case would choose to route over the A-B-D path because the cost is lower.
- Nodes B and C advertise the cost of their routes as external. The external cost for A-B-D is 30 which is the cost of routing from B to D. The external cost for A-C-D is 20. Node A in this case would choose to route over the A-C-D path because the cost of this route is lower.
- Nodes B and C advertise the cost of their routes as both internal and external. The internal and external cost of the routes are added to their respective routing tables. Because internal routes are preferred over external routes, the router chooses the internal route of A-B-D.

Note: Because there is no exterior routing protocol, all prefix routes between domains must be statically configured.

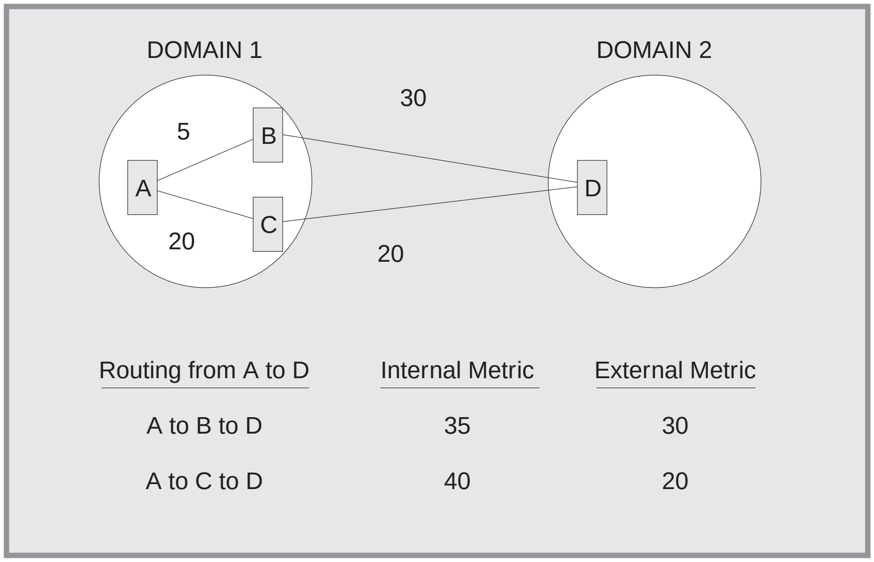


Figure 25. Internal and External Routing Metrics

Address Prefix Encoding

When entering address prefix routes into the router, carefully consider the difference between encoding rules for NSAPs and for prefix routes. The following four examples illustrate address prefix encoding.

Encoding a Fixed Length IDI

For many address prefixes, encoding the prefix and the corresponding NSAP is the same. For example, you are using a GOSIP 1.0 address and you want to create a route to an organization in the DoD. The Org IDI is 1234 and the DoD IDI is 0006. The encoded NSAP address is

```
4700061234CCCC222222222222
```

The encoded address prefix is a result of the truncation of the NSAP

```
4700061234
```

The encoding rules are about all NSAP formats having a fixed length IDI and to any address prefix ending after the IDP.

Encoding an AFI

An address prefix based entirely on the AFI is encoded only on the 1 octet AFI field. For example, if an address prefix is needed for all X.121 format addresses (used on X.25 networks), you would use the X.121 AFI of 37.

Encoding a Variable Length IDI

NSAP addresses that have variable length IDI formats, such as X.121, F.69, E.163, and E.164, use a more complicated encoding scheme. When variable length IDIs are encoded as an NSAP, the address is left padded with zeros; however, when the IDI is encoded as an address prefix, there is no left padding.

For example, you want to route X.25 calls from the U.S. to an X.25 carrier in the Netherlands. The carrier has a Data Network Identifier Code (NDIC) of 2041. The encoding of the address prefix would be

```
372041
```

An X.25 subscriber having a national telephone number (NTN) of 117010 on this carrier would have an NSAP of

```
3700002041117010
```

Notice that the IDI of the NSAP is left padded with zeros to 14 digits because the resulting international data number (2041117010) was less than 14 digits.

If, however, you want an address prefix that points only to this one X.25 subscriber, the encoding would then be the NSAP (3700002041117010), because the prefix does not end in the IDP.

Default Address Prefixes

A default address prefix is used when you want to originate a default route to all addresses outside your domain. Default address prefixes are of zero length, so there is nothing to encode.

Authentication Passwords

To provide a minimum layer of security to the network, OSI provides the option of authentication passwords. When authentication is enabled, any IS-IS packet that does not contain the proper password is not accepted by the IS. The authentication field of the NPDU contains the authentication passwords. There are two types of authentication passwords, transmit and receive.

A transmit password is added to IS-IS packets transmitted by the IS. A receive password is a listing of the transmit passwords that the IS accepts. For example, with authentication enabled, if a transmit password is not added to the packet, or a listing of the transmit password is not in the receive password database, the packet is dropped. There are three types of transmit and receive passwords: domain, area, and circuit.

A domain password provides security for L2 routing information. An area password provides security for L1 routing information. A circuit password provides security for IS-IS hello messages.

ESIS Protocol

The ES-IS protocol enables ESs and ISs attached to the same subnetwork to dynamically discover each other’s existence and availability. This information also permits ESs to obtain information about each other without an available IS.

Route redirection information enables an IS to inform an ES of a better route when forwarding NPDUs to a particular destination. For example, a better route could be another IS on the same subnetwork as the ES, or the destination ES located on the same subnetwork.

Hello Message

Addressing information is passed on to ESs and ISs through hello messages.

A local configuration timer (CT) and a holding timer (HT) is present on each ES and IS. Each time the CT expires, a hello message is multicast on the LAN. When the hello message is received, the recipient sets its HT value according to the value transmitted in the HT field of the message. The recipient is expected to retain this information until the HT expires to ensure correct operation of the ES-IS protocol.

End System Hello (ESH) Message

The ESH message is multicast from the ES to all L1 ISs when its local CT expires. The ES constructs this message to inform an IS of any NSAPs that it serves. Upon receiving this message the IS extracts the NSAP and SNPA information and stores the pair in its L1 routing table, replacing any other information currently stored there.

Intermediate System Hello (ISH) Messages

The ISH message is multicast to all adjacent ESs when its local CT expires. The IS constructs this message to inform the ES of its NET. Upon receiving of this message, the ES extracts the NET and SNPA information and stores the pair in one of its local routing tables, replacing any other information currently stored there.

X.25 Circuits for DECnet V/OSI

For X.25 networks, the router establishes X.25 switched virtual circuits (SVCs) on routing circuits.

Note: To enable DECnet V/OSI for X.25, you must enter the DECnet IV process and define your router to be a DEC-AREA or DEC-ROUTING-IV router. You must do this (and restart the router!) to enable the commands to do the DECnet V/OSI configuration. Use the **define executor type** command.

Routing Circuits

Routing circuits are point-to-point connections between nodes that implement the ISO CLNS protocol. The router employs these types of routing circuits:
- Static incoming circuits
- Static outgoing circuits
- Dynamically assigned circuits

Static incoming and static outgoing circuits have only one SVC associated with them, and they carry both user data and non-user data (such as routing protocol messages). You bring static circuits up and down explicitly using DECnet V/OSI configuration commands. Dynamically assigned routing circuits are established upon data arrival and are cleared when there is no data being transmitted or received. A dynamically assigned circuit can have multiple SVCs, but can carry only user data.

DECnet V/OSI controls calls for each of the types of routing circuits by using *filters* and *templates*. Filters are used to process incoming calls; templates are used to establish outgoing calls.

Filters

A *filter* is a collection of user-configurable parameters that define the criteria for accepting all incoming calls for the specified X.25 routing circuit.

The parameters defined in a filter include the calling DTE address, a filter priority, and call/user data.

Filters and Routing Circuits

Incoming calls can be on a static incoming circuit or a dynamically assigned (DA) circuit. One or more filters may be defined for the same routing circuit. For example, a DA circuit can have multiple adjacencies and more than one filter may be defined for that routing circuit.

Filter Priorities

The list of filters for static incoming circuits and DA circuits are intermixed and ordered by descending priority. When an incoming call is received, the router searches the list of filters, highest priority first. To prevent a static circuit from being erroneously assigned to a DA circuit, it is recommended that the filters of all static circuits be assigned a higher priority than the filters of all DA circuits.

Filter Constraints on Calls

For a static incoming circuit, the filter should specify a particular calling DTE address, but the first octet of the call/user data must contain the ISO 8473 Protocol Discriminator (129). For correct operation of multiple DA circuits, additional constraints should be configured for each defined filter. This ensures that the selection criteria specified in those filters permit the required distinction to be made between incoming calls.

Note: If a DA circuit should incorrectly connect to a static circuit, the architecture makes no attempt to identify the condition or rectify the problem. The usual "initialization failure" may be generated on the static side due to non-response to its link initialization queries. The static SVC is then subsequently cleared.

Templates

A template is a collection of user configurable parameters for outgoing calls. It sets the parameters so that the circuit on the remote router accepts the incoming calls. The parameters defined in a template include the calling DTE address and the call/user data.

You can define only one template per outgoing static routing circuit.

Link Initialization

Link initialization is a procedure proprietary to Digital Equipment Corporation (and is not part of OSI). Link initialization immediately follows SVC establishment. It is used primarily to establish the DECnet relationship with a remote system on a point-to-point link.

On receipt of an Initialization/XID message, verification can be performed on two levels: on a circuit basis or on a system basis. Basically, the process of verification compares the incoming verification data against data specified locally either for the circuit or for the calling system. The verification data appears in the verification data field of the XID message.

Note: This release of the router software does not support verification by the system.

OSI/DECnet V Configuration

Note: When operating DNA IV networks together with DNA V networks, all DNA IV configuring and monitoring must be done from the DNA IV `NCP>` configuration process. For information on configuring DNA IV, refer to "Chapter 8. Using DNA IV" on page 291. The use of the term "OSI" in this chapter refers to both the OSI and DNA V environments unless indicated otherwise.

Basic Configuration Procedure

This section outlines the minimum configuration steps that you are required to perform to get the OSI/DNA V protocol up and running over a LAN (Ethernet or Token-Ring), X.25 packet switching networks, and Frame Relay. Before beginning any configuration procedure, use the **list device** command from the **config** process to list the interface numbers of the different devices. If you desire any further configuration command explanations, refer to the configuration commands described in this chapter.

Note: You must restart the router for new configuration changes to take effect.

Do the following basic configuration procedure before beginning the specialized procedures described in the following sections.

Setting the network entity title (NET)
Set the router's NET using the set **network-entity-title** command. The NET consists of the router's system ID and its area address. Use the **list globals** command to verify that the NET is configured correctly.

Globally enabling OSI
Enable the OSI software to run on the router using the **enable OSI** command. Use the **list globals** command to verify that the OSI protocol is enabled.

Configuring OSI Over an Ethernet or a Token-Ring LAN

To configure the OSI protocol to run over an Ethernet or over a Token-Ring LAN, set the subnet. There is a one-to-one correspondence between subnetworks and interfaces. Use the **set subnet** command to configure all LAN subnets (Ethernet, Token-Ring, or . Use the default multicast addresses for Ethernet. When configuring a token-ring, use these addresses:

Parameter
Functional Address 802.5

All ESs [09002B000004]
C00000004000

All ISs [09002B000005]
C00000008000

All L1 ISs [0180C2000014]
C00000008000

All L2 ISs [0180C2000015]
C00000008000

Use the **list subnet detailed** or **list subnet summary** command to verify that you have configured the subnets correctly.

Configuring OSI Over X.25 or Frame Relay

To configure the OSI protocol to run over the X.25 or Frame Relay interface, do the following:

Set the subnet
Use the **set subnet** command to set the interface to X.25 or FRL (Frame Relay). Use the defaults for all the required information. Use the **list subnet detailed** or **list subnet summary** command to verify that you have configured the subnets correctly.

Set the virtual-circuit

Use the **set virtual-circuit** command to configure an X.25 or a Frame Relay virtual circuit.

Note: The router will prompt you for a DTE address. For frame relay, enter the DLCI (Data Link Control Identifier) number. For X.25 the enter the PSN's DTE address.

Configuring a DNA V Router for a DNA IV Environment

When configuring a DNA V router, you may need to configure an interface to run in a DNA IV environment. For example, the router is attaching to both a DNA V and DNA IV network, or a DNA IV ES is attached to a DNA V router.

Before beginning the steps below, use the appropriate preceding section to configure OSI over a LAN, X.25, or Frame Relay.

1. Enter the DN configuration process. Exit `OSI config>` and enter `NCP>`. Use the **protocol DN** command.
2. Define the global DNA address. Use the **define executor address** command to configure the DNA node and area number of the router.
3. Globally enable DNA. Use the **define executor state** command to enable the DNA protocol to run on the router.
4. Enable inter-area routing. If the L2 routing algorithm is distance vector at level 2, use the **define executor type area** command to ensure that this router can exchange DNA IV level 2 routing information.
5. Enable the DNA IV circuit. Enable the circuit that the router will use to exchange the routing information. Use the **define circuit** *type* **state on** command.

DNA IV and DNA V Algorithm Considerations

DNA IV uses a distance-vector routing algorithm. DNA V can use either a distance-vector or a link-state routing algorithm. The algorithm is selected according to what is enabled and disabled, and combinations that can result from these two protocols:

DNA IV disabled *and* **OSI/DNA V enabled**

This combination is considered a pure OSI/DNA V environment and the algorithm is automatically set to link-state at both levels 1 and 2 regardless of how the **set algorithm** command is configured.

DNA IV enabled *and* **OSI/DNA V disabled**

This combination is considered a pure DNA IV environment and the algorithm is set automatically to distance-vector regardless of how the **set algorithm** command is configured.

DNA IV enabled *and* **OSI/DNA V enabled**

This is a mixed environment and the algorithm information is configured and read out of SRAM. Use the **set algorithm** command to configure this information into SRAM.

Chapter 11. Configuring and Monitoring OSI/DECnet V

This chapter describes the OSI/DECnet V configuring and monitoring commands and includes the following sections:

- “Accessing the OSI/DECnet V Monitoring Environment” on page 369
- “OSI/DECnet V Monitoring Commands” on page 369

Accessing the OSI Configuration Environment

For information on how to access the OSI configuration environment, refer to “Getting Started (Introduction to the User Interface)” in the *Access Integration Services Software User’s Guide*.

OSI/DECnet V Configuration Commands

This section summarizes and then explains the OSI configuration commands. The OSI configuration commands enable you to create or modify an OSI configuration. Enter all the OSI configuration commands following the `OSI Config>` prompt. Defaults for any command and its parameters are enclosed in brackets immediately following the prompt.

The configuring commands manipulate the permanent OSI database (SRAM).

Table 104. OSI 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 xxviii.
Add	Adds areas this node supports; receive passwords for authentication purposes; prefix addresses for other domains; and aliases
Change	Modifies some parameters set up with the **add** command.
Clear	Clears a receive password, transmit password, or SRAM
Delete	Deletes areas, PVCs, prefix-addresses, adjacencies, aliases, subnets, and X.25 routing circuit parameters.
Disable	Disables a subnet, the OSI protocol, or an X.25 routing circuit.
Enable	Enables a subnet, the OSI protocol, or an X.25 routing circuit.
List	Displays the current configuration of adjacencies, aliases, passwords, pvcs, prefix-addresses, subnets, algorithm, phaseivpfx, global information, or X.25 routing circuits.
Set	Configures the properties associated with OSI parameters (switches, globals, NETs, timers, subnets, transmit-password, prefix-addresses, adjacencies, pvc, algorithm, and phaseivpfx)
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxviii.

Add

Use the **add** command to configure area and prefix addresses, receive passwords, and address aliases.

Syntax:

add alias
area...
filter...

prefix-address

receive-password

routing-circuit...

template...

alias Adds an ASCII string that designates a particular area address or system ID. The ASCII string can be *a-z, A-Z, 0-–9*, a few other characters including the hyphen (-), comma (,), and underscore (_). Do not use escape characters.

The offset indicates the position, in semi-octets (nibbles), where the ASCII string begins within the address (aliases used for system IDs have an offset of 1). The string must be the same size or longer than the segment it is designating or you will receive an `invalid segment length` message. The maximum allowable alias is 20 bytes.

Note: When using an alias input, you must surround it with brackets. For example: **l1_update 47[*newname*]99999000012341234.**

Example:

```
add alias
Alias [ ]:
Segment [ ]:
Offset [1]:
```

Alias The character string you want to use

Segment
The NSAP segment that the alias is replacing

Offset The location of the alias (in 4-bit, semi-octets) within the NSAP. The offset is determined from the beginning (left) of the NSAP as it is displayed on the terminal.

area *area-addr*
Adds additional area addresses (18-byte maximum) that the node supports. An L1 node that supports other areas considers those synonymous areas. One area address is the area portion of the configured NET. If you try to add a duplicate area address, the router will display an error message.

Example:

```
add area 47000580999999000012341234
```

Note: When adding synonymous areas to an L1 node, use the **set globals** command to configure the maximum number synonymous areas allowed for this node. All routers within an area must use the same maximum number of synonymous areas. Adjacencies can not be established if they are different.

filter *filter-name routing-circuit-name calling-DTE call-UserData priority*
Adds parameters upon which the router bases its acceptance of incoming X.25 calls on an routing circuit, either a static incoming or dynamically assigned (DA) circuit.

The *filter-name* is the name you give the filter. The *routing-circuit-name* is the name of the routing circuit with which the filter is associated.

The *calling-DTE* is the address of the calling router.

The local router checks the DTE address of an incoming call against a prioritized list of filters for all circuits. A higher filter *priority* in the list means that a connection to that filter's calling DTE address is made first. It is recommended that you assign a higher priority to filters for static circuits than for DA circuits. This can prevent an incoming static call from being assigned a DA circuit.

The *call-UserData* can have one of three values - *osi, dec,* or *user*:

- For *osi*, the router automatically configures an ISO protocol discriminator for the call data and requires the call to be from an OSI node.
- For *dec*, the router expects the incoming calls to be from a Digital Equipment Company router.
- For *user*, you are prompted for an additional entry of up to 16 octets. Enter text to constrain the acceptance of incoming calls. The *call-UserData* field of the incoming call must match the specified text.

Example:

```
add filter
Filter Name [ ]:
Routing Circuit Name [ ]:
DTE Address [ ]:
Call UserData (OSI/DEC/USER)]:
```

If you select **user**, and additional prompt appears for you to enter user data, followed by a Priority prompt:

```
(max 16 octets) [ ]?
Priority (1-10) [5]?
```

prefix-address

Adds static routes to destinations outside the IS-IS domain. This parameter prompts you for different information depending on the type of subnet (X.25, LAN, or FRL) that was configured using the **set subnet** command.

Note: If no Address Prefix is entered, the default prefix is assumed.

Example:

LAN Subnet:

```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
MAC Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]:
```

X.25 Subnet:

```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
Mapping Type[Manual]:
DTE Address[]:
Default Metric[20]:
Metric Type [Internal]:
State [ON]:
```

Frame Relay Subnet:

```
add prefix-address
Interface Number [0]:
Address Prefix [ ]:
DTE Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]:
```

Note: If the subnet does not exist, you will receive the error message
```
Subnet does not exist – cannot define a reachable address.
```

Interface Number
Defines the interface over which the address is reached

Address Prefix
Defines the NSAP prefix (20 bytes maximum).

MAC Address
Defines the destination MAC address. You must specify this address if the interface corresponds to a LAN subnet. This prompt will only appear if the interface is connected to a LAN subnet.

Mapping Type
Defines how the destination physical address is determined, manual or X.121.
If manual, the protocol will prompt for the DTE address.
If X.121, the protocol will not prompt you for the DTE address. The DTE address in this instance is extracted from the NSAP.

DTE Address
Defines the destination DTE address. You must specify this address if the interface is X.25 and the mapping type is manual. This prompt only appears if the interface is configured for X.25 and the mapping type is manual.

Default Metric
Defines the cost of the address.

Metric Type
Defines whether the metric cost is used for external (E) routing or internal (I) routing.

State When set to ON, this prefix-address is advertised to other L2 routers. When set to OFF, this is a non-functional prefix-address.

routing-circuit
Adds a communications channel for X.25 switched virtual circuits (SVCs) that the routing layer uses to send and receive data.

The routing circuit parameter is only applicable if you configure your router as a DEC-type router. You can specify on of these types of routing circuit:
- static-in
- static-out
- dynamically-assigned

A static-in circuit handles incoming X.25 calls. A call filter (see **add filter**) specifies data the router uses to accept or reject incoming calls on the circuit. A static-out circuit initiates outgoing X.25 calls. The router uses a call template (see **add template**) to make outgoing calls. A dynamically-assigned circuit can have multiple SVCs running simultaneously. Unlike static circuits, the router uses a dynamically-assigned circuit only when there is traffic in or out of the router. It closes the dynamically-assigned circuit upon expiration of an idle timer.

The **add routing-circuit** command prompts you for values for its parameters.

Example:

```
add routing-circuit
Interface number  [0]?
Circuit Name  [ ]?
Circuit Type (STATIC/DA)  [STATIC]?
Circuit Direction (OUT/IN)  [OUT]?
```

If you select **STATIC** and **OUT**, the following additional prompts appear:

```
Recall Timer (0-65535)  [60]?
Max Call Attempts (0-255)  [10]?
Initial Min Timer (1-65535)  [55]?
Enable IS-IS  [YES]?
Level 2 only  [NO]?
External Domain  [NO]?
Default Metric  [20]?
ISIS Hello Timer [3]?
Enable DECnetV Link Initialization  [YES]?
Modify Receive Verifier  (YES/NO)  [NO]?
Transmit Verifier (YES/NO)  [NO]?
Explicit Receive Verification (TRUE/FALSE)  [TRUE]?
```

If you select **STATIC** and **IN**, the following additional prompts appear:

```
Initial Min Timer (1-65535)  [55]?
Enable IS-IS [YES]?
Level 2 only [NO]?
External Domain [NO]?
Default Metric [20]?
ISIS Hello Timer [3]?
Enable DECnetV Link Initialization [YES]?
Modify Receive Verifier (YES/NO) [NO]?
Modify Transmit Verifier (YES/NO) [NO]?
Explicit Receive Verification (TRUE/FALSE) [TRUE]?
```

If you select **DA** for the circuit type, the following additional prompts appear:

```
Recall Timer (0-65535) [60]?
Reserve Timer (1-65536) [600]?
Idle Timer (1-65536) [30]?
Max SVCs (1-65535) [1]?
```

Interface Number
Specifies the logical X.25 interface for this routing-circuit.

Circuit Name
Sets up the alphanumeric name of this routing-circuit record.

Circuit Type
Specifies whether this routing circuit is either a STATIC circuit or a DYNAMICALLY ALLOCATED circuit.

Circuit Direction
Specifies IN or OUT to determine whether the SVC of the static circuit will be established with an incoming call request or an outgoing call request. In both cases, the SVC is initially established upon operator action, but the circuit is not fully enabled until both ends of the circuit have initialized successfully.

Recall Timer
Defines the time in seconds that an out-static circuit or a DA circuit must wait before attempting a new call request. This is a result of the initial call request failing or a subsequent call having been cleared.

Max Call Attempts
If a call request fails, Max Call Attempts defines the maximum number of subsequent call requests that are attempted by the out-static circuit before no further attempts are made. At this point, a call failure is logged and operator intervention is required to activate the out-static circuit.

Initial Min Timer
Specifies the amount of time (in seconds) an out-static circuit waits for a link to be initialized (reception of either an ESH or an ISH) after the call request has been accepted. If the initial min timer expires before the link has been fully initialized, the SVC is cleared and an event generated that indicates initialization failure.

Enable IS-IS
Defines whether the IS-IS protocol is enabled on this routing-circuit. When set to ON, the IS-IS protocol is enabled; when set to OFF, the IS-IS protocol is not enabled.

Level2 Only
Specifies if this routing-circuit is used for Level2 routing only.

External Domain
Specifies whether the router transmits and receives messages to and from a domain outside its IS-IS routing domain.

Default Metric
Defines the cost of this address.

ISIS Hello Timer
Defines the time interval between transmission of ISIS hellos.

Enable DECnetV Link Initialization
Defines whether DEC-style link initialization for this circuit is enabled (YES) or not (NO).

Modify Receive Verifier
Specifies verification data to be checked against on receiving an XID when verifying by circuit.

Modify Transmit Verifier
Specifies verification data to be included in the XID.

Explicit Receive Verification
Defines whether verification is by circuit or by system. TRUE specifies verification by circuit, and FALSE specifies by system.

Reserve Timer
Defines the time after the idle timer expires during which the router still considers a remote node on a DA circuit as “active.” The router can forward data on the DA circuit until the reserve timer expires.

Idle Timer
Defines the length of time a DA adjacency my be idle (no data transmission) before it is cleared.

Max SVCs
Defines the maximum number of SVC adjacencies supported by this DA circuit. If no call can be placed because the maximum SVC adjacencies has been reached, then an event "Exceed Max SVC adjacencies" is generated.

receive-password
Adds an ASCII character string (16 characters maximum) that authenticates all incoming packets. An incoming packet whose password matches one of the set of receive-passwords is processed through the IS; any incoming packets whose passwords do not match are dropped.

Example:

```
add receive-password
```

Note: You get an error message if you use an invalid *password type.*

```
Password type [Domain]:
Password [ ]:
Reenter password:
```

Password type

Designates one of the two types of passwords, *domain* or *area*.

Domain passwords are used with L2 LSPs (Level 2, Link State Packets) and SNPs (Sequence Number PDU).

Area passwords are used with L1 LSPs and SNPs.

Password

Designates the character string that you are using for authentication. Maximum allowable string is 16 characters.

template *template-name routing-circuit-name destination-DTE call-UserData*

Creates a template by which the router makes outgoing calls on a static-out routing circuit. Templates for static-out circuits are analogous to filters for static-in circuits.

The *template-name* is the name you give the template. The *routing-circuit-name* is the name of the routing circuit with which the template is associated.

The *destination-DTE* is an address for the remote router of up to 14 digits.

The *call-UserData* must match the call data set up for a filter on the remote circuit. *Call-UserData* can have one of three values - *osi, dec,* or *user*:

- For *osi* the router automatically configures an ISO protocol discriminator for the call data and requires the call to go to an OSI router.
- For *dec* the user data identifies the outgoing calls as coming from a Digital Equipment Company router.
- For *user* you are prompted for an additional entry of up to 16 octets. Enter text to match the user data of the appropriate filter on a remote router.

Example:

```
add template
Template Name []?
Routing Circuit Name []?
DTE Address []?
Call UserData (OSI/DEC/USER) ?
```

If you choose **user** this additional prompt appears:

```
(max 16 octets) [] ?
```

Enter up to 16 octets of text for user data.

Change

Allows you to modify the parameters of ISO/DNV records created in the permanent database.

Syntax:

change	filter
	prefix-address
	routing-circuit
	template

filter *filter-name*

Changes the values for routing circuit filter parameters. You can enter a filter name or let the router prompt you for the filter name.

The values in brackets [] are the current values for the parameters; the configured value read from the permanent database.

Example: `change filter`

```
Filter Name [currentvalue]?
DTE Address [currentvalue]?
Call Userdata (OSI/DEC/USER)? [currentvalue]?
```

If you select **user**, this additional prompt appears for you to enter user data; followed by a Priority prompt:

```
(max 16 octets) [currentvalue] ?
```

prefix-address

Changes the address data for subnets. The router prompts you for the address data.

Example: `change prefix-address`

LAN Subnet:

```
Interface Number [0]:
Address Prefix [ ]:
MAC Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?
```

X.25 Subnet:

```
Interface Number [0]:
Address Prefix [ ]:
Mapping Type [Manual]:
DTE Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?
```

Frame Relay Subnet:

```
Interface Number [0]:
Address Prefix [ ]:
DTE Address [ ]:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?
```

Interface Number

Indicates the interface over which the address is reached.

Address Prefix

Indicates the destination NSAP prefix (20 bytes maximum).

MAC Address

Indicates the destination MAC address. You must specify this address if the interface corresponds to a LAN subnet. This prompt will only appear if the interface is connected to a LAN subnet.

Mapping Type

Indicates how the destination physical address is determined, *manual* or *X.121*.

If manual, the protocol prompts you for the DTE address.
If X.121, the protocol will not prompt you for the DTE address. The DTE address in this instance is extracted from the NSAP.

DTE Address

Defines the destination DTE address. You must specify this address if the interface is X.25 and the mapping type is manual. This prompt only appears if the interface is configured for X.25 and the mapping type is manual.

Default Metric
Indicates the cost of the address.

Metric Type
Indicates whether the metric cost is used for external (E) routing or internal (I) routing.

State When set to ON, this address will receive packets. When set to OFF, this is a non-functional address.

routing-circuit *routingcircuitname*
Changes the values of the configuration for a routing circuit. You can enter a routing circuit name or let the router prompt you for a name. The values in brackets [] are the current values taken from the permanent database.

Example: `change routing-circuit`

```
Routing Circuit Name [currentvalue]?
Recall Timer (0-65535) [currentvalue]?
Max Call Attempts (0-255) [currentvalue]?
Initial Min Timer (1-65535) [currentvalue]?
Enable ES-IS [currentvalue]?
Enable IS-IS [currentvalue]?
Level 2 only [currentvalue]?
External Domain [currentvalue]?
Default Metric [currentvalue]?
ESIS IS Hello Timer [currentvalue]?
ISIS Hello Timer [currentvalue]?
Enable DECnetV Link Initialization [currentvalue]?
Modify Receive Verifier (YES/NO) [currentvalue]?
Modify Transmit Verifier (YES/NO) [currentvalue]?
Explicit Receive Verification (TRUE/FALSE) [currentvalue]?
```

template *template-name*
Changes the values of the template for a static-out routing circuits. You can enter a template name or let the router prompt you for a template name. The values in brackets [] are the current values for the parameters; the configured values read from the permanent database.

Example: `change template`

```
Template Name [currentvalue]?
DTE Address [currentvalue]?
Call UserData (OSI/DEC/USER)? [currentvalue]
```

If you select **user**, this additional prompt appears for you to enter your user data; followed by a Priority prompt:

```
(max 16 octets) [currentvalue] ?
Priority (1-10) [currentvalue]?
```

Clear

Use the clear command to erase SRAM or to remove the receive or transmit password.

Syntax:

clear	receive-password
	sram
	transmit-password

receive-password
Removes all of the receive-passwords previously configured using the **add receive-password** command.

Note: You will receive an error message if you use an invalid password type.

Example:

```
clear receive
Password Type [Domain]:
```

Password Type
Specifies the type of password being used, *Domain* or *Area*. Refer to the **add receive-password** command for description of these passwords.

SRAM

Use this parameter to erase the OSI configuration from SRAM.

Attention: Use this command ***only*** if you intend to erase the configuration.

Example:

```
clear sram
Warning:  All OSI SRAM Information will be erased.
Do you want to continue? (Y/N) [N]?
```

Transmit-password
Removes the transmit-password previously configured using the **set transmit-password** command. The output for this parameter is the same as that of the receive-password parameter.

Note: You will receive an error message if you use an invalid password type.

Example:

```
clear password transmit
Password Type [Domain]:
```

Delete

Use the **delete** command to remove parameters previously configured using the **set** or **add** command.

Syntax:

delete adjacency
alias
area
filter (DEC configuration only)
prefix-address
routing-circuit
subnet
template (DEC configuration only)
virtual-circuit

adjacency
Removes a statically configured ES adjacency previously configured with the **set adjacency** command.

Example:

```
delete adjacency
Interface Number [0]?
Area Address [ ]?
System ID [ ]?
```

Interface number
Indicates the interface of the adjacency.

Area address
Indicates the area address of the adjacency.

System ID
Indicates the portion of the NET that identifies the adjacency within the area.

alias Removes the ASCII string that designates a portion of an area address or system ID.

Example:

```
delete alias
ALIAS [ ]?
```

area *address*
Removes the area address (*address*) previously configured with the **add area** command.

Example:

```
delete area 47000580999999000012341234
```

filter *filter-name*
Removes a filter record from the permanent database.

Example:

```
delete p_systems
```

prefix-address
Removes the prefix-address previously configured with the **set prefix-address** command.

Example: `delete prefix-address`

```
Interface Number [0]?
Address Prefix [ ]
```

Interface number
Indicates the interface number over which the prefix-address is configured.

Address Prefix
Indicates the destination NSAP prefix.

Interface number
Indicates the interface number over which the PVC is configured.

DTE address
Indicates the DTE address of the X.25 network to which you are connecting or the DLCI of Frame Relay network to which you are connecting.

routing-circuit *routing-circuit-name*
Removes an X.25 routing circuit that was established with **add routing-circuit** from the permanent database.

Example:

```
delete routing-circuit p_system2
```

subnet *intfc#*
Removes a subnet that was previously configured with the **set subnet** command. *Intfc#* indicates the interface number of the configured subnet.

Example:

```
delete subnet 1
```

template *template-name*
Removes the template for a static outgoing routing circuit by which the router generates outgoing X.25 messages from the permanent database.

Example:

```
delete template x25_5
```

virtual-circuit
Removes an X.25 or a Frame Relay virtual circuit that was previously configured with the set virtual-circuit command.

Example:

```
delete virtual-circuit
Interface number [0]?
DTE address []?
```

Interface number
Interface number over which the virtual circuit is configured.

DTE address
DTE address of the X.25 network to which you are connecting or the DLCI of Frame Relay network to which you are connecting.

Disable

Use the **disable** command to disable those features previously enabled using the **enable** command.

Syntax:

disable	osi
	routing-circuit
	subnet

osi Disables the OSI protocol on the router.

routing-circuit *routing-circuit-name*
Disables the specified routing circuit.

Use the **add routing-circuit** command to set up routing-circuits.

subnet interface#
Disables the OSI protocol on the specified subnet (*interface#*).

Example:

```
disable subnet 0
```

Enable

Use the **enable** command to enable the OSI protocol or an OSI subnet.

Syntax:

enable	osi
	routing-circuit...

subnet...

osi Enables the OSI protocol on the router.

routing-circuit *routing-circuit-name*
Enables the specified routing circuit.

Use the **add routing-circuit** command to set up routing-circuits.

Example:

```
enable routing-circuit p_system2
```

subnet interface#
Enables the OSI protocol on the specified subnet (*interface#*).

Example:

```
enable subnet 0
```

List

Use the list command to display the current configuration of the OSI protocol.

Syntax:

list
- adjacencies
- algorithm
- alias
- filter (DEC configuration only)
- globals
- password
- phaseivpfx
- prefix-address
- routing-circuits (DEC configuration only)
- subnets
- templates (DEC configuration only)
- timers
- virtual-circuits

adjacencies
Displays all statically configured ES adjacencies.

Example:

```
list adjacencies
Ifc    Area Address    System ID         MAC Address
 0                     0001-0203-0405    0001-0203-0405
 1                     0002-4000-0000    0000-0019-3004
```

Ifc Indicates the interface number that connects to the adjacency.

Area Address
Indicates the area address of this ES adjacency.

System ID
Indicates the portion of the NET that identifies the adjacency.

MAC Address
Indicates the MAC address (SNPA) of the adjacency.

algorithm

Displays the routing algorithm that is configured in SRAM for the DNA V protocol. If you are running the OSI protocol only, this parameter is unsupported.

Example:

```
list algorithm
Level 1 algorithm  LINK_STATE
Level 2 algorithm  DISTANCE_VECTOR
```

Level 1 Algorithm
Indicates the current configuration of the routing algorithm for level 1, Link State (default) or Distance Vector.

Level 2 Algorithm
Indicates the current configuration of the routing algorithm for level 2, Link State or Distance Vector (default).

Note: Depending on whether DNA IV is enabled or disabled, the routing algorithm displayed here may be different from what is running on the router.

alias Displays the configured aliases and their corresponding address segments.

Example:

```
list aliases
Alias        Segment          Offset

joplin       AA0004000104        1
moon         0000931004F0        1
trane        000093E0107A        1
```

filter Displays the defined filters for X.25 circuits.

Example:

```
list filters
            Rout Cir Name   Filter Name   DTE Addr   Pri   Call Data
            routeCir2       filter1       25         5     81
```

globals

Displays the router's current NET, area addresses, switch settings, global parameters, and timer configuration.

Example:

```
list globals
DNAV State: Enabled*   Network Entity Title:  4700050001:0000931004F0
Manual Area Addresses:
1. 4700050001    2. 7700050011

Switches:
ESIS Checksum = On              ESIS Init Option = Off
Authentication = Off

Globals:
IS Type = L2                    System ID Length = 6
L1 LSP Size = 1492 bytes        L2 LSP Size = 1492 bytes
Max IS Adjs = 50                Max ES Adjs = 200
Max Areas = 50                  Max ESs per Area = 50
Max Ifc Prefix Adds = 100       Max Ext Prefix Adds = 100
Max Synonymous Areas = 3        Max Link State Updates = 100
```

OSI State or DNAV State
Indicates if the OSI or DNA V protocol is running on the router.

Network Entity Title
Indicates the area address and system ID that make up the router's NET.

Manual Area Addresses
Areas that the router operates within. The first area address reflects

the router's configured NET area address. Additional area addresses were added with the **add area** command.

Globals:
Indicates the currently configured global parameters:

IS Type
The router's designation in the OSI environment: L1 or L2.

Domain ID Length
The size (in bytes) of the system ID portion of the NET.

Note: All routers throughout the domain must agree on the length of the domain ID.

L1 LSP Size/L2 LSP Size
Displays the L1 and L2 maximum LSP buffer size.

Max IS Adjacencies/Max ES Adjacencies
Displays the maximum number of ES and IS adjacencies that are allowed for all circuits.

Max Areas
Displays the maximum number of areas in the routing domain.

Max ESs per Area
Displays the maximum number of ESs allowed in one area.

Max Int Prefix Adds
Displays the maximum number of internal prefix addresses.

Max Ext Prefix Adds
Displays the maximum number of external prefix addresses.

Max Synonymous Areas
Displays the maximum number of level 1 areas serviced by this router.

password
Displays the number of transmit and receive passwords configured for each OSI Domain and Area. You configure receive passwords using the **add receive-password** command. You configure transmit passwords using the **set transmit-password** command.

Example:

```
list password
  Number of Passwords Configured:
      -- Domain --
  Transmit = 3
  Receive  = 2
      -- Area --
  Transmit = 4
  Receive  = 6
```

phaseivpfx
Displays the configured DNA phase IV address-prefix that the OSI protocol is using to route packets to a connected DNA IV network.

Example:

```
list phaseivpfx
            Local Phase IV Prefix: 49
```

prefix-address
Displays all the SNPAs for statically configured routes.

Example:

```
list prefix:-addresses
Ifc  Type  Metric  State  Address Prefix  Dest Phys Address
 0    INT    20     On        470006        302198112233
 1    EXT    50     OFF       470006        302198223344
```

Ifc Indicates the interface number where the address can be reached.

Type Indicates the type of metric, either internal (INT) or external (EXT).

Metric Indicates the cost of the reachable address.

Address prefix
Indicates the destination NSAP prefix. This prefix may be 20 bytes long.

Dest Phys Address
Indicates the destination DTE address if this interface is X.25 and the configured mapping is manual.

routing-circuits
Displays a summary of all routing-circuits or details of each routing circuit.

Example:

```
list routing circuits
Summary or Detailed [Summary]? Summary

Ifc   Name        Type                 Enabled
0     routecir1   STATIC-OUT           YES
0     routecir2   STATIC-IN            YES
0     routecir3   DA                   YES


Summary or Detailed [Summary]? Detailed

Routing Circuit Name []  routecir2
Interface #:                0
Enabled:                    YES
Type:                       STATIC
Direction:                  Incoming
Initial Minimum Timer:      55
Enable IS-IS:               YES
L2 Only:                    NO
External Domain:            NO
Metric:                     20
IS-IS Hello Timer:          3
DECnetV Link Initialization:   YES
Receive Verifier:
Transmit Verifier:
Explicit Receive Verification: TRUE
```

Interface # / Ifc
The logical X.25 interface for this routing-circuit.

Name The alphanumeric name of this routing-circuit record.

Enabled
Indicates the state of the routing-circuit: YES for enabled, NO for disabled.

Type Indicates whether the circuit is STATIC-IN, STATIC-OUT, or DA (dynamically allocated).

Direction
Indicates how the router establishes a static routing circuit: by an incoming call request (IN) or an outgoing call request (OUT).

In either case, the SVC is initially established upon operator action, but the circuit is not fully enabled until both ends of the circuit have initialized successfully.

Initial Min Timer
The amount of time (in seconds) that a static-out circuit waits for a link to be initialized (reception of either an ESH or an ISH) after the call request

has been accepted. If the initial min timer expires before the link is fully initialized, the SVC is cleared and an event is generated indicating initialization failure.

Enable IS-IS
Indicates whether the IS-IS protocol is enabled on this circuit.

L2 Only
Indicates whether this routing circuit is used for Level2 routing only.

External Domain
Indicates whether the router transmits and receives messages to and from a domain outside its IS-IS routing domain.

Metric Gives the cost of this address.

ISIS Hello Timer
Gives the time interval between transmissions of ISIS hellos.

DECnetV Link Initialization
Indicates whether DEC-style link initialization for this circuit is enabled (YES) or disabled (NO).

Receive Verifier
Displays verification data to be checked against a received XID when verifying by circuit.

Transmit Verifier
Displays verification data to be included in XIDs when verifying by circuit.

Explicit Receive Verification
Indicates whether verification is done by the circuit or the system. TRUE indicates verification by the circuit, FALSE indicates verification by the system.

Subnet *subnet.reprt intfc#*
Displays subnet information.

- *Subnet.reprt* has two options, Summary and Detailed.
  - *Summary* displays information for all configured subnets.
  - *Detailed* displays information for LAN subnets only.
- *Intfc#* is the interface that connects to the subnet.

Example:

```
list subnet summary
Ifc  State  Type  ESIS  ISIS  L2 Only  Ext Dom  Metric  EIH (sec)  IIH(sec)
0    On     LAN   Enb   Enb   False    False    20       10         3
2    On     X25
3    On     Frl
```

Ifc Indicates the interface number of the subnet.

State Indicates the state of the interface, ON or OFF.

Type Indicates the type of subnet: LAN, X25,

ESIS Indicates the state of the ES-IS protocol, enabled (Enb) or disabled (Dis).

ISIS Indicates the state of the IS-IS protocol, enabled (Enb) or disabled (Dis).

L2 Only
Indicates if the router is operating at level 2 only, yes (true) or no (false).

Ext Dom
Indicates if the router is operating outside the IS-IS routing domain (external domain).

Metric Indicates the cost of using this subnet.

EIH Indicates the interval at which ES hello messages are sent out over the subnet.

IIH Indicates the interval at which IS hello message are sent out over the subnet.

Example:

```
list subnet detailed
            Interface Number [0]? 0

            Detailed information for subnet 0:
               ISIS Level 1 Multicast: 018002B000014
               ISIS Level 2 Multicast: 018002B000015
               All ISs Multicast:      009002B000005
               All ESs Multicast:      009002B000004
               Level 1 Priority: 64
               Level 2 Priority: 64
```

ISIS Level 1 Multicast
Indicates the multicast address to use when transmitting and receiving L1 IS-IS PDUs.

ISIS Level 2 Multicast
Indicates the multicast address to use when transmitting and receiving L2 IS-IS PDUs.

All ISs Multicast
Indicates the multicast address to use when receiving ES hellos.

All ESs Multicast
Indicates the multicast address to use when transmitting IS hellos.

Level 1 Priority/Level 2 Priority
Indicates the router’s priority for becoming the designated router on the LAN.

templates
Displays a list of templates defined on this router.

Example:

```
list template
Route Cir Name      Template Name      DTE Addr      Call UserData
routetest2          temptest2          25            81
```

timers Displays the OSI/DNA V timer configuration (what is running on the router, OSI, or DNA V).

Example:

```
list timers
            Timers:
            Complete SNP (sec) = 10        Partial SNP (sec) = 2
            Min LSP Gen (sec) = 30         Max LSP Gen (sec) = 900
            Min LSP Xmt (sec) = 30         Min Br LSP Xmt (msec) = 33
            Waiting Time (sec) = 60        DR ISIS Hello (sec) = 1
            ES Config Timer (sec) = 10
```

Timers:
Indicates the configuration of the OSI timers excluding any per circuit timers.

Complete SNP
The interval between generation of complete SNPs.

Partial SNP
The minimum interval between sending partial SNPs.

Min LSP Generation/Max LSP Generation
The minimum and maximum intervals between generations of LSPs.

Min LSP Transmission
The minimum interval between LSP retransmissions.

Min Broadcast LSP Transmission
The minimum interval between LSP retransmissions on a broadcast circuit.

Waiting Time
The time the update process must delay before entering the ON state.

DR ISIS Hello
The interval between generations of IS-IS hello PDUs if this router is a designated router.

ES Config Timer
The minimum interval between that an ES must send a hello packet each time an interface comes up.

virtual-circuits
Displays information about all X.25 virtual circuits.

Example: `list virtual-circuits`

Set

Use the **set** command to configure the router to run the OSI protocol.

Syntax:

set	adjacency
	algorithm
	globals
	network-entity-title
	phaseivpfx
	subnet
	switches
	timers
	transmit-password (DEC configuration only)
	virtual-circuit (IBM 2212 configuration only)

adjacency
Adds or changes an ES adjacency. Add an ES adjacency for all LAN ESs that do not run the ES-IS protocol.

Example:

```
set adjacency
Interface Number [0]:
Area Address [ ]:
System ID [ ]:
MAC Address [ ]:
```

Interface Number
Indicates the interface number that connects to the adjacency.

Area Address
Indicates the area where the adjacency is located.

System ID
Indicates system ID portion of the NET that is used to identify the adjacency.

MAC Address
Indicates the MAC address (SNPA) of the adjacency.

algorithm

Note: This is a DNA phase V command. This command will work only if the DNA phase V protocol is included in the software load. This enables you to select the type of routing algorithm that you are using for the DNA routing protocol, link state (DNA V) or distance vector (DNA IV).

Example:

```
set algorithm
Level 1 Algorithm [link_state]?
Level 2 Algorithm [distance_vector]?
```

Level 1 Algorithm
Selects the type of routing algorithm, link_state (for DNA V networks) or distance_vector (for DNA IV networks).

Level 2 Algorithm
Selects the type of routing algorithm, link_state (for DNA V networks) or distance_vector (for DNA IV networks).

globals
Configures the global parameters required by the OSI protocol.

Example:

```
set globals
IS Type [L2]:
System ID Length [6 bytes]:
Max Synonymous Areas [3]:
L1 LSP Buffer Size :[1492 bytes]:
L2 LSP Buffer Size [1492 bytes]:
Max IS Adjacencies ]50[:
Max ES Adjacencies [200]:
Max Areas in Domain [50]:
Max ESs per Area [500]:
Max Internal Prefix Addresses [100]:
Max External Prefix Addresses [100]:
Max Link State Updates [100]?
```

IS Type (L1 or L2)
Selects the level of the router, level 1 or level 2.

System ID Length
Selects the length of the domain ID portion of the NET. This length must be the same for all routers in same domain.

Max Synonymous Areas
Selects the maximum number of level 1 areas that are serviced by this router.

L1 LSP Buffer Size
Selects the buffer size of the level 1 LSPs and SNPs originated by the router. Range is 512 to 1492. If the interface packet size is less than what you configured here, OSI will not run, and the router generates the ELS message ISIS.053.

L2 LSP Buffer
Selects the buffer size of the level 2 LSPs and SNPs originated by the router. Range is 512 to 1492. If the interface packet size is less than what you configured here, OSI will not run, and the router generates the ELS message ISIS.053.

Max IS Adjacencies
Selects the total number of IS adjacencies allowed for all circuits. This number is used to size the IS adjacency free pool.

Max ES Adjacencies
Selects the total number of ES adjacencies allowed for all circuits. This number is used to size the ES adjacency free pool.

Max Areas in Domain
Selects the total number of areas in the routing domain. This number is used to size the L2 routing table.

Max ESs per Area
Selects the total number ESs in any one area. This number is used to size the L1 routing table.

Max Internal Reachable Addresses
Selects the number you are using to size the internal metric routing table.

Max External Reachable Addresses
Selects the number you are using to size the external metric routing table.

Max Link State Updates
Selects the number you are using to size the link state database.

network-entity-title
Configures the router's NET. The NET consists of the router's system ID and area address.

Example:

```
set network-entity-title
Area-address [ ]
System-ID [ ]:
```

Area-address
Indicates one of area address portion of the router's NET. It is included as the first address in the router's set of manual area addresses. Each area address may be a maximum of 19 bytes.

System-ID
Defines the portion of the NSAP that identifies this specific router. The system ID can be a maximum of 19 bytes, but the length must agree with the domain ID length that you configured with the **set globals** command.

phaseivpfx
Configures the prefix-address to allow the OSI protocol to route packets to the attached DNA IV network. The default is 49 (hexadecimal).

Example:

```
set phaseivpfx

Local Phase IV prefix [49]?
```

subnet

Adds or changes a subnet. This parameter prompts you for different information depending on the type of subnet that your configuring: X.25, or LAN.

Example:

X.25 subnet:

```
set subnet
Interface number [0]:
Interface Type [X25]:
```

LAN subnet:

```
Interface number [0]:
Interface Type [LAN]:
Enable ES-IS [N]?
Enable IS-IS [N]?
Level 2 Only [N]?
External Domain [N]?
Default Metric [20]:
ESIS IS Hello Timer [10 sec]:
ISIS Hello Timer [3 sec]:
Modify Transmit password [No]?
Modify the set of receive passwords [No]?
L1 Priority [64]:
L2 Priority [64]:
All ESs [0x09002B000004]:
All ISs [0x09002B000005]:
All L1 ISs [0x0180C2000014]:
All L2 ISs [0x0180C2000015]:
```

Frame Relay subnet:

```
Interface number [0]:
Interface Type [FRL]:
```

Interface number
Binds the subnet to the specified interface.

Enable ES-IS
Indicates whether the ES-IS protocol is going to run over the interface, yes (Y) or no (N).

Enable IS-IS
Indicates whether the IS-IS protocol is going to run over the interface, yes (Y) or no (N).

Interface Type
Indicates the type of subnet: LAN, X.25, and Frame Relay (FRL). LAN includes Ethernet and Token-Ring.

Level 2 Only
Indicates whether the subnet should run at level 2 only, yes (Y) or no (N). A no designation allows the router to route over that subnet at both level 1 and level 2.

External Domain
Indicates whether the circuit is operating outside the IS-IS routing domain.

Default Metric
Indicates the cost of the subnet. Cost range 20–63.

IS Hello Timer
Indicates the period between transmissions of IS hello PDUs.

ISIS Hello Timer
Indicates the period between transmissions of L1 and L2 IS-IS hello PDUs.

Modify Transmit password
Removes or changes a circuit transmit password. When you select yes, this option prompts you with the following:

```
Delete or change the transmit password
[change]?
```

Modify the set of receive passwords
Removes all or adds one circuit receive-password. When you select yes, this option prompts you with the following:

```
Delete all or add 1 receive password
[add]?
```

L1 Priority/L2 Priority
Indicates the router priority for becoming the designated router on the LAN.

All ESs
Indicates the multicast address to use when transmitting IS hellos. The default address reflects the ethernet/802.3 multicast address. If you are connecting to a 802.5 LAN, use **C00000004000**.

All ISs
Indicates the multicast address to use when receiving ES hellos. The default address reflects the ethernet/802.3 multicast address. If you are connecting to a 802.5 LAN, use **C00000008000**.

All L1 ISs
Indicates the multicast address to use when transmitting and receiving L1 IS-IS PDUs. The default address reflects the ethernet/802.3 multicast address. If you are connecting to a 802.5 LAN, use **C00000008000**.

All L2 ISs
Indicates the multicast address to use when transmitting and receiving L2 IS-IS PDUs. The default address reflects the ethernet/802.3 multicast address. If you are connecting to a 802.5 LAN, use **C00000008000**.

switches
Turns the OSI options on or off.

Example:

```
set switches
ES-IS Checksum Option [OFF]?
ES-IS Init Option [OFF]?
ISIS Authentication [OFF]?
```

IS-IS Checksum Option
When switched on, the router generates checksums for all sourced ES-IS packets.

ES-IS Init Option
When switched on, the router sends a directed IS Hello to a new ES neighbor.

IS-IS Authentication
If switched on, each IS-IS packet includes the transmit password configured for the domain, area, and circuits. Also, no checking against receive passwords is done.

timers Configures the OSI timers, excluding any circuit timers.

Example:

```
set timers
Complete SNP [10 sec]:
Partial SNP [2 sec]:
Minimum LSP Generation [30 sec]:
Maximum LSP Generation [900 sec]:
Minimum LSP Transmission [5 sec]:
Minimum Broadcast LSP Transmission [33 msec]:
Waiting Time [60 sec]:
Designated Router ISIS Hello [1 sec]:
Suggested ES Configuration Timer (sec) [10]:
```

Complete SNP
Selects the interval between the generation of complete sequence number PDUs (SNP) by the designated router on a broadcast circuit.

Partial SNP
Selects the minimum interval between sending partial sequence number PDUs (SNP).

Minimum LSP Generation
Selects the minimum interval between successive generations of Link State Packets (LSPs) with the same LSP ID generated by the router.

Maximum LSP Generation
Selects the maximum interval between LSPs generated by the router.

Minimum LSP Transmission
Selects the minimum interval between retransmissions of a LSP.

Minimum Broadcast LSP Transmission
Selects the minimum transmission, in milliseconds, between transmission of LSPs on a broadcast circuit.

Waiting Time
Selects the number of seconds the update process should delay in the waiting state before entering the ON state.

Designated Router ISIS Hello
Selects the interval between the generation of IS-IS hello PDUs by the router if the router is the designated router on a LAN.

Suggested ES Configuration Timer
Sets the option field of the IS hello message that instructs the ES to change the rate at which it sends ES hellos.

transmit-password
Sets or changes a transmit password.

Example:

```
set transmit-password
Password type [Domain]:
Password [ ]:
Reenter password:
```

Password type
Selects the type of password: *domain* or *area.*
Domain passwords are used with L2 LSPs and SNPs. Area passwords are used with L1 LSPs and SNPs.

Password
Indicates the character string that your using for authentication. Maximum allowable string can be 16 characters.

virtual-circuit

Configures an X.25 SVC or PVC, or a Frame Relay PVC.

Example:

```
set virtual-circuit
Interface Number [0]:
DTE Address []:
Enable ISIS (Y or N) [Y]?
L2 only (Y or N) [N]?
External Domain (Y or N) [N]?
Default Metric [20]:;
ISIS Hello Timer [3 sec]?
Modify transmit password (y or n) [N]?
Modify the set of receive passwords [No]?
```

Interface Number
Indicates the X.25 or Frame Relay interface over which the virtual circuit is configured.

DTE Address
Indicates the destination DTE address for X.25 or the DLCI (Data Link Control Identifier) for Frame Relay. This address must be the same as the one defined for the virtual circuit in the X.25 configuration or the Frame Relay configuration.

Default Metric
Indicates the cost of the circuit.

Enable IS-IS
Indicates whether the IS-IS protocol is going to run over the interface, yes (Y) or no (N).

L2 only
Indicates whether the circuit should run at level 2 only, yes (Y) or no (N). A no designation allows the router to route at both level 1 and level 2.

External Domain
Indicates whether the circuit is operating outside the IS-IS routing domain.

Accessing the OSI/DECnet V Monitoring Environment

For information on how to access the OSI/DECnet V monitoring environment, refer to *Getting Started (Introduction to the User Interface)* in the *Access Integration Services Software User's Guide*

OSI/DECnet V Monitoring Commands

This section describes the OSI/DECnet V Monitoring commands. Use these commands to gather information from the database.

The monitoring commands either display or modify the volatile database.

Table 105. OSI/DECnet V Monitoring 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 xxviii.
Addresses	Displays the router's NET and area addresses.
Change Metric	Modifies the cost of a circuit.
CLNP-Stats	Displays OSI CLNP statistics.

Table 105. OSI/DECnet V Monitoring Commands Summary (continued)

Command	Function
DNAV-info	Displays the DNAV Level1 and Level2 routing algorithm currently in effect.
Designated-router	Displays the designated router for the LAN.
ES-adjacencies	Displays all the ES adjacencies in the adjacency database.
ES-IS-Stats	Displays statistics associated with the ESIS protocol.
IS-adjacencies	Displays all the IS adjacencies in the adjacency database.
IS-IS-Stats	Displays statistics associated with the ISIS protocol.
L1-routes	Displays all the L1 routes in the Level 1 database.
L2-route	Displays all the L2 routes in the Level 2 database.
L1-summary	Displays a summary of the level 1 link state database.
L2-summary	Displays a summary of the level 2 link state database.
L1-update	Displays the information contained in L1 link state update packet.
L2-update	Displays the information contained in L2 link state update packet.
Ping-1139	Causes the router to send an echo request to a destination and wait for a reply.
Route	Displays the route a packet takes to a specified destination.
Send echo packet	Encodes an echo request message in the CLNP packet.
Show routing circuits	Displays the state of user-defined routing circuits for the specified interface. Applies when the router is configured as a DEC-style router.
Subnets	Displays all user-defined subnets.
Toggle	Enables or disables the NSAP alias substitution function.
Traceroute	Displays the route a packet travels to its destination.
Virtual-circuits	Displays all user-defined virtual circuits. Applies when the router is configured as an IBM 2212-style router.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Addresses

Use the **addresses** command to list the router's NET and the area addresses configured for this router.

Syntax:

addresses

Example:

```
addresses
Network Entity Title:
4700-0500-01  000-9310-04F0
Area Addresses:
4700-0500-01
4900-02
```

Network Entity Title
Identifies the router. The NET consists of an area address and a system ID.

Area Address
Indicates addresses within the routing domain. The router can have a maximum of three area addresses configured at any one time.

Change Metric

Use the **change metric** command to modify the cost of a circuit.

Syntax:

change metric

Example:

```
change metric
Circuit [0]?
New Cost [0]?
```

Circuit
Indicates the circuit number that you want to change.

New Cost
Indicates the new cost of the circuit. Range: 1 to 63.

CLNP-Stats

Use the **clnp-stats** command to display the OSI Connectionless Layer Network Protocol (CLNP) statistics.

Syntax:

clnp-statistics

Example:

```
clnp-statistics

Received incomplete packet                      0
Received packet with bad NSAP length            0
Received packet with bad checksum               0
Received packet with bad version number         0
Received packet with bad type                   0
Received packet with expired lifetime           0
Received packet with bad option                 0
Received packet with unknown destination        0
Received packet with no segmentation permitted  0
Received data packet cannot be forwarded        0
CLNP input queue overflow                       0
No buffer available to send error packet        0
No route to send error packet                   0
Received OK CLNP packet                         0
Cannot forward error packet                     0
ISO unknown initial protocol ID                 0
Received error packet                           0
Received local data packet                      0
Sent error packet                               0
received echo packet - destination unknown      0
cannot send an echo packet, handler error       0
sent ECHO reply packet                          0
sent ECHO request packet                        0
received ECHO Request                           0
received ECHO reply                             0
Error PDU dropped - SP, MS or E/R flag set      0
```

Received incomplete packet
Indicates that a data packet fragment recognized as an ISO CLNP data packet was received.

Received packet with bad NSAP length
Indicates that an ISO CLNP data packet was received with an incorrect NSAP length.

Received packet with bad checksum
Indicates that an ISO CLNP data packet was received with a bad checksum.

Received packet with bad version number
Indicates that an ISO CLNP data packet was received with an incorrect or unsupported version number.

Received packet with bad type
Indicates that an ISO CLNP data packet was received with an incorrect or unsupported type field.

Received packet with expired lifetime
Indicates that an ISO CLNP data packet was received with an expired lifetime.

Received packet with bad option
Indicates that an ISO CLNP data packet was received with a bad optional parameter.

Received packet with unknown destination
Indicates that an ISO CLNP data packet was received but could not be routed. The routing table contains no entry for the destination.

Received packet with no segmentation permitted
Indicates that an ISO CLNP data packet was received that needed segmentation. The segmentation permitted flag was not set.

Received data packet cannot be forwarded
Indicates that an ISO CLNP data packet was received but could not be routed because of a handler error.

No buffer available to send error packet
An attempt to send an ISO CLNP error packet failed because of a lack of system I/O buffers.

No route to send error packet
An attempt to send an ISO CLNP error packet failed because it could not be routed.

Received OK CLNP packet
Indicates that an ISO CLNP data packet was received and passed error checking.

Cannot forward error packet
Indicates that an ISO CLNP error packet could not be routed because of a handler error.

ISO unknown initial protocol ID
Indicates that an ISO CLNP packet was received with an unknown or unsupported initial protocol identifier.

Received error packet
Indicates that an ISO CLNP error packet was received for this router.

Received local data packet
Indicates that an ISO CLNP data packet was received with the destination NSAP indicating one of the router's NSAPs.

Sent error packet
Indicates that ISO CLNP error packet was sent on receipt of a bad packet.

Designated-router

Use the **designated-router** command to display the designated router for the LAN subnets that are physically attached to this router and actively running IS-IS.

Syntax:

designated-router

Example:

```
designated-router
Designated Router Information:
Hdw   Int#   Circ       L1DR                L2DR
Eth/1  1      2         0000931004F002      0000931004F002
TKR/0  0      1         Elvis-01            Elvis-01
```

Hdw Indicates the type and instance of LAN attached to this router.

Int# Indicates the interface number of this router that attaches to the LAN.

Circ Indicates the circuit number assigned by the router. This number is always one more than the interface number for LAN subnets.

L1DR Indicates the LAN ID of the designated router. If the use of an alias is enabled, this command displays the alias of the particular segment. The LAN ID is the designated router's system ID concatenated with a 1-byte locally-assigned circuit ID.

L2DR Description is the same as L1DR described above.

Note: If the designated router has not been elected yet, "Not Elected" will be displayed instead of a LAN ID.

DNAV-info

Use the **dnav-info** command to display the routing algorithm that is currently running on the router.

Syntax:

dnav-info

Example:

```
dnav-info
DNA V Level 1 Routing Algorithm: Distance-vector
DNA V Level 2 Routing algorithm: Distance-vector
```

Note: Depending on whether or not DNA IV is enabled or disabled, the routing algorithm displayed here may differ from what is configured in memory using the **set algorithm** command at the OSI/DECnet V `config>` prompt.

If DNA IV is enabled - the routing algorithm is the one configured in memory.

If DNA IV is disabled - the routing algorithm is set to link state and may differ from that set in memory.

ES-Adjacencies

Use the **es-adjacencies** command to display all the End System (ES) adjacencies that are either configured or learned through the ESIS protocol.

Syntax:

es-adjacencies

Example:

```
es-adjacencies
End System Adjacencies
System ID       MAC Address      Interface    Lifetime   Type
6666-6666-6666  1234-FEAA-041C       0        50         DNAIV
```

System ID
The system ID of the ES adjacency.

MAC Address
Indicates the MAC address of the ES on the subnet.

Interface
Indicates the router's interface number where the ES adjacency was learned.

Lifetime
Indicates the amount of time, in seconds, that the router has left before the information received in the last ES Hello message is discarded. In the case of static or a manually configured ES-Adjacency, this field reads **Static**.

Type
Indicates the type of ES adjacency, OSI, DNAIV, DNAIV', and MANUAL for statically configured adjacencies.

ES-IS-Stats

Use the **es-is-stats** command to display the statistics for the ESIS protocol.

Syntax:

es-is-stats

Example:

```
es-is-stats

ESIS input queue overflow                      0
Received incomplete packet                     0
Received packet with bad checksum              0
Received packet with bad version               0
Received packet with bad type                  0
No iob available to send hello                 0
Cannot send hello due to packet handler error  0
Sent hello                                     3672
Received packet with bad header                0
Received hello with bad nsap                   0
Received hello packet with bad option          0
Received hello                                 0
Received hello with unsupported domain source  0
No resources to install route                  0
Received hello with conflicting route          0
Timed out route reactivated                    0
No resources to send redirect                  0
Redirect not sent - handler error              0
Sent redirect                                  0
Timed out route                                0
Timed out route                              0
Unable to  allocate resources for a new ES adjacency 0
hello PDU dropped, received over point-to-point circ 0
ESIS hello PPDU dropped, no matching area address 0
dropped hello packet - manual ES adjacency exists 0
```

ESIS input queue overflow
The ESIS packet was dropped because of a task input queue has overflowed.

Received incomplete packet
A packet fragment recognized as an ESIS packet was received.

Received packet with bad checksum
An ESIS packet with a bad checksum was received.

Received packet with bad version
An ESIS packet with a bad or unsupported version was received.

Received packet with bad type
An ESIS packet with a bad or unsupported type field was received.

No iob available to send hello
An attempt to send an ESIS hello failed because of a lack of system I/O buffers.

Cannot send hello due to packet handler error
An ESIS hello could not be sent because of a handler error.

Sent hello
An ESIS hello was sent out an interface.

Received packet with bad header
An ESIS hello packet with a bad holding time or received field was received.

Received hello with nsap
An ESIS hello packet with a bad NSAP or an NSAP that over ran the field was received.

Received hello packet with bad option
An ESIS CLNP data packet was received with a bad option parameter.

Received hello
An ESIS hello packet was received on the interface.

Received hello with unsupported domain source
An ESIS hello packet was received from an unspecified domain source.

No resources to install route
An ESIS hello packet was received, but there were no resources to install the route.

Received hello with conflicting route
An ESIS hello packet was received but could not be entered into the database. A previously-defined static or dynamic route in the database conflicts with the route in the hello.

Timed out route reactivated
An ESIS hello packet with a previously timed out route was received.

No resources to send redirect
An ESIS redirect packet could not sent because of a lack of resources.

Redirect not sent handler error
An ESIS redirect packet could not be sent because of a handler error.

Sent redirect
An ESIS redirect packet was sent out the interface.

Timed out route
An ESIS hello route has timed out.

Unable to allocate resources for a new ES adjacency
An ES-IS hello packet was received but the router had insufficient resources to establish an ES adjacency with the sending node.

hello PDU dropped, received over point-to-point circ
An ES-IS hello packet was dropped because the circuit involved is a point-to-point circuit.

ESIS hello PPDU dropped, no matching area address
An ES-IS hello packet was dropped because the area did not match the router’s area address. The ES-IS protocol applies to one area only.

dropped hello packet-manual ES adjacency exists.
An ES-IS hello packet was dropped because a static ES adjacency exists with the sending node.

IS-Adjacencies

Use the **IS-adjacencies** command to list all the IS adjacencies that are learned through the ISIS protocol.

Syntax:

is-adjacencies

Example:

```
is-adjacencies
Intermediate System Adjacencies
System ID        MAC Address     Int  Level  Usage   State   Life   Type
0000-9310-04C8   AA00-0400-EF04   0     L1   L1/L2   DOWN            OSI
0000-9310-04C8   AA00-0400-EF04   0     L2   L1/L2   DOWN          DNAIV
AA00-0400-0504   AA00-0400-0504   1     L2     L2     UP     5390    OSI
```

System ID
The system ID of the IS adjacency.

MAC Address
Indicates the MAC Address of the IS adjacency.

Int Indicates the router's interface number that connects to the IS adjacency.

Level For LANs this indicates the neighbor system level from type of hello message, L1 or L2. For point-to-point this indicates the neighbor system type L1 only, otherwise L2.

Usage Indicates from the hello packet circuit type, L1 only, L2 only, or L1 and L2.

State Indicates the operational state of the IS adjacency, up or down.

Life Indicates the amount of time, in seconds, before discarding the last IS Hello message.

Type Indicates the routing protocol type of the IS adjacency, OSI or DNA IV.

IS-IS-Stats

Use the **is-is-stats** command to display information associated with the ISIS protocol.

Syntax:

is-is-stats

Example:

```
is-is-stats
Link State Database Information

no. of level 1 LSPs       1      no. of level 2 LSPs       0
no. of L1 Dijkstra runs   21     no. of L2 Dijkstra runs   0
no. of L1 LSPs deleted    0      no. of L2 LSPs deleted    0
no. of routing table entries allocated   6

Packet Information

level 1 lan hellos rcvd  0      level 1 lan hellos sent   10967
level 2 lan hellos rcvd  0      level 2 lan hellos sent   10967
pnt to pnt  hellos rcvd  0      pnt to pnt  hellos sent   0
level 1 LSPs rcvd        0      level 1 LSPs sent         40
level 2 LSPs rcvd        0      level 2 LSPs sent         0
level 1 CSNPs rcvd       0      level 1 CSNPs sent        0
```

```
level 2 CSNPs rcvd       0      level 2 CSNPs sent       0
level 1 PSNPs rcvd       0      level 1 PSNPs sent       0
level 2 PSNPs rcvd       0      level 2 PSNPs sent       0
```

no. of level 1/level 2 LSPs
Indicates the number of L1 and L2 link state packets that are in the database.

no. of L1/L2 Dijkstra runs
Indicates the number of times the router computed the L1 and L2 routing tables.

no. of L1/L2 LSPs deleted
Indicates the number of L1 and L2 link state packets that were deleted from the database.

no. of routing table entries allocated
Indicates the number of entries the routing able currently holds.

level 1/level 2 lan hellos rcvd
Indicates the number of LAN hellos the router has received.

level 1/level 2 hellos sent
Indicates the number of LAN hellos that router has sent.

pnt to pnt hellos rcvd
Indicates the number of point-to-point hellos that the router has received.

pnt to pnt hellos sent
Indicates the number of point-to-point hellos that the router has sent.

level 1/level 2 LSPs rcvd
Indicates the number of L1 and L2 link state packets (LSPs) that the router has received.

level 1/level 2 LSPs sent
Indicates the number of L1 and L2 LSPs that the router has sent.

level 1/level 2 CSNPs rcvd
Indicates the number of L1 and L2 complete sequence number PDUs (CSNPs) that the router has received.

level 1/level 2 CSNPs sent
Indicates the number of L1 and L2 CSNPs that the router has sent.

level 1/level 2 PSNPs rcvd
Indicates the number of L1 and L2 partial sequence number PDUs (PSNPs) that the router has received.

level 1/level 2 PSNPs sent
Indicates the number of L1 and L2 PSNPs that the router has sent.

L1-Routes

Use the **l1-routes** command to display all the level 1 routes that are in the L1 routing database.

Syntax:

l1-routes

Example:

```
l1-routes
Level 1 Routes
Destination System ID   Cost    Source       Next Hop
```

```
0000-9300-0047          0      LOCArea         *
AA00-0400-080C          1      ESIS        AA00-0400-0C04, Ifc 7
7777-7777-7777          0      ISIS        3455-6537-2215
```

Destination System ID
Indicates the system ID of the destination host.

Cost Indicates the cost of this route.

Source
Indicates the one of three sources where the router learned of the route: LOCAREA, ESIS, or ISIS.

Next Hop
Indicates the next hop a packet would take on its route. An asterisk (*) designation refers to the router itself as the packet's destination. An address with an interface number is either the MAC address of a directly connected ES, or the DTE address if the next hop is an X.25 switch, or a DLCI if the next hop is Frame Relay switch. A system ID (34555372215) refers to the next hop to destination.

L2-Routes

Use the **l2-routes** command to display all the level 2 routes in the L2 database.

Syntax:

l2-routes

Example:

```
l2-routes
Level 2 Routes
Destination                Cost        Type       Next Hop
4700-0500-01                0          LOC-AREA      *
4900-02                     20         AREA       0000-9310-04C9
```

Destination
Indicates the system ID of the destination area or reachable address.

Cost Indicates the cost of this route.

Type Indicates the four types of routes: LOC-area (local), LOC-prefix, area, prefix/I, and prefix/E. LOC-area is a directly connected area; a LOC-prefix is a prefix that this router advertises; prefix/I and prefix/E are routes that require another hop to reach their destination.

Next Hop
Indicates the next hop a packet would take on its route. An * designation, or a direct designation, refers to a directly-connected host off the router. A system ID refers to the next router the packet must pass through to reach its destination.

L1-Summary

Use the **l1-summary** command to display a summary of the level 1 link state database.

Syntax:

l1-summary

Example:

```
l1-summary
Link State Database Summary - Level One

LSP ID               Lifetime   Sequence #   Checksum   Flags   Cost
0000-9300-40B0-0000    0           0            0         0     1024
0000-93E0-107A-0000    384         CE          3CC9       1     0
AA00-0400-0504-0000    298         8E          40F1       B     20
AA00-0400-0504-0100    4           B8          A812       3     20

Total Checksum 25CC
```

LSP ID
This represents the system ID of the source of the link state PDU plus two additional bytes. The first additional byte designates the type of update. 00 represents a non-psuedonode update. 01–FF represents a pseudonode update for that circuit number. The second byte represents the LSP number. This number is attached to the packet when the data is contained in more than one packet.

Lifetime
Indicates the amount of time, in seconds, that router will maintain the LSP.

Sequence #
Indicates the sequence number of the LSP.

Checksum
Indicates the checksum value of the LSP.

Flags Indicates a one-octet value that reflects the flag field of the LSP. The eight bits are broken down as follows:

Bit 8 Indicates the P flag. When set (1), the issuing IS supports the optional Partition Repair function.

Bits 7-4
Indicate the ATT flag. When set (1), the issuing IS is attached to other areas using one of the following: the Default Metric (bit 4), the Delay Metric (bit 5), the Expense Metric (bit 6), or the Error Metric (bit 7).

Bit 3 Indicates the LSPDBOL flag. When set (1), an LSP database overload has occurred. An LSP with this bit set is not used by the decision process to calculate routes to another I through the originating system.

Bits 2-1
Indicate the IS Type flag. When set to the following values, designates the type of IS router, level 1 or level 2.

Value	Description
0	Unused.
1	Bit 1 set. Level 1 IS.
2	Unused.
3	Bits 1 and 2 set. Level 2 IS.

Cost Indicates the cost of routing to that neighbor.

L2-Summary

Use the **l2-summary** command to display a summary of the level 2 link state database.

Syntax:

l2-summary

Example:

```
l2-summary
Link State Database Summary - Level Two

LSP ID               Lifetime   Sequence #   Checksum   Flags   Cost
0000-9310-04F0-0000     33E     12             EF19       3       0
0000-5000-FB06-0000     455      4             2BB1       3      20
0000-5000-FB06-0100     469     12             DE32       3      20

Total Checksum 0
```

The description of the L2-summary output is the same as the l1-summary command.

L1-Update

Use the **l1-update** command to display a link state update for the specified level 1 IS.

Syntax:

l1-update

Example:

```
l1-update
LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F00000

Area Addresses

470005001

Intermediate System Neighbors     Metric      Two Way

0000931004F002                      20           N
0000931004F001                      20           Y

End System Neighbors              Metric

00009310004F0                        *
```

LSP ID
: Indicates the system ID of the source of the link state PDU plus two additional bytes. The first byte designates the type of update. 00 represents a non-pseudonode update. 01–FF represents a pseudonode update. The second byte represents the LSP number. This number is attached to the packet when the data is contained in more than one packet.

Area Addresses
: Indicates the area addresses in which this router is configured to route packets.

Intermediate System Neighbors
: Indicates adjacent neighbor ISs.

Metric
: Indicates the cost to the neighbor IS.

Two Way
: Indicates whether the router is receiving updates from its neighbor.

End System Neighbors
: Indicates any directly connected ESs.

L2-Update

Use the l2-update command to display the link state update for the specified level 2 IS.

Syntax:

l2-update

Example:

```
l2-update
LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F00000

INTERMEDIATE SYSTEM NEIGHBORS    METRIC   TWO WAY
   0000931004F002                  20        N
   0000931004F001                  20        N
   55002000182000                  20        N
```

Intermediate System Neighbors
Indicates other directly connected ISs.

Metric Indicates the cost to the IS.

Two Way
Indicates whether the router is receiving updates from its neighbor.

Ping-1139

Causes the router to send an echo request to a destination and wait for a reply, as recommended in RFC 1139. RFC 1139 specifies this as an OSI function and not as a DECnet function. **Ping-1139** supports short- and long-term echos. Short-term echos use regular CLNP data packets, which makes them transparent to intermediate systems that do not support RFC1139. Long-term echos use PING request/reply packets.

The default data length of the echo request packet is 16 bytes. You can set the data length up to 64 bytes.

Once you enter the **ping-1139** command, echo requests are sent continually until you press any key. At that time, statistics are displayed showing the number of requests transmitted and the number of replies received.

Syntax:

ping-1139

Example:

```
ping-1139
Long-term/Short-term [LONG-TERM]?
Destination NSAP:  []? AA0003000A14
Data Length [16]?

PINGing AA0003000A14

---- PING Statistics ----
 8 requests transmitted, 8 replies received
```

Route

Use the **route** command to display the next hop a packet would take to a specified destination (destnsap).

Syntax:

route *dest-nsap*

Example:

```
route 490002aa0004000e08
Destination System: 0000-9310-04C9
Destination MAC Address: AA00-0400-1408
Interface: 0
```

Destination System
Indicates the system ID of the next hop IS. For a directly connected ES, this will be blank.

Destination MAC Address
Indicates the MAC address of the next hop IS or the directly-connected ES.

Interface
Indicates the interface that a packet would go out over to reach the next hop IS or the directly-connected ES.

Send (Echo Packet)

Use the **send echo packet** command to encode an echo request message in the CLNP packet to the specified destination nsap. During this command, the system does not interact with the OSI monitoring. To verify that the echo request was sent and that an echo reply was received, check the ELS (Event Logging System).

Note: You cannot send an echo packet to yourself. If you try, you will receive an CLNP.004 ELS message.

Syntax:

send

Example:

```
send
Destination NSAP: []?
```

Subnets

Use the **subnets** command to display information on all operational subnets. Subnets that are down or disabled will not be listed.

Syntax:

subnets

Example:

```
subnets
                       L2
 Hdw    Int #  Circ  Only  ES-IS IS-IS  L1DR  L1Pri  L2DR   L2pri  Cost   Ext
 PPP/2 2        3     N     N     Y
 Eth/0 0        1     N     Y     Y      Y     64    N      64     20    N
```

Hdw The type and instance of the network that connects to the subnet.

Int # The router's interface number that connects to the subnet.

Circ The circuit assigned ID for the ISIS protocol.

L2 only
Whether this router is a level 2 router only, Y (yes) or N (no).

ES-IS The ES-IS protocol is enabled on the subnet, Y or N.

IS-IS The IS-IS protocol is enabled on the subnet, Y or N.

L1DR This router is the level 1 designated router for this subnet, Y or N.

L1Pri The subnet’s level 1 priority for becoming the designated router.

L2DR This router is the level 2 designated router for this subnet, Y or N.

L2Pri The LAN subnet’s level 2 priority for becoming the designated router.

Cost The cost of the circuit.

Ext Whether the subnet is operating outside the IS-IS routing domain (external).

Toggle (Alias/No Alias)

Use the **toggle** alias/no alias command to enable or disable the NSAP alias display function for the OSI protocol.

Syntax:

toggle

Example:

```
toggle
Alias substitution is ON
```

Traceroute

Use the **traceroute** command to track the path an OSI packet takes to a destination.

Note: You cannot do a traceroute to yourself or you will receive the following error message:

```
Sorry, can't traceroute to this router.
```

Syntax:

traceroute *address*

Example:

```
traceroute 490002aa0004000e08
Successful trace:

TRACEROUTE 470007: 56 databytes

1          490002aa0004000e08      32ms      5ms       5ms

Destination unreachable response:

Destination unreachable

No response:

1 * * *
2 * * *
```

TRACEROUTE
Displays the destination area address and the size of the packet being sent to that address.

1 The first trace showing the destination’s NSAP and the amount of time it took the packet to arrive at the destination. The packet is traced three times.

Destination unreachable
Indicates that no route to destination is available.

1 * * *

2 * * * Indicates that the router is expecting some form of response from the destination, but the destination is not responding. The router will wait 32 hops before timing out. Go to the ELS and turn on OSI CLNP messages to determine why the host is not responding.

Chapter 12. Using IP Version 6 (IPv6)

This chapter describes how to use IPv6.

IPv6 Overview

IP Version 6 (IPv6) is a new version of the Internet Protocol. It is designed as a successor to IP Version 4 (IPv4). The following list identifies some of the advantages provided by IPv6:

- Large address space

  IPv6 uses a 128-bit address.
- Routing

  Using the large address size, IPv6 provides an hierarchical address scheme which allows you to create a flexible routing hierarchy.
- Ease of configuration

  NDP provides host autoconfiguration.
- Security

  IPv6 makes IP Security mandatory.
- Support for multimedia traffic

  The IPv6 header has priority and flow label fields to accommodate integrated Quality of Service.
- Simplification

  The IPv6 header is fixed and simplified. The router is no longer required to perform fragmentation, simplifying packet processing. In addition, options type data is implemented in extension headers that are only processed by the destination node.

IPv6 Comparison with IPv4

IPv6 includes many changes from IPv4. The most significant changes are:
- Address
- Header format
- Minimum MTU
- Mandatory Path MTU discovery
- Mandatory IP security
- Neighbor Discovery Protocol (NDP)

IPv6 Addressing

IPv6 addressing increases the address from 32 bits to 128 bits. This increase allows more degrees of hierarchy than the basic layers of network, subnet and host.

IPv6 addresses belong to one of three categories:
- Unicast. A packet is delivered to the interface identified by the address.
- Multicast. A packet is sent to all members of the multicast group identified by the address.
- Anycast. A packet is sent to only the nearest member of the group identified by the address.

Broadcast addressing has been replaced by multicast addressing in IPv6.

IPv6 Address Format

The IPv6 address is composed of 128 bits. These bits are written as eight 16-bit integers separated by colons.

Example:

ABCD:1234:0000:1234:5555:FFEE:7777:0123

You can use the following simplifying rules:

- Skip leading zeroes.

  Example:

  ABCD:1234:0:1234:0:FFEE:7777:123
- Inside an address, a set of consecutive, null 16-bit numbers can be replaced by two colons.

  Example:

  ABCD:1234::1234:5555:FFEE:7777:123

  1234::7899

  The double colon can be used only once inside the address.
- When dealing with a mixed environment of IPv4 and IPv6 nodes, you can use the form **x:x:x:x:x:x:d.d.d.d**

  , where the x’s are hexadecimal values of the six high-order 16-bit pieces of the address, and the d’s are the decimal values of the four low-order 8-bit pieces of the address in standard IPv4 representation.

  Example:

  ABCD:1234::1234:5555:FFEE:1.2.3.4

  ::1.2.3.4

Text Representation of Address Prefixes

An IPv6 address prefix is represented by the notation:

IPv6-address/prefix-length

The IPv6 address can use any of the notations listed in “IPv6 Address Format” and the prefix length is a decimal value specifying how many of the leftmost contiguous bits of the address comprise the prefix.

Example:

ABCD:1234::1234:5555:FFEE:1.2.3.4/64

IPv6 Header Format

The IPv6 header has a total of 8 fields, eliminating some IPv4 fields such as checksum and fragmentation.

IPv6 Minimum MTU

The minimum MTU for IPv6 is 1280 bytes. You cannot enable IPv6 on an interface with an MTU less than 1280 bytes.

IPv6 Mandatory Path MTU Discovery

Path MTU Discovery is a protocol that allows a host to determine the maximum size packet that will successfully traverse a path to a destination without fragmentation. As packets are generated and sent from the host, the MTU of the particular output interface that the packet will be transmitted to is available.

If the packet will fit on the output interface, either as a whole or in fragments, it is transmitted. If a router in the path needs to forward that packet onto a net with a smaller MTU than the packet size, the packet will be dropped and an ICMP message will be sent to the originator of the packet indicating the packet size that is necessary to fit onto the output net of the intermediate router. The host receiving this message will adjust the size of subsequent packets forwarded on the path. This process may occur multiple times before the packet reaches its final destination. Once the packet reaches its destination, subsequent packets should not be dropped because their packet size being too large.

Because the route can change dynamically, the path MTU may increase and will need adjustment in the host node. Learned path MTUs are aged and the Path MTU Discovery process re-occurs. This allows the transmitted packet size to react to the dynamic nature of routes through the network.

Path MTU Discovery is mandatory because fragmentation is not allowed on transit routers.

If the device is acting as a transit router, it will not forward packets that are larger than the output net’s MTU. It will generate an ICMP Packet Too Big message back to the source of the packet.

The **enable path-mtu-discovery** command at the `IPv6 Config>` prompt can be used to enable or disable path MTU discovery. Path MTU discovery is enabled by default.

Use the **set path-mtu-aging-timer** command at the `IPv6 Config>` prompt to specify the aging time for path MTUs that have been determined.

IPv6 Mandatory Security

An IPv6 node must support IP security. IP security can be enabled or disabled. See “Using IP Security” and “Configuring and Monitoring IP Security” in the *Using and Configuring Features* for additional information about IP security.

1. Use the **add packet** command at the `IPv6 Config>` prompt to add a packet filter.
2. Use the **update packet** command at the `IPv6 Config>` prompt to update the packet filter.
3. Use the **add access** command at the `Packet-filter 'filter_name' Config>` prompt to add access controls.
4. Use the **set acc on** command at the `IPv6 Config>` prompt to enable access control.

IPv6 Neighbor Discovery Protocol (NDP)

IPv6 uses NDP to perform autoconfiguration. NDP allows IPv6 nodes on the same link to discover each other's presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors.

Router and Prefix Discovery

Hosts use Router Discovery to discover routers that reside on an attached link. Each router periodically multicasts a Router Advertisement packet, if configured, announcing its availability. Router advertisements contain a list of prefixes used for on-link determination and autonomous address configuration. Hosts can use the advertised on-link prefixes to determine when a packet's destination is on the link or beyond a router.

Address Autoconfiguration

Router advertisements allow routers to inform host how to perform address autoconfiguration. Routers can specify whether hosts use stateful or autonomous (stateless) address configuration.

Address Resolution

Routers accomplish address resolution by multicasting a neighbor solicitation message that asks the target node to return its link-layer address. The link-layer address is returned in a unicast neighbor advertisement. By including its link-layer address in the neighbor solicitation message, a single request-response pair of messages, the message initiator and the target can determine each other's link-layer addresses.

Neighbor Unreachability Detection

NDP can detect the failure of a neighbor or the failure of the forward path to the neighbor. When no positive confirmation has been received from a neighbor for a time interval, the node actively probes the neighbor using unicast neighbor solicitation messages to verify that the forward path is still working.

Redirect

If the source address of the packet and the next hop are on the same network, a router may send a redirect message informing the sender that the next hop is a neighbor.

Use the **p ndp** command at the `Config>` prompt to configure NDP parameters.

IPv6 over IPv4 Tunneling

IPv6 over IPv4 tunneling allows you to migrate from IPv4 networks to IPv6 networks without the need to simultaneously upgrade all equipment to IPv6 support. IPv6 over IPv4 tunneling allows IPv6 frames to cross an IPv4 network and reach an IPv6 destination. The IPv6 frame is encapsulated in an IPv4 frame and this encapsulated frame is forwarded through the IPv4 network to a specific IPv4 destination, called the endpoint of the tunnel. At this endpoint, the packet is decapsulated and forwarded to the final IPv6 destination.

Adding a configured tunnel causes a virtual interface to be added. That virtual interface is then treated as a normal interface by IPv6 and may be used by RIP for route establishment.

Use the **add tunnel** command at the `IPv6 Config>` prompt to add an IPv6 over IPv4 tunnel.

Protocol Independent Multicast (PIM)

| See “Using PIM” on page 429 for usage information about the PIM protocol.

Chapter 13. Configuring and Monitoring IPv6

This chapter describes how to use the IPv6 configuration and operating commands and includes the following sections:

Accessing the IPv6 Configuration Environment

Use the following procedure to access the IPv6 configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to *The OPCON Process and Commands* in the Access Integration Services Software User’s Guide.) For example:

   ```
   * talk 6
   Config>
   ```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the CONFIG prompt, enter the **p ipv6** command to get to the `IPv6 Config>` prompt.

IPv6 Configuration Commands

To configure IPv6, enter the commands at the `IPv6 Config>` prompt.

Table 106. IPv6 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 xxviii.
add	Adds an address, leaked-routes, packet-filter, route, or tunnel.
change	Changes an address, leaked routes, packet-filter, route, or tunnel.
delete	Deletes an address, leaked routes, packet filter, route, or tunnel.
disable	Disables icmp redirects, packet filter, or path MTU discovery.
enable	Enables ICMP redirects, packet filters, or path MTU discovery.
list	Lists the configuration.
move	Moves access control.
set	Sets configuration values associated with automatic tunnels, fast forwarding path cache buffer size, default gateway, MLD, path MTU aging timer, packet reassembly buffer size, routing table size, router id, and router time to live.
update	Updates the packet filter.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page xxviii.

Add

Use the **add** command to add an IPv6 address, leaked routes, packet filters, routes, or IPv6 over IPv4 tunnels.

add acess-control
address *n*et address prefix
leaked-routes*destination*

packet-filter *name interface*
route *destination mask gateway cost ...*
tunnel *destination prefix raddress locaddress cost ttl fragmentation*

Example:

```
IPv6 config>add address
Which net is this address for [0]? 5
New address []? 1::2
Prefix length must between 8 and 128 [128]?

IPv6 config>add leaked
IPV4 destination []? 1.2.3.4
Address mask [255.0.0.0]? 255.255.255.255

IPv6 config>add packet-filter
Packet-filter name []?  pktf01
Filter incoming or outgoing traffic [IN]
Which interface is this filter for [0]? 3

IPv6 config>add route
IPv6 destination []? 8::9
Prefix length must between 8 and 128 [8]? 128
Via gateway 1 at []? 1::2
Cost [1]?
Via gateway 2 at []? 2::3
Cost [1]? 1000
Via gateway 3 at []? 3::4
Cost [1]? 10000
Via gateway 4 at []? 4::5
Cost [1]? 10
IPv6 config>add tunnel
Add a static route through this tunnel? [Yes[:
IPv6 destination network []? 3::4
Prefix length must between 0 and 128 [64]? 128
IPV4 tunnel remote address []?1.2.3.4
IPV4 tunnel local address []? 2.3.40.0
Cost [1]?
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):
```

access-control
Adds access control.

access control type
Indicates what is done with packets that match the access control rule parameters.

E Exclusive; matching packets are discarded.

I Inclusive; matching packets are processed further by the router.

Internet source
Source Internet address.

Valid Values: Any valid Internet address

Default Values: None

Source Prefix length
Specifies the prefix length for the Internet source address.

Valid Values: 0 - 128

Default Values: 128

Internet destination
Destination Internet address.

Valid Values: Any valid Internet address

Default Value: None

Destination Prefix length
Specifies the prefix length for the Internet destination address.

Valid Values: 0 - 128

Default Values: 128

Starting protocol number
Specifies the starting protocol number for a range of protocol numbers. Enter a value of *0* to select all protocols.

Some common protocol numbers are:
1 for ICMP
6 for TCP
17 for UDP
89 for OSPF
50 for ESP-Encryption
51 for AH-Encryption

Valid Values: 0 to 255

Default Values: 0

Ending protocol number
Specifies the ending protocol number for a range of protocol numbers. Enter a value of *0* to select all protocols.

Some common protocol numbers are:
1 for ICMP
6 for TCP
17 for UDP
89 for OSPF
50 for ESP-Encryption
51 for AH-Encryption

Valid Values: 0 to 255

Default Values: the value specified as the **starting protocol number**

Starting destination port number
Specifies the starting port number for a range of TCP/UDP destination port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17.

Some commonly used port numbers are:
21 for FTP
23 for Telnet
25 for SMTP
513 for rlogin
520 for RIP for IPv4
521 for RIP6 for IPv6

Valid Values: 0 - 65535

Default Value: 0

Ending destination port number

Specifies the ending port number for a range of TCP/UDP destination port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17.

Some commonly used port numbers are:

21 for FTP
23 for Telnet
25 for SMTP
513 for rlogin
520 for RIP for IPv4
521 for RIP6 for IPv6

Valid Values: 0 - 65535

Default Value: the value specified as the **starting destination port number**

Starting source port number

Specifies the starting port number for a range of TCP/UDP source port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17. See the description of **starting destination port number** for a list of commonly used TCP/UDP port numbers.

Valid Values: 0 - 65535

Default Value: 0

Ending source port number

Specifies the ending port number for a range of TCP/UDP source port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17. See the description of **starting destination port number** for a list of commonly used TCP/UDP port numbers.

Valid Values: 0 - 65535

Default Value: the value specified as the **starting source port number**

address

Adds an IPv6 address.

Which net is this address for

Specifies the net to which the IPv6 address is to be added.

Valid Values: A numeric value identifying a network interface

Default Value: 0

New address

Specifies the new IPv6 address to be added.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length
Decimal value specifying how many of the leftmost contiguous bits of the address comprise the prefix.

Valid Values: 8 - 128

Default Value: 128

leaked-routes
Adds a leaked route.

IPV4 destination
Specifies the IPv6 address of the destination for the leaked route.

Valid Values: Any valid IPv6 address

Default Value: None

packet-filter
Adds a packet-filter.

packet-filter name
Specifies an alphanumeric name used to identify the packet filter.

Valid Values: Any alphanumeric character string up to 16 characters in length

Default Value: None

Filter incoming or outgoing traffic?
Specifies whether you want to filter incoming or outgoing traffic.

Valid Values: OUT or IN

Default Value: IN

which interface is this filter for
Specifies the network interface number to which the packet filter is to be added.

Valid Values: A numeric value identifying any interface for which IPv6 is a valid protocol, or “a”, which specifies that this filter is for the automatic tunnel.

Default Value: 0

route Adds a route.

IPv6 destination
Specifies the IPv6 address of the target for the route.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length
Specifies the mask to be applied to the destination address.

Valid Values: 8 - 128 (0 is allowed if the IPv6 destination is 0::0)

Default Value: 8

Via gateway 1
Specifies the IPv6 address of the gateway 1.

Valid Values: Any valid IPv6 address

Default Value: None

Cost Specifies the cost of this route.

Valid Values: A numeric value

Default Value: 1

Via gateway 2
Specifies the IPv6 address of the gateway 2.

Valid Values: Any valid IPv6 address

Default Value: None

Cost Specifies the cost of this route.

Valid Values: A numeric value

Default Value: 1

Via gateway 3
Specifies the IPv6 address of the gateway 3.

Valid Values: Any valid IPv6 address

Default Value: None

Cost Specifies the cost of this route.

Valid Values: A numeric value

Default Value: 1

Via gateway 4
Specifies the IPv6 address of the gateway 4.

Valid Values: Any valid IPv6 address

Default Value: None

Cost Specifies the cost of this route.

Valid Values: A numeric value

Default Value: 1

tunnel Adds a tunnel.

Add a static route through this tunnel?
Specifies whether or not the tunnel will have a static route defined.

Valid Values: Yes or No

Default Value: Yes

IPv6 destination network
Specifies the IPv6 address of the destination network that will be reached by the tunnel.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length
Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.

Valid Values: 8 - 128

Default Value: 64

IPv4 tunnel remote address
Specifies the IPv4 address for the IPv6 frames passed through the tunnel.

Valid Values: Any valid IP (32-bit) address

Default Value: None

IPv4 tunnel local address
Specifies the IPv4 source address for the IPv6 frames passed through the tunnel.

Valid Values: Any valid IP (32-bit) address

Default Value: None

Cost
Specifies the cost associated with the tunnel which will be used during route lookups to find the best route to the destination.

Valid Values: 1 - 255

Default Value: 1

TTL value
Specifies the time-to-live value used in frames encapsulated for this tunnel

Valid Values: Any numeric value in the range of 1 - 255

Default Value: 64

Allow fragmentation in the tunnel?
Specifies whether the fragmentation in the tunnel will be allowed. Specifying *yes* allows fragmentation in the tunnel in case the IPv4 network that the tunnel is using does not provide enough information to allow the device to return a “Packet Too Big” message to the IPv6 host.

Valid Values: yes or no

Default Value: no

Change

Use the **change** command to add an access control record, IPv6 address, leaked routes, packet filters, routes, or tunnels.

Syntax:

change	access-control *index*
	address *net address prefix*
	leaked-routes*destination*
	packet-filter *name interface*
	route *destination mask gateway cost ...*
	tunnel *destination prefix raddress locaddress cost ttl fragmentation*

access-control
Changes access control configuration.

address
Changes an address.

leaked-routes
Changes a leaked route configuration.

packet-filter
Changes a packet filter configuration.

route Changes a route configuration.

tunnel Changes a tunnel configuration.

See "Add" on page 391 for a description of the parameters associated with the **change** command.

Delete

Use the **delete** command to remove an access control record, address, leaked-routes, packet filter, route or tunnel.

Syntax:

delete access-control *index*
address *address*
leaked-routes *destination*
packet-filter *name*
route *destination mask gateway*
tunnel *tunnel#*

Disable

Use the **disable** command to disable ICMP redirect, packet filters, and path MTU discovery.

Syntax:

disable icmp-redirect *address*
packet-filter *packet-filter-name*
path-mtu-discovery

icmp-redirect
Disables ICMP redirects.

packet-filter
Disables a packet-filter.

packet-filter name
Specifies the name of the packet filter to be disabled.

Valid Values: Any configured packet filter

Default Value: None

path-mtu-discovery
Disables Path MTU Discovery.

Enable

Use the **enable** command to enable ICMP redirects, packet filters, or path MTU discovery.

Syntax:

enable icmp-redirect *address*
packet-filter *packet-filter-name*
path-mtu-discovery

icmp-redirect
Enables ICMP redirects.

interface address
Specifies the interface address.

Valid Values: Any valid IPv6 address

Default Value: Null (specifies all addresses)

packet-filter
Enables a packet-filter.

packet-filter name
Specifies the name of the packet-filter to be enabled. This name is configured using the **add packet-filter** command.

Valid Values: Any valid IPv6 address

Default Value: None

path-mtu-discovery
Enables Path MTU Discovery, a protocol that allows a host node to determine the maximum size packet that will traverse a path to a destination without fragmentation.

List

Use the **list** command to display the IPv6 configuration.

Syntax:

list all
access-control
addresses
icmp-redirect
leaked-routes
mld
packet-filter
routes
sizes
tunnels

Example:

```
IPv6 config>list all
Interface addresses
IPv6 addresses for each interface:
   intf  0                                    IP disabled on this interface
   intf  1                                    IP disabled on this interface
   intf  2                                    IP disabled on this interface
   intf  3                                    IP disabled on this interface
   intf  4                                    IP disabled on this interface
   intf  5   1234:1234:1234:1234:5234:6234:7234:8234/128
             1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8

Routing

route to: 1234::1223/128
     via: 1234:0:9::8                            cost: 100
     via: 1234:0:9:8:8:7:6:8                     cost: 232
     via: 1:2:3:4:5:6:7:8                        cost: 1
     via: 8:7:6:5:4:3:2:1                        cost: 1
route to: ::/0
     via: 1::8                                   cost: 100
route to: 2::8:9/8
     via: 1::8                                   cost: 1
```

```
Path MTU Discovery:  disabled
Path MTU Aging Timer:  10 minutes


Access Control is:   enabled

IPv6 config>list addresses
IPv6 addresses for each interface:
   intf  0                                     IP disabled on this interface
   intf  1                                     IP disabled on this interface
   intf  2                                     IP disabled on this interface
   intf  3                                     IP disabled on this interface
   intf  4                                     IP disabled on this interface
   intf  5   1234:1234:1234:1234:5234:6234:7234:8234/128
             1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8
IPv6 config>list icmp-redirect
ICMP Redirect generation for IP interface:
   intf  0                                     IP disabled on this interface
   intf  1                                     IP disabled on this interface
   intf  2                                     IP disabled on this interface
   intf  3                                     IP disabled on this interface
   intf  4                                     IP disabled on this interface
   intf  5   1234:1234:1234:1234:5234:6234:7234:8234/128 ICMP Redirect enabled
                                     1223::7:1234/8 ICMP Redirect enabled
   intf  6                                     IP disabled on this interface
   intf  7                                     IP disabled on this interface


IPv6 config>list leaked-routes
#  IPv4 Address     Mask
IPv6 config>list mld
Net      Query Interval      Response Interval      Leave Query Interval
             (secs)                (secs)                  (secs)
---      --------------      -----------------      --------------------

 5           125                   10                       1

IPv6 config>list packet-filter

List of packet-filter records:

Name              Interface   State
packet01          0           On
pack01            5           On
Access Control is: enabled
IPv6 config>list routes

route to: 1234::1223/128
     via: 1234:0:9::8                         cost: 100
     via: 1234:0:9:8:8:7:6:8                  cost: 232
     via: 1:2:3:4:5:6:7:8                     cost: 1
     via: 8:7:6:5:4:3:2:1                     cost: 1
route to: ::/0
     via: 1::8                                cost: 100
route to: 2::8:9/8
     via: 1::8                                cost: 1

IPv6 config>list sizes

Routing table size: 768 nets (79872 bytes)
Reassembly buffer size: 12000 bytes
Routing cache size: 64 entries
```

```
Time to live: 64
Path MTU aging timer: 10

IPv6 config>list tunnel
Tun#  Remote Endpoint  Local Endpoint   Frag Allowed   TTL  Cost Net#  IPv6 Address/Prefix
 1    1.2.3.4          2.3.4.5               No        100    100  7   1:2:3:4:5:6:7:8/128
IPv6 config>
```

Move

Use the **move** command to change the order of configured access control records.

Syntax:

move access-control

Index of control to move
Select the index number of the access control record you want to move.

Move record AFTER record number
Select the index number of the access control record you want this record to follow.

Are you sure that this is what you want to do
Allows you to confirm that the move instruction is correct.

Set

Use the **set** command to set configuration parameters.

Syntax:

set
access-control
automatic-tunnel-parameters *ttl fragmentation hopcount*
cache-size *#entries*
default *...*
internal-ip-address
mld *...*
path-mtu-aging-timer
reassembly-size
router-id
routing *#nets*
ttl

Example:

```
IPv6 config>set au
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):

IPv6 config>set ca
number of cache entries [64]?

IPv6 config>set mld query-interval
Network interface [0]? 5
New Query Interval (in secs) [125]?

IPv6 config>set mld response-interval
Network interface [0]? 5
New Response Interval (in secs) [10]?

IPv6 config>set mld robust
Network interface [0]? 5
New Robustness Variable [2]?
```

```
IPv6 config>set mld leave
Network interface [0]?
New Leave Interval (in secs) [1]?
IPv6 config>?
```

access-control
Specifies whether access control is enabled or disabled.

Valid Values: on or off

Default Value: off

automatic-tunnel-parameters
Specifies the tunnel parameter values for automatic tunnels that flow through the router.

ttl value
Specifies the time-to-live value for the frames encapsulated for the tunnel.

Valid Values:

Default Value: 64

allow fragmentation in tunnel?
Specifies whether the fragmentation in the tunnel will be allowed. Specifying *yes* allows fragmentation in the tunnel in case the IPv4 network that the tunnel is using does not provide enough information to allow the device to return a “Packet Too Big” message to the IPv6 host.

Valid Values: yes or no

Default Value: no

hop count
Specifies the hop count to be used on automatically tunnelled packets.

Valid Values: 1 - 255

Default Value: 64

cache-size
Specifies the buffer size for the fast forwarding path cache.

number of cache entries
Specifies the number of entries in the fast forwarding path cache.

Valid Values: 64 - 10 000

Default Value: 64

default network-gateway

default gateway

Valid Values: Any valid IPv6 address

Default Value: none

gateway’s cost
Specifies the cost associated with this gateway.

Valid Values: 1 - 255

Default Value: 1

default subnet-gateway

for which subnetted network

Valid Values: Any valid IPv6 address

Default Value: none

default gateway

Valid Values: Any valid IPv6 address

Default Value: none

gateway's cost
Specifies the cost associated with this gateway.

Valid Values: 1 - 255

Default Value: 1

internal-ip-address

Valid Values: Any valid IPv6 address

Default Value: None

mld

query-interval

network interface

Valid Values: Any valid network interface number

Default Value: 0

new query interval (in secs)

Valid Values: 1 - 3600

Default Value: 125

response-interval

network interface

Valid Values: Any valid network interface number

Default Value: 0

new response interval (in secs)

Valid Values: 1 - 60

Default Value: 10

robustness-variable

network interface

Valid Values: Any valid network interface number

Default Value: 0

new robustness variable

Valid Values: 2 - 10

Default Value: 2

leave-interval

network interface

Valid Values: Any valid network interface number

Default Value: 0

new leave interval (in secs)

Valid Values: 1 - 60

Default Value: 1

path-mtu-aging-timer
Specifies the aging time in minutes for path MTUs that have been determined using path MTU discovery.

Valid Values: 10 - 60 minutes, where 0 = disable

Default Value: 10

reassembly-size
Specifies the size of the reassembly buffers used for processing the fragment header.

Valid Values: 2048 - 65536

Default Value: 12000

router-id
Specifies the IPv6 address of the router.

Valid Values: Any valid IPv6 address

Default Value: None

routing table-size

number of nets

Valid Values: 64 - 65 535

Default Value: 768

ttl Specifies the IPv6 time-to-live value.

Valid Values:

Default Value: 64

Update

Use the **update** command to update the packet filter

Syntax:
update packet-filter

packet-filter
Use this command to access the `Packet-filter 'xx' Config>` command prompt from which you can configure packet-filters.

Update Packet-filter Commands

Table 107. Update Packet-filter 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 xxviii.
Add	Adds access control.
Change	Changes access control.
Delete	Deletes access control.

Table 107. Update Packet-filter Configuration Command Summary (continued)

Command	Function
Move	Reorders the access control list applied to the packet filter.
List	
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Add

Use the **update packet-filter add** command to add an access control list.

Syntax:

add access-control *type sourceaddr sourceprefix destaddr destprefix*

access-control

Adds an access-control item to the access control list.

Type Specifies whether the access control is inclusive or exclusive.

Valid Values: I or E

Default Value: I

Internet source

Specifies the IPv6 address of the packet source.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length

Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.

Valid Values: 0- 128

Default Value: 128

Internet destination

Specifies the IPv6 address of the packet destination.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length

Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.

Valid Values: 0- 128

Default Value: 128

Starting protocol number

Specifies the starting protocol number for a range of protocol numbers. Enter a value of *0* to select all protocols.

Some common protocol numbers are:

1 for ICMP
6 for TCP
17 for UDP
89 for OSPF
50 for ESP-Encryption
51 for AH-Encryption

Valid Values: 0 to 255

Default Values: 0

Ending protocol number

Specifies the ending protocol number for a range of protocol numbers. Enter a value of *0* to select all protocols.

Some common protocol numbers are:
1 for ICMP
6 for TCP
17 for UDP
89 for OSPF
50 for ESP-Encryption
51 for AH-Encryption

Valid Values: 0 to 255

Default Values: the value specified as the **starting protocol number**

Starting destination port number

Specifies the starting port number for a range of TCP/UDP destination port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17.

Some commonly used port numbers are:
21 for FTP
23 for Telnet
25 for SMTP
513 for rlogin
520 for RIP

Valid Values: 0 - 65535

Default Value: 0

Ending destination port number

Specifies the ending port number for a range of TCP/UDP destination port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17.

Some commonly used port numbers are:
21 for FTP
23 for Telnet
25 for SMTP
513 for rlogin
520 for RIP

Valid Values: 0 - 65535

Default Value: the value specified as the **starting destination port number**

Starting source port number

Specifies the starting port number for a range of TCP/UDP source port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17. See the description of **starting destination port number** for a list of commonly used TCP/UDP port numbers.

Valid Values: 0 - 65535

Default Value: 0

Ending source port number
Specifies the ending port number for a range of TCP/UDP source port numbers. These parameters are valid only if the range of protocol numbers includes 6 (for TCP) or 17 (for UDP). These parameters are ignored for packets in which the protocol number is not 6 or 17. See the description of **starting destination port number** for a list of commonly used TCP/UDP port numbers.

Valid Values: 0 - 65535

Default Value: the value specified as the **starting source port number**

Change

Use the **update packet-filter change** command to change access control.

Syntax:

change	access-control *type sourceaddr sourceprefix destaddr destprefix*

access-control
Changes an access-control item.

Type Specifies whether the access control item is inclusive or used to identify packets to be secured..

Valid Values: I or S

Default Value: I

Internet source
Specifies the IPv6 address of the packet source.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length
Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.

Valid Values: 0- 128

Default Value: 128

Internet destination
Specifies the IPv6 address of the packet destination.

Valid Values: Any valid IPv6 address

Default Value: None

Prefix length
Decimal value specifying how many of the leftmost contiguous bits of the IPv6 address comprise the prefix.

Valid Values: 0- 128

Default Value: 128

Delete

Use the **update packet-filter delete** command to remove an access control item from the access control list.

Syntax:

delete access-control *index#*

access-control
Deletes access-control.

index of access control to be deleted
Specifies the index of the access control configuration to be removed.

Valid Values: 1 to the number of access control records defined for this packet filter

Default Value: 1

Move

Use the **update packet-filter move** command to re-order the access control list applied to the packet-filter.

Syntax:

move access-control *index# after#*

access-control

index of control to move

Valid Values: 1 to the number of access control records defined for this packet filter

Default Value: 1

Move record after record number
Specifies target location in the access-control list. You will be asked to verify that this is the action you want to configure.

Valid Values: 1 to the number of access control records defined for this packet filter

Default Value: 0

List

Use the **update packet-filter list** command to display the access control list configuration.

Syntax:

list access-controls

Example:

```
Packet-filter 'x' Config> li acc
Access control is : enabled
List of access control records:

1   Type=IS   Source=2001:1::6101/128
              Dest=  2001:1::86/128
              Tid=3

2   Type=I    Source=::/0
```

```
                Dest=::/0

Packet-filter 'x' Config>
```

Accessing the IPv6 Monitoring Environment

Use the following procedure to access the IPv6 monitoring commands. This process gives you access to the IPv6 monitoring process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to the chapter entitled "The OPCON Process and Commands" in the *Access Integration Services Software User's Guide*.) For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the + prompt, enter the **p ipv6** command to get you to the `ipv6>` prompt.

   Example:

   ```
   + p ipv6
   ipv6>
   ```

IPv6 Monitoring Commands

This section describes the IPv6 monitoring commands.

Table 108. IPv6 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 xxviii.
access-control	Displays access control records.
cache	Displays cache entries.
counters	Display counters
dump routing tables	Dumps the configured routing tables.
interface addresses	Displays the addresses defined on the interface.
internal address	Displays the specified internal address.
mcast	Displays a list of registered multicast addresses.
mld	Displays MLD counters or parameters.
reset	Resets the IPv6 interface.
route	
sizes	Displays buffer sizes.
sniffer	Sets various trace options.
static routes	Displays static routes.
packet-filter	Displays configured packet filters.
path-mtu	
ping6	Activates Ping.
traceroute6	Dynamically traces a route.
tunnels	Displays configured tunnels.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Access-control

Use the **access-control** command to monitor configured access control records.

Syntax:
access-control

Cache

Use the **cache** command to display

Syntax:
cache

Example:

```
IPv6>cache
Destination                                  Usage        Next hop
```

Counters

Use the **counters** command to display the status of counters.

Syntax:
counters

Example:

```
IPv6>counters
Routing errors
Count  Type
   0   Routing table overflow
   0   Net unreachable
   0   Bad subnet number
   0   Bad net number
   0   Unhandled broadcast
   0   Unhandled anycast
   0   Unhandled directed broadcast
   0   Attempted forward of LL broadcast
   0
   0   None

Packets discarded through filter  0
IP multicasts accepted:           0

IP input packet overflows
    Net   Count
   TKR/0  0
   TKR/1  0
    FR/0  0
   PPP/0  0
  IP64/0  0
```

Dump routing tables

Use the **dump** command to display the configured routing tables.

Syntax:
dump

Example:

```
IPv6>dump
Type   Dest net/Prefix            Cost     Age       Next hop(s)

Stat*  1:2:3:4:5:6:7:8/128              100 30        IP64/0

IPv6 Routing table size: 768 nets (79872 bytes), 1 nets known
                      0 nets hidden, 0 nets deleted, 0 nets inactive
                      0 routes used internally, 767 routes free
```

Interface addresses

Use the **interface** command to display addresses configured on the interface.

Syntax:
interface

Example:

```
IPv6>interface

                         IPV6  IPV6    ICMP    IPV6
Interface    Net:Status  State MTU     redir   Address/Prefixlen
   Eth/0      0 : DWN    DWN   1500    Enabled 2003:6:14:1::610/64
   Eth/1      1 : DWN    DWN   1500    Enabled 2003:7:6:1::610/64
  IP64/0      3 : UP     UP    2048    Enabled FE80::14FF:FE80:3/64
```

Internal address

Use the **internal** command to display the specified internal address.

Syntax:
internal

Mcast

Use the **mcast** command to display configured multicast addresses.

Syntax:
mcast

Example:

```
IPv6>mcast
List of IPV6 registered multicast addresses



 Interface: Eth/0:

      Address/Ref_Cnt
      FF02::1/1
      FF02::2/1
      FF02::1:FF00:610/1
      FF02::1:FF02:6200/1
      FF02::9/1
```

Mld

Use the **mld** command to display configured.

Syntax:
mld counters

parameters

Example:

```
IPv6>mld counters
Net      Querier      Polls Sent      Polls Rcvd      Reports Rcvd
---      -------      ----------      ----------      ------------

IPv6>mld parameters
Net   Robustness    Query Interval     Response Interval     Leave Query Interval
      Variable      (secs)               (secs)                  (secs)
---   ----------    --------------     -----------------     --------------------

IPv6>
```

Reset

Use the **reset** command to dynamically reset the IPv6 interface.

Syntax:
reset ipv6

Example:

```
IPv6>reset ipv6
```

Route

Use the **route** command to show the route to the IPv6 address.

Syntax:
route *address*

Example:

```
IPv6>route 6::9
IPv6>
```

Sizes

Use the **sizes** command to display configured buffer sizes.

Syntax:
sizes

Example:

```
IPv6>sizes
      Routing table size:            768
        Table entries used:            3
        Reassembly buffer size:        12000
        Largest reassembled pkt:       0
        Size of routing cache:         64
        # cache entries in use:        0

IPv6>
```

Sniffer

Use the **sniffer** command to set various trace options.

Syntax:
sniffer trace command

Choose the **trace command** from this list:

1 List current traces

2 Trace source address

3 Trace destination address

4 Trace protocol

5 Trace TCP source port

6 Trace TCP destination port

7 Trace UDP source port

8 Trace UDP destination port

9 Clear trace

10 Exit

Static routes

Use the **static** command to display configured static routes.

Syntax:
static

Example:

```
IPv6>static
Net/Mask_len                            Cost  Next hop
1234::1223/128    100    1234:0:9::8 PPP/0
                                232    1234:0:9:8:8:7:6:8 PPP/0
8::9                                     128  N/A   filter

IPv6>
```

Packet-filter

Use the **packet-filter** command to display a summary of configured packet filters.

Syntax:
packet-filter

Example:

```
IPv6>pac
Name               Dir  Intf  State  #Access-Controls
packet01           Out  0     On     0
pack01             Out  5     On     2
IPv6>
```

Path-mtu

Use the **path-mtu** command to show the paths that have been identified as having an MTU that is less than the size of a packet sent along that path.

Syntax:
path-mtu

Example:

Ping6

Use the **ping6** command to ping an IPv6 address.

Syntax:
ping6

Example:

```
IPv6>ping
Destination IPv6 address [::]? 8::9
Source IPv6 Address [1::8]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
PING6 1::8 -> 8::9: 56 data bytes, ttl=64, every 1 sec.

----8::9 PING6 Statistics----
36 packets transmitted, 36 packets received
```

Destination IPv6 address

Valid Values: Any valid IPv6 address

Default Value: None

Source IPv6 address

Valid Values: Any valid IPv6 address

Default Value: None

Ping data size in bytes

Valid Values: 0 to size of global buffer

Default Value: 56

Ping ttl
Specifies the time-to-live for the ping.

Valid Values: 1 - 255

Default Value: 64

Ping rate in seconds
Specifies the ping frequency.

Valid Values: 1 - 60

Default Value: 1

Traceroute6

Use the **traceroute6** command to dynamically trace a route.

Syntax:
traceroute6 ...

Example:

```
IPv6>traceroute6
Destination IPv6 address []? 7::8
Source IPv6 address []? 6::9
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
```

```
Maximum TTL [32]?
TRACEROUTE6 7::8: 56 data bytes
 1 * * * *
IPv6>
```

Destination IPv6 address

Valid Values: Any valid IPv6 address

Default Value: None

Source IPv6 address

Valid Values: Any valid IPv6 address

Default Value: None

Data size in bytes

Valid Values: 0 to size of global buffer

Default Value: 56

Number of probes per hop

Valid Values: 1 - 10

Default Value: 3

Wait time between retries in seconds

Valid Values: 1 - 60

Default Value: 3

Maximum ttl

Valid Values: 1 - 255

Default Value: 32

Tunnels

Use the **tunnels** command to display configured tunnels.

Syntax:
tunnels

Example:

```
IPv6>tunnels
                   Configured Tunnels
Tun#  Remote Endpoint  Local Endpoint  Frag Allowed  TTL  MTU  Net#  IPv6 Address/Prefix
 1    1.2.3.4          2.3.4.5               No       100   2048    7   1:2:3:4:5:6:7:8/128

                   Automatic Tunnels
Tun#  Remote Endpoint  Frag Allowed   TTL    MTU
IPv6>
```

IPv6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

IP Version 6 (IPv6) supports the CONFIG (Talk 6) **delete interface** command with no restrictions.

GWCON (Talk 5) Activate Interface

IPv6 supports the GWCON (Talk 5) **activate interface** command with the following consideration:

If IPv6 was not configured before, you need to reboot.

All IPv6 interface-specific commands are supported by the GWCON (Talk 5) **activate interface** command.

GWCON (Talk 5) Reset Interface

IPv6 supports the GWCON (Talk 5) **reset interface** command with the following considerations:

- If IPv6 was not configured before, you need to reboot.
- If memory allocation fails, you need to reboot.

All IPv6 interface-specific commands are supported by the GWCON (Talk 5) **reset interface** command.

GWCON (Talk 5) Component Reset Commands

IPv6 supports the following IPv6-specific GWCON (Talk 5) **reset** commands:

GWCON, Protocol IPv6, Reset IPv6 Command

Description:
Rereads the SRAM and reinitializes IPv6. Also resets RIP6, NDP6, and PIM6.

Network Effect:
None.

Limitations:
None.

All IPv6 configuration changes are automatically activated except the following:

Commands whose changes are not activated by the GWCON, protocol ipv6, reset ipv6 command
CONFIG, protocol ipv6, set routing table-size
CONFIG, protocol ipv6, set reassembly-size
CONFIG, protocol ipv6, set cache-size

CONFIG (Talk 6) Immediate Change Commands

IPv6 supports the following CONFIG commands that immediately change the operational state of the device. These changes are saved and are preserved if the device is reloaded, restarted, or you execute a dynamically reconfigurable command.

Commands
CONFIG, protocol ipv6, add route
CONFIG, protocol ipv6, delete route
CONFIG, protocol ipv6, change route
CONFIG, protocol ipv6, enable icmp-redirect
CONFIG, protocol ipv6, disable icmp-redirect

CONFIG, protocol ipv6, set access-control
CONFIG, protocol ipv6, set ttl
CONFIG, protocol ipv6, set path-mtu-aging-timer

Chapter 14. Configuring and Monitoring Neighbor Discovery Protocol (NDP)

Configuration for NDP is done for each interface. This chapter describes how to use the NDP configuration and operating commands and includes the following sections:

Accessing the NDP Configuration Environment

Use the following procedure to access the NDP configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to *The OPCON Process and Commands* in the Access Integration Services Software User's Guide.) For example:

   ```
   * talk 6
   Config>
   ```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the CONFIG prompt, enter the **p ndp** command to get to the `NDP6 Config>` prompt.

NDP Configuration Commands

To configure NDP, enter the commands at the `NDP6 Config>` prompt.

Table 109. NDP 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 xxviii.
add	Adds a router advertisement or parameters.
change	Changes a router advertisement or parameters.
delete	Deletes a router advertisement or parameters.
disable	Disables router advertisement.
enable	Enables router advertisement.
list	Lists the configuration.
set	Sets the DHCP Hop Count.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Add

Use the **add** command to add a router advertisement.

add ra *...*
dhcp-server

ra Adds a router advertisement.

add router advertisement on which interface
Specifies the interface to which the router advertisement is to be added.

Valid Values: A numeric value identifying a network interface

Default Value: 0

Managed address configuration (stateful)
Specifies whether hosts use the administered protocol for address autoconfiguration in addition to addresses autoconfigured using stateless autoconfiguration.

Valid Values: yes or no

Default Value: n

If you specify *yes*, the DHCPv6 relay agent allows hosts to use local link addresses at address configuration time, even though the DHCPv6 server is not on the same link.

Other stateful configuration
Specifies whether hosts use the administered protocol for autoconfiguration of other (non-address) information.

Valid Values: yes or no

Default Value: no

Include link layer address with router advertisement
Specifies whether to include the link layer address in the router advertisement. A router may omit the link layer address in the router advertisement in order to enable inbound load sharing across multiple link layer addresses.

Valid Values: yes or no

Default Value: yes

Hop limit
Specifies the default value to be placed in the hop limit field in the router advertisement messages sent by the router. This value is used in the hop count field of the IP header for outgoing IP packets.

Valid Values: 0 - 255, where 0 means unspecified by this router

Default Value: 0

Maximum router advertisement interval
Specifies the maximum time, in seconds, allowed between sending unsolicited multicast router advertisements from the interface.

Valid Values: 4 - 1800 seconds

Default Value: 600

Minimum router advertisement interval
Specifies the minimum time, in seconds, allowed between sending unsolicited multicast router advertisements from the interface.

Valid Values: 3 - (.75 * *Maximum router advertisement interval*)

Default Value: *Maximum router advertisement interval*/3

Router lifetime
Specifies the time, in seconds, that the router is to be used as a default router.

Valid Values: 0 or 4 - 9000 seconds, where 0 indicates that the router is not being used as a default router

Default Value: (3 * *Maximum router advertisement interval*)

Reachable Time
Specifies the time, in seconds, that a node assumes a neighbor is reachable after having received a reachability confirmation.

Valid Values: 0 - 3 600 seconds, where 0 indicates unspecified by this router

Default Value: 0

Retransmit timer
Specifies the time, in seconds, between retransmitted neighbor solicitation messages.

Valid Values: 0 - 3 600 seconds, where 0 indicates unspecified by this router

Default Value: 0

link-mtu
Specifies the value to be placed in the MTU options sent by the router. This value should be sent on links that have a variable MTU and may be sent on other links.

Valid Values: A 32-bit unsigned integer, where 0 indicates that no MTU options are sent

Default Value: 0

dhcp-server
Adds a DHCP server.

server addresses
Specifies a list of unicast IPv6 server addresses to be used to forward the initial DHCPv6 solicitation message. If no addresses are specified, the DCHPv6 relay agent sends the packet to the DHCP servers multicast address.

Note: If you use the multicast servers address, you must enable multicast routing in the box by enabling and configuring Protocol Independent Multicast (PIM). See "Chapter 15. Configuring and Monitoring Protocol Independent Multicast Routing Protocol (PIM)" on page 429 for information.

Valid Values: Any valid IPv6 address

Default Value: None

Change

Use the **change** command to change a route advertisement or prefix.

Syntax:

change ...prefix ...
ra

prefix Changes a configured prefix. Prefixes are added or deleted as you modify the IPv6 address configuration. See "Add" on page 391 for more information about adding IPv6 addresses.

To add a prefix:

```
Config> p IPv6
IPv6 user configuration
IPv6 config> add addr
Which net is this address for [0]?  5
New address []? 2002:9::6204
Prefix length must be between 8 and 128 [128]? 64
IPv6 config> exit
```

To change a prefix:

```
Config> p ndp6
Neighbor Discovery for IPv6 user configuration
NDP6 Config> change prefix
Change Prefix Information option for which Prefix address []? 2002:2::
Use this prefix for on-link determination? [Yes]:
Use this prefix for autonomous address configuration? [Yes]: n
Valid lifetime for Prefix [2592000]? ffffffff
Decrement the Valid Lifetime in real time? [No]:
Preferred Lifetime for Prefix [604800]? ffffffff
Decrement the Preferred Lifetime in real time? [No]:
```

Change prefix information options for which prefix address?

Specifies the IPv6 address prefix to be placed in the prefix information option in router advertisements sent from the interface.

Valid Values: Any valid IPv6 address

Default Value: None

Use this prefix for on-link determination?

Specifies the value to be placed in the on-link flag in the prefix information option. When set to *yes*, the prefix can be used for on-link determination. When set to *no*, the advertisement will make no statement about on-link or off-link properties of the prefix.

Valid Values: yes or no

Default Value: yes

Use this prefix for autonomous address configuration?

Specifies the value to be placed in the autonomous address configuration flag in the prefix information option. When set to *yes*, the prefix can be used for autonomous address configuration.

Valid Values: yes or no

Default Value: yes

Valid Lifetime for Prefix?

Specifies the amount of time, in seconds, to be placed in the valid lifetime in the prefix information option. This value represents the length of time, relative to the time that the packet is sent, that the prefix is valid for the purpose of on-link determination.

Valid Values: A 32–bit unsigned integer, where X'FFFFFFFF' represents unlimited lifetime

Default Value: 259200 (which is 30 days)

Decrement the Valid Lifetime in real time?

Specifies whether the Valid Lifetime decrements in real time, resulting in a lifetime of zero at the specified time in the future OR is fixed (stays the same in consecutive router advertisements).

Valid Values: yes or no

Default Value: no

Preferred lifetime for prefix
Specifies the amount of time, in seconds, to be placed in the preferred lifetime in the prefix information option. This value represents the length of time, relative to the time that the packet is sent, that addresses generated from the prefix via stateless address autoconfiguration remain preferred.

Valid Values: A 32–bit unsigned integer, where X'FFFFFFFF' represents unlimited lifetime

Default Value: 604800

Decrement the Preferred Lifetime in real time?
Specifies whether the Preferred Lifetime decrements in real time, resulting in a lifetime of zero at the specified time in the future, or is fixed (stays the same in consecutive router advertisements).

Valid Values: yes or no

Default Value: no

ra Changes a configured route advertisement.See “Add” on page 419 for a description of the parameters associated with the **change ra** command.

Delete

Use the **delete** command to remove a configured route advertisement.

Syntax:

delete	dhcp-server
	ra

Disable

Use the **disable** command to disable route advertisement.

Syntax:

disable	dhcp-relay
	ra

dhcp-relay
Disables the DHCPv6 relay agent.

ra Disables route advertisement.

Enable

Use the **enable** command to enable route advertisement.

Syntax:

enable	dhcp-relay
	ra

dhcp-relay
Enables DHCPv6 relay agent.

ra Enables route advertisement.

List

Use the **list** command to display the NDP configuration.

Syntax:

list	dhcp
	ndp6 configuration
	prefix
	ra

Example:

```
NDP>list dhcp

DHCPv6 Relay Agent
------------------
State          Hopcount
DISABLED           4
NDP>
NDP config>list ndp6


NDP config>list ra


NDP config>list prefix
NDP config>
```

Set

Use the **set** command to set the DHCP hop count.

Syntax:

set	dhcp-hopcount

dhcp-hopcount

Specifies the number of hops to be used in relaying DHCPv6 packets.

Valid Values:

Default Value: 4

Example:

```
NDP6 Config>set dhcp-hopcount
Hop Count [4]?
NDP6 Config>
```

Accessing the NDP Monitoring Environment

Use the following procedure to access the NDP monitoring commands. This process gives you access to the NDP monitoring process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to "The OPCON Process and Commands" in *Access Integration Services Software User's Guide*.) For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the + prompt, enter the **p ndp** command to get you to the `NDP>` prompt.

Example:

```
+ p ndp
NDP>
```

NDP Monitoring Commands

This section describes the NDP monitoring commands.

Table 110. NDP 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 xxviii.
dhcpv6-relay	Sets DHCPv6-relay counters and parameters.
dump	Displays routing tables.
list	Displays the configuration.
ping6	Dynamically pings an IPv6 address.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

DHCPv6-Relay

Use the **dhcpv6-relay** command to set DHCPv6-Relay counters and parameters.

Syntax:

dhcpv6-relay counters
parameters

counters

parameters

Example:

Dump

See "Dump routing tables" on page 435 for information about the **dump** command.

List

Use the **list** command to display the configuration. Only interfaces with RA configured are displayed even though a prefix may exist in the prefix list on other interfaces as a result of IPv6 address configuration.

Syntax:

list dhcpv6-relay
dump routing tables
ndp6 parameters
ping6

Example:

```
NDP>list dhcp

DHCPv6 Relay Agent
------------------
State          Hopcount
DISABLED           4
NDP>
NDP>list ndp6
```

```
Router Advertisement for Interface 0 (PPP/0):
                      Hop    RA Interval  Rtr       Reach    Retrans
  State      M  O LLA Limit   Min - Max   Lifetime  Time     Timer    MTU
  ENABLED    N  N  Y  0       200 - 600   1800      0        0        0

  Advertised Prefixes:
  Prefix/Length                               On-Link Auto Valid/Preferred Life
```

Ping6

See “Ping6” on page 414 for details about the **ping6** command.

NDP6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Neighbor Discovery Protocol for IPv6 (NDP6) supports the CONFIG (Talk 6) **delete interface** command with no restrictions.

GWCON (Talk 5) Activate Interface

NDP6 supports the GWCON (Talk 5) **activate interface** command with no restrictions.

The following table summarizes the NDP6 configuration changes that are activated when the GWCON (Talk 5) **activate interface** command is invoked:

Commands whose changes are activated by the GWCON (Talk 5) activate interface command
CONFIG, protocol NDP6, add ra
CONFIG, protocol NDP6, change prefix
CONFIG, protocol NDP6, change ra
CONFIG, protocol NDP6, delete ra
CONFIG, protocol NDP6, disable ra
CONFIG, protocol NDP6, enable ra

GWCON (Talk 5) Reset Interface

NDP6 supports the GWCON (Talk 5) **reset interface** command with no restrictions.

The following table summarizes the NDP6 configuration changes that are activated when the GWCON (Talk 5) **reset interface** command is invoked:

Commands whose changes are activated by the GWCON (Talk 5) reset interface command
CONFIG, protocol NDP6, add ra
CONFIG, protocol NDP6, change prefix
CONFIG, protocol NDP6, change ra
CONFIG, protocol NDP6, delete ra

CONFIG, protocol NDP6, disable ra
CONFIG, protocol NDP6, enable ra

GWCON (Talk 5) Component Reset Commands

NDP6 supports the following NDP6-specific GWCON (Talk 5) **reset** commands:

GWCON, Protocol IPV6, Reset IPV6 Command

Description:
Dynamically resets all of the NDP6 configuration parameters. See the command description under IPv6 for complete details of this command.

Network Effect:
No network disruption for NDP6.

Limitations:
None.

The following table summarizes the NDP6 configuration changes that are activated when the **GWCON, protocol ipv6, reset ipv6** command is invoked:

Commands whose changes are activated by the GWCON, protocol ipv6, reset ipv6 command
CONFIG, protocol NDP6, add ra
CONFIG, protocol NDP6, change prefix
CONFIG, protocol NDP6, change ra
CONFIG, protocol NDP6, delete ra
CONFIG, protocol NDP6, disable ra
CONFIG, protocol NDP6, enable ra

Chapter 15. Configuring and Monitoring Protocol Independent Multicast Routing Protocol (PIM)

Configuration for PIM is done for each interface. This chapter describes how to use the PIM configuration and operating commands and includes the following sections:

Using PIM

Protocol Independent Multicast dense mode (PIM-DM) is a broadcast and prune multicast protocol used by IP. It supports both IPv4 and IPv6 and the commands and syntax are identical for both versions. It works well in campus networks, where bandwidth is plentiful and users are closely grouped, not dispersed over a wide area of networks. PIM uses a broadcast and prune approach for the multicast forwarding of datagrams and is used when multicast groups are densely distributed across the Internet. It assumes that all downstream systems want to receive multicast datagrams and prunes back branches from those systems which do not.

PIM-DM is a soft state protocol. This means that the prune states, if not removed by some other activity (such as grafting or joining), are removed after a period of time (configurable) and the multicast data is once again broadcasted to all downstream systems where pruning once again occurs.

PIM-DM establishes adjacency to neighboring PIM routers by exchanging Hello messages with all neighbors. It keeps the adjacency active until it is timed out. As long as the neighboring routers are active and running, new Hello messages are sent to refresh the Hello state and prevent the adjacency from timing out. You can configure how often Hello messages are sent.

PIM-DM uses the unicast routing table, regardless which unicast protocol owns an entry, to perform the reverse path forwarding calculation on a received multicast datagram. Reverse path forwarding (RPF) is used to validate whether the received multicast datagram arrived on an interface that would be valid for forwarding to the source address contained in the multicast datagram. If this is an incorrect interface, the datagram is discarded, or else a new multicast entry is built and the multicast datagram is forwarded on all other interfaces (those with PIM-DM active, local host members, and any additional interfaces added by other multicast protocols). The use of unicast routes to perform RPF for input interface validation requires unicast routing to be symmetrical.

Grafting is also supported to allow hosts to dynamically join a group. This grafts a branch to an already existing multicast tree, removing all prune states where required, to ensure that the joined hosts receive the requested group multicast datagrams.

Because of the independent nature of PIM with respect to unicast routing protocols and the broadcast nature of PIM-DM, parallel paths from the source may occur and duplicate multicast data may be forwarded. PIM-DM uses an Assert procedure to choose the appropriate forwarding router when this occurs. Preferences may be configured on routers that run different unicast routing protocols to resolve which router is desired to have precedence. When unicast routing is the same, unicast metric costs to the source are used to determine the best route. And when all else is equal, the router with the largest IP interface address is chosen as the appropriate forwarder.

Use the **p pim** command at the `Config>` prompt to configure PIM parameters.

Accessing the PIM Configuration Environment

Use the following procedure to access the PIM configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to "The OPCON Process and Commands" in *Access Integration Services Software User's Guide*.) For example:

   ```
   * talk 6
   Config>
   ```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. For IPv4, at the CONFIG prompt, enter the **p pim** command to get to the `PIM Config>` prompt. For IPv6, enter the **p pim6** command to get to the `PIM6 Config>` prompt.

PIM Configuration Commands

To configure PIM for IPv4, enter the commands at the `PIM Config>` prompt. For IPv6, enter the commands at the `PIM6 Config>` prompt.

Table 111. PIM 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 xxviii.
delete	Deletes a PIM interface.
disable	Disables PIM on the device.
enable	Enables PIM on the device and sets global PIM default configuration values.
list	Lists the configuration.
set	Sets PIM configuration parameter values.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Delete

Use the **delete** command to remove a configured PIM interface.

Syntax:
delete *interfaceaddr*

Interface address

Example:

```
PIM Config> delete
 Interface address []?
```

Disable

Use the **disable** command to disable PIM on the device.

Syntax:
disable

Enable

Use the **enable** command to enable PIM on the device and set global PIM default configuration values.

Syntax:
enable

List

Use the **list** command to display the PIM configuration.

Syntax:

list	all
	interface
	preference
	variables

all Displays all PIM configuration information.

interface
Displays PIM configuration information about the currently configured interfaces.

Example:

```
PIM Config>list i

                                                 Hello        State
     Type              IP Address               Interval     Holdtime
     Physical          9.37.2.1                   30           210
```

Type Identifies the type of interface that is configured.

IP address
Identifies the IP address assigned to this interface.

Hello Interval
Identifies the interval between hello messages, in seconds, sent on this interface.

State holdtime
Identifies the number of seconds to tell other devices upstream to hold PIM state for this device. For PIM, this is the amount of time for upstream devices to keep prunes alive.

variables
Displays configuration information about global PIM variables.

Example:

```
PIM Config>list v

          PIM Global Configuration Values

                PIM:  on
```

```
                  Graft Timeout:       3 seconds
                  Assert Timeout:    210 seconds
PIM Config>
```

PIM: on/off
Identifies whether PIM is currently enabled or disabled.

Graft timeout
Identifies the number of seconds that grafts are retransmitted if no graft acknowledgement has been received.

Assert timeout
Identifies the number of seconds that assert information learned by upstream devices is retained before reverting back to local routing information.

preference
Displays current configured routing type metric preferences.

Example: (IPv4 only)

```
PIM Config>list p

     Direct     0
     Static     1
     OSPF     110
     RIP      120
     BGP      200

PIM Config>
```

Route type
Identifies the route type supported and lists a hexadecimal value displaying the currently configured metric preference.

Set

Use the **set** command to change PIM configuration parameter values. You can use this command to add a new physical interface.

Syntax:

set interface *interfaceaddress helloperiod joinpruneholdtime*
preference *routetype preferencevalue*
variables

interface

Example:

```
PIM Config>set interface
Interface address []?
Hello period [30]?
Join Prune Hold Time [210]?
```

Interface address

Valid Values: Any valid IP address

Default Value: None

Hello period
Specifies the number of seconds between Hello messages. On point-to-point interfaces, this value is ignored. Once the 2212 establishes adjacency, Hello messages are silenced.

Valid Values: 1 - 65535

Default Value: 30

Join prune hold time
Controls messages to inform the receiving device on how long (in seconds) to hold the state activated by the message. Prunes sent to the device remain active for this number of seconds.

Valid Values: 1 - 65535

Default Value: 210

preference *routetype*
This is a configured metric preference to be used in the assert process. It allows the user to selectively select which unicast route types in the unicast forwarding tables has precedence over other route types. It is of local significance only, meaning it is used for this device and all its attached PIM activated interfaces. This can be used if several unicast routing protocols are in use by this router, adjacent routers are running different routing protocols, or route types, such as default routes, are desired over learned routes.

Routetype can specify the following route types:

- direct
- static
- ospf (IPv4 only)
- rip (IPv4 only)
- bgp

Example:

```
PIM Config> set preference rip
RIP Metric Preference [120]?
```

Metric Preference
This value is sent to other routers in the assert process during duplicate multicast forwarding detection and is used with route metric costs to determine which router should be the forwarding router. All metric preferences are initially set to 0.

Range: 0 - 65535

Default Values:

direct 0

static 1

ospf 110

rip 120

bgp 200

variables cache_life

Example:

```
PIM Config>set v cache_life
Mcfwd cache Holdtime [60]
```

Mcfwd cache holdtime
Specifies the amount of time in seconds that a multicast forwarding entry which has not been used to forward any multicast datagrams will be allowed to exist in the multicast forwarding cache before it is removed.

Valid Values: A numeric value greater than 0

Default Value: 60

variables assert_tout

Example:

```
PIM Config>set v assert_tout
PIM Assert Time Out [210]
```

Assert time out

The amount of time in seconds that downstream routers will save assert information received from two or more asserting upstream routers. Assert information is used to ensure the downstream routers understand who the correct upstream router is, or forwarding router, so that PIM messages may be sent to the correct router. If no further asserts are received before the assert time has expired, the assert information is discarded and the router uses local information in the unicast routing tables to determine the correct upstream forwarding router.

Valid Values: 1 - 65535

Default Value: 210

variables graft_tout

Example:

```
PIM Config>set v graft_tout
PIM Graft Time Out [3]
```

Graft time out

Specifies the number of seconds that the device that has sent a graft message, but has received no acknowledgement, will wait before sending another message.

Valid Values: 1 - 65535

Default Value: 3

Accessing the PIM Monitoring Environment

Use the following procedure to access the PIM monitoring commands. This process gives you access to the PIM monitoring process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to *The OPCON Process and Commands* in the Access Integration Services Software User’s Guide.) For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.

2. For IPv4, at the + prompt, enter the **p pim** command to get to the `PIM>` prompt. For IPv6, at the + prompt, enter the **p pim6** command to get to the `PIM6>` prompt.

   Example:

   ```
   + p pim
   PIM>
   ```

PIM Monitoring Commands

This section describes the PIM monitoring commands.

Table 112. PIM 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 xxviii.
dump	Displays routing tables.
clear	Clears the multicast forwarding table.
interface	Displays the status of the interface.
join	Joins a multicast group.
leave	Leaves a multicast group.
mcache	Displays currently active multicast forwarding table cache entries.
mgroups	Displays group membership of the device's attached interfaces.
mstats	Displays various multicast routing statistics.
neighbor	Displays information about current adjacencies.
pim	Displays the PIM state database.
summary pim	Displays a summary of the PIM state database.
ping	Dynamically pings an IPv6 address.
reset	Dynamically resets PIM.
traceroute	Dynamically traces a route.
variables	Displays the configuration values for PIM variables.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Dump routing tables

Use the **dump** command to display the configured routing tables.

Syntax:
dump

For an example of the output of this command, see the description of the **dump routing table** command at IP Monitoring Commands in *Protocol Configuration and Monitoring Reference Volume 1*.

Clear

Use the **clear** command to reset the cache.

Syntax:
clear

Example:

```
PIM>clear

Mfwd Cache has been cleared!

PIM>
```

Interface

Use the **interface** command to display a summary of the statistics and parameters related to the interface.

Syntax:
interface

Example:

```
PIM>interface
PIM Interface Table
                                            Hello     State
IP Address                                 Interval  Holdtime  Status   Type
9.32.45.1                                     30        210    up       TKR/0
9.10.32,23                                    30        210    up       TKR/1
PIM>
```

IP address
Specifies the IP address of the interface.

Hello interval
Specifies the number of seconds between hello messages on this interface.

State holdtime
Specifies the number of seconds upstream devices are informed to hold state information before discarding. For PIM, this is the number of seconds a prune is active upstream.

Status
Specifies the current status of the interface.

up The interface is up and fully operational, but does not generate the mld queries.

disabled
The interface is operational but is disabled and PIM is not active.

down The interface is not operational.

Join

Use the **join** command to join a multicast group.

Syntax:
join

Example:

```
PIM>join 224.12.2.2
```

Leave

Use the **leave** command to leave a multicast group. This prevents the device from responding to pings and SNMP queries sent to the group address.

Syntax:
leave

Example:

```
PIM>leave 224.12.2.2
```

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.

Syntax:
mcache

Example:

```
PIM>mcache

             0: TKR/0          1: TKR/1          2: TKR/2
             3: IPPN/0         4: BDG/0          5: Internal

                            Prot    Count      Upstr     Downstream

 Source         Destination   Owner   Count      Upst    Downstream
 9.10.12.3      224.12.2.2    PIM     124          0       1, 2
*10.23.55.2     224.32.4.5    PIM     3            1       1
PIM>
```

Prot Specifies the owning protocol of the multicast forwarding table entry.

Count Displays the number of multicast packets received for this multicast forwarding table entry.

Upstr Displays the neighboring network or router from which the datagram must be received in order to be forwarded.

Downstream
Displays the total number of downstream interfaces or neighbors to which the datagram will be forwarded.

Mgroups

Use the **mgroups** command to display the group membership of the device'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:

```
PIM>mgroups

           Local Group Database
Group                   Interface              Lifetime (secs)

224.12.2.2              9.32.4.5 (TKR/0)       176
224.5.5.5               Internal               1

PIM>
```

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

Interface
Displays the interface address to which the group address has been reported (through MLD). The router's internal group membership is indicated by a value of *internal*. For these entries, the lifetime field (see following description) 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.

Mstats

Use the **mstats** 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:

```
PIM>mstats

              MOSPF forwarding:       Disabled
              Inter-area forwarding:  Disabled
              DVMRP forwarding:       Enabled
              PIM forwarding:         Disabled

Datagrams received:          10143  Datagrams fwd (multicast):  10219
Datagrams fwd (unicast):         0  Locally delivered:              0
Unreachable source:              0  Unallocated cache entries:      0
Off multicast tree:              0  Unexpected DL multicast:        0
Buffer alloc failure:            0  TTL scoping:                    0
Administrative filtering:      235

# DVMRP routing entries:         5  # DVMRP entries freed:          0
# fwd cache alloc:               1  # fwd cache freed:              0
# fwd cache GC:                  0  # local group DB alloc:         0
# local group DB free:           0

PIM>
```

Datagrams received
Displays the number of multicast datagrams received by the router.

Datagrams fwd (multicast)
Displays the number of datagrams that have been forwarded as data-link 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 data-link unicasts.

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

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 data-link multicasts on those interfaces that have been configured for data-link 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.

Administrative filtering
Displays the number of datagrams discarded because of outbound filtering.

#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**).

#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 entires 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.

Neighbor

Use the **neighbor** command to display information about neighbor PIM devices and their adjacency status.

Syntax:
neighbor

Example:

```
PIM>neighbor
PIM Neighbor Listing

                                              Last     First
Neighbor Addr                           DR    Heard    Heard    Ifc
9.12.2.2                                NO    21       6139     TKR/0
9.25.3.111                              YES   29       6204     TKR/1

PIM>
```

Neighbor Addr
Identifies if this router has identified the neighbor as the designated router.

DR Identifies if this router has identified the neighbor as the designated router.

Last Heard
The number of seconds since last heard from the neighbor.

First Heard
The total number of seconds since the adjacency was first established to this neighbor.

Ifc The interface that the neighbor was discovered on.

PIM

Use the **pim** command to display the PIM state database.

Syntax:
pim

Example:

```
PIM>pim
                        PIM State Database
                        -------------------
Interface   Group            Source            Lifetime (sec)
1   PRUNE   224.12.2.2       9.32.4.128        205
1   PRUNE   224.23.121.4     9.124.23.1        155

PIM>
```

Group The destination group address associated with the entry.

Source
The source address of the originator of the multicast datagram.

Interface
The PIM interface number and the type of PIM state in the database.

Lifetime
The total lifetime, in seconds, of the state received, obtained from the PIM control message that set up the state.

Summary PIM

Use the **summary pim** command to display summary information about the PIM state database.

Syntax:
summary pim

Example:

```
PIM>s

                Summary PIM State Database
                --------------------------
0)     Group:  224.0.1.42
0)    Source:  9.37.179.1
0)    States:  1-P  2-P

PIM>
```

Group The destination group address associated with the entry.

Source
The source address of the originator of the multicast datagram.

States Displays the interfaces and states associated to the source group pair. P identifies a prune state.

Ping

Use the **ping** command to dynamically ping another destination IPv6 address.

Syntax:
ping

For an example of the output of this command see the description of the **ping** command at IP Monitoring Commands in *Protocol Configuration and Monitoring Reference Volume 1*.

See “Ping6” on page 414 for a description of the parameters.

Reset

Use the **reset** command to reset PIM and reload the configuration.

Syntax:
reset

Example:

```
PIM>reset
```

Traceroute

Use the **traceroute** command to dynamically trace a route.

Syntax:
traceroute

For an example of the output of this command see the description of the **traceroute** command at IP Monitoring Commands in *Protocol Configuration and Monitoring Reference Volume 1*. See “Traceroute6” on page 414 for a description of the parameters.

Variables

Use the **variables** command to display information about the PIM configuration variables.

Syntax:
variables

Example:

```
PIM>variables

   PIM: on

          Graft Timeout:      3 seconds
         Assert Timeout:    210 seconds

PIM Unicast Metric Preferences
Direct     0
Static     1
OSPF     110
RIP      120
BGP      200

PIM>
```

PIM Monitoring Commands (Talk 5)

PIM: on/off
This indicates whether PIM-DM is currently enabled or disabled.

Graft Timeout
The number of seconds that grafts are retransmitted if no graft acknowledgement has been received.

Assert Timeout
The number of seconds that assert information learned by upstream routers is retained before reverting back to local routing information.

PIM Unicast Metric Preferences
Displays current configured routing type metric preferences. Each route type supported is listed with a decimal value displaying the currently configured metric preference.

PIM Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Protocol Independent Multicast (PIM) supports the CONFIG (Talk 6) **delete interface** command with no restrictions.

GWCON (Talk 5) Activate Interface

PIM supports the GWCON (Talk 5) **activate interface** command with the following consideration:

PIM must be globally enabled before PIM can be activated on a network interface.

All PIM interface-specific commands are supported by the GWCON (Talk 5) **activate interface** command.

GWCON (Talk 5) Reset Interface

PIM supports the GWCON (Talk 5) **reset interface** command with the following consideration:

PIM must be globally enabled before PIM can be activated on a network interface.

All PIM interface-specific commands are supported by the GWCON (Talk 5) **reset interface** command.

GWCON (Talk 5) Component Reset Commands

PIM supports the following PIM-specific GWCON (Talk 5) **reset** commands:

GWCON, Protocol PIM, Reset Command

Description:
Dynamically resets PIM variable values and interfaces.

Network Effect:
Loss of PIM neighbor adjacency on all interfaces running PIM. This may impact IP multicast forwarding, though information is corrected after a period of time during which neighbor adjacency is once again established.

Limitations:
None.

All PIM commands are supported by the **GWCON, protocol pim, reset** command.

PIM for IPv6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Protocol Independent Multicast for IPv6 (PIM6) supports the CONFIG (Talk 6) **delete interface** command with no restrictions.

GWCON (Talk 5) Activate Interface

PIM6 supports the GWCON (Talk 5) **activate interface** command with the following consideration:

PIM6 must be globally enabled before PIM6 can be activated on a network interface.

All PIM6 interface-specific commands are supported by the GWCON (Talk 5) **activate interface** command.

GWCON (Talk 5) Reset Interface

PIM6 supports the GWCON (Talk 5) **reset interface** command with the following consideration:

PIM6 must be globally enabled before PIM6 can be activated on a network interface.

All PIM6 interface-specific commands are supported by the GWCON (Talk 5) **reset interface** command.

GWCON (Talk 5) Component Reset Commands

PIM6 supports the following PIM6-specific GWCON (Talk 5) **reset** commands:

GWCON, Protocol PIM, Reset Command

Description:
Dynamically resets PIM6 variable values and interfaces.

Network Effect:
Loss of PIM6 neighbor adjacency on all interfaces running PIM6. This may impact IPv6 multicast forwarding, though information is corrected after a period of time during which neighbor adjacency is once again established.

Limitations:
None.

All PIM6 commands are supported by the **GWCON, protocol pim, reset** command.

Multicast Forwarding Cache Dynamic Reconfiguration Support

Note: The following commands are common among MOSPF, DVMRP, and PIM and are considered MFC commands for IPv4:
- **join**
- **leave**
- **mcache**
- **mgroups**
- **mstats**

Refer to “Configuring and Monitoring OSPF” for more information about MOSPF and “Configuring and Monitoring DVMRP” for more information about DVMRP. Both chapters are in *Protocol Configuration and Monitoring Reference Volume 1*.

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Multicast Forwarding Cache (MFC) supports the CONFIG (Talk 6) **delete interface** command with the following consideration:

IP must notify MFC of address update.

GWCON (Talk 5) Activate Interface

MFC supports the GWCON (Talk 5) **activate interface** command with the following consideration:

IP must notify MFC of address update.

All MFC interface-specific commands are supported by the GWCON (Talk 5) **activate interface** command.

GWCON (Talk 5) Reset Interface

MFC supports the GWCON (Talk 5) **reset interface** command with the following consideration:

IP must notify MFC of address update.

All MFC interface-specific commands are supported by the GWCON (Talk 5) **reset interface** command.

Non-Dynamically Reconfigurable Commands

All MFC configuration parameters can be changed dynamically.

Multicast Forwarding Cache V6 Dynamic Reconfiguration Support

Note: The following PIM commands are considered Multicast Forwarding Cache (MFC6) commands for IPv6:
- **join**
- **leave**
- **mcache**
- **mgroups**
- **mstats**

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Multicast Forwarding Cache V6 (MFC6) supports the CONFIG (Talk 6) **delete interface** command with the following consideration:

IPv6 must notify MFC6 of address update.

GWCON (Talk 5) Activate Interface

Multicast Forwarding Cache V6 (MFC6) supports the GWCON (Talk 5) **activate interface** command with the following consideration:

IPv6 must notify MFC6 of address update.

All Multicast Forwarding Cache V6 (MFC6) interface-specific commands are supported by the GWCON (Talk 5) **activate interface** command.

GWCON (Talk 5) Reset Interface

Multicast Forwarding Cache V6 (MFC6) supports the GWCON (Talk 5) **reset interface** command with the following consideration:

IPv6 must notify MFC6 of address update.

All Multicast Forwarding Cache V6 (MFC6) interface-specific commands are supported by the GWCON (Talk 5) **reset interface** command.

Non-Dynamically Reconfigurable Commands

All Multicast Forwarding Cache V6 (MFC6) configuration parameters can be changed dynamically.

Chapter 16. Configuring and Monitoring Routing Information Protocol (RIP6)

RIP6 is a distance vector routing protocol. Configuration for RIP6 is done for each interface. This chapter describes how to use the RIP6 configuration and operating commands and includes the following sections:

Accessing the RIP6 Configuration Environment

Use the following procedure to access the RIP6 configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to "The OPCON Process and Commands" in *Access Integration Services Software User's Guide*.) For example:

   ```
   * talk 6
   Config>
   ```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the CONFIG prompt, enter the **p rip6** command to get to the `RIP66 Config>` prompt.

RIP6 Configuration Commands

To configure RIP6, enter the commands at the `RIP66 Config>` prompt.

Table 113. RIP6 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 xxviii.
add	Adds RIP6 on an interface.
change	Changes RIP6 metric configuration values or the originating default.
delete	Removes RIP6 from an interface.
disable	Disables RIP6 on an interface.
enable	Enables RIP6 on an interface.
list	Lists the configuration.
set	Sets RIP6 metric values.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Add

Use the **add** command to add RIP6 on an interface.

Syntax:

add *interface#*

interface#
Specifies the interface to which RIP6 protocol is to be added.

Note: This interface must have an IPv6 address configured or be the virtual interface of an IPv6 over IPV4 tunnel.

Valid Values: Any valid interface number

Default Value: None

Change

Use the **change** command to change a RIP6 metric.

Syntax:

change	originating-default
	rip6-in-metric
	rip6-out-metric

originating-default

This following configuration parameters allow you to change the originating default router.

Always originate default route

Enabling this parameter allows RIP6 to advertise the router as a default router (called “originating the default route”). The default router performs routing for other routers on the Internet that have packets for an unknown network destination.

Valid Values: Yes or No

Default Value: No

Originate default dependent on BGP route availability

This field allows user to enable or disable a router running EGP/BGP to advertise itself as a default router via its IGP (RIP6 in this case.)

Valid Values: Yes or No

Default Value: No

From AS number

If you are configuring RIP6 to originate a default route when EGP routes are available, you can also configure it to originate the default only if EGP routes are received from a particular AS. For example, if you want a default route generated only if an EGP route is received from AS number 12, you would set this parameter to 12. Setting the AS number to 0 means “from any AS.”

Valid Values: 0 - 65535

Default Value: None

Destination prefix (or network number)

If you are originating a default route when EGP routes are available, you can also choose to originate the default only if a particular route is received through the EGP. For example, if you want a default route generated only if a route to network N is received, you would set this parameter to N. Setting the network number to :: (zero) means “any route received.”

Valid Values: Any IPv6 unicast address, no multicast address, no loopback address, no linklocal address, no site local address, no IPv4 mapped address

Default Value: None

Prefix length
The length of the prefix. This parameter must be configured if **originate default if BGP routes available** is *yes*.

Valid Values: 8 - 128

Default Value:

Originate default if OSPF6 routes available
You can configure a router running OSPF6 to advertise itself as the default router (called originating the default route) via RIP6. When this parameter is enabled, the router advertises itself as the default router via RIP6 if it has OSPF6-derived routes in its routing table. The default router performs routing for other routers on the Internet that have packets for an unknown network destination.

Valid Values: Yes or No

Default Value: No

Originated default cost
This parameter specifies the cost that RIP will advertise with the default route that it originates. The cost is used to determine the shortest path for the default route to its neighbor router.

Valid Values: 1 - 16

Default Value: 1

Example:

```
RIP6 config>set originating
      Always originate default route? [No]: Yes
      Enter Originated default cost: between 1 and 15  [1]? 1
      Update RIP6 default origination dynamically: OK
      RIP6 config>
```

Example:

```
RIP6 config>set originating
      Always originate default route? [Yes]: no
      Originate default dependent on BGP6 route availability? [No]: yes
      From AS number [0]? 10
      Dest. prefix (or network number) [::]? 1234::0
      Prefix length must between 8 and 128 [64]? 64
      Enter Originated default cost: between 1 and 15  [1]? 1
      Update RIP6 default origination dynamically: OK
      RIP6 config>
```

rip6-in-metric
Changes the value of the RIP6 metric for the incoming RIP6 updates.

Change RIPng metric on which interface?
Specifies the interface number on which RIP6 input metric is to be changed.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

RIP6 input Metric
Changes the value of the RIP6 metric on incoming RIP6 updates.

Valid Values: 1 - 15

Default Value: 1

rip6-out-metric
Changes the RIP6 metric on the outgoing RIP6 updates.

Change RIPng metric on which interface?
Specifies the interface number on which RIP6 output metric is to be changed.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

RIP6 output Metric
Specifies the value of the RIP6 metric on outgoing RIP6 updates.

Valid Values: 0 - 15

Default Value: 0

Delete

Use the **delete** command to remove RIP6 from the specified interface.

Syntax:

delete	*interface#*

interface#
Specifies the interface from which RIP6 protocol is to be removed.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: None

Disable

Use the **disable** command to disable RIP6.

Syntax:

disable	override ...
	rip6
	sending ...

override ...

static-routes
Overrides RIP6 static routes on an interface.

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be disabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

default
Overrides RIP6 default routes on an interface.

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be disabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

rip6 Disables RIP6 on the specified interface.

Valid Values: Yes or No

Default Value: Yes

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be disabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

sending ...

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be disabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

all-routes
Disables advertisement of all RIP6 routes on an interface.

Valid Values: Yes or No

Default Value: Yes

default-routes
Disables advertisement of RIP6 default routes on an interface.

Valid Values: Yes or No

Default Value: Yes

static-routes
Disables advertisement of RIP6 static routes on an interface.

Valid Values: Yes or No

Default Value: Yes

poisoned-reverse-routes
Disables poison reverse in sending RIP6 updates on an interface.

Valid Values: Yes or No

Default Value: Yes

Enable

Use the **enable** command to enable RIP6.

Syntax:

enable	override ...
	rip6
	sending ...

override ...

static-routes
Overrides RIP6 static routes on an interface.

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be enabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

default
Overrides RIP6 default routes on an interface.

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be enabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

rip6 Enables RIP6 on the specified interface.

Valid Values: Yes or No

Default Value: Yes

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be enabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

sending ...

Modify RIP6 flags on which interface?
Specifies the interface number on which RIP6 is to be enabled.

Note: The interface must have RIP6 configured.

Valid Values: Any valid interface number

Default Value: 0

all-routes
Enables advertisement of all RIP6 routes on an interface.

Valid Values: Yes or No

Default Value: Yes

default-routes
Enables advertisement of RIP6 default routes on an interface.

Valid Values: Yes or No

Default Value: Yes

static-routes
Enables advertisement of RIP6 static routes on an interface.

Valid Values: Yes or No

Default Value: Yes

poisoned-reverse-routes
Enables poison reverse in sending RIP6 updates on an interface.

Valid Values: Yes or No

Default Value: Yes

List

Use the **list** command to display the RIP6 configuration.

Syntax:
list all

Example:

```
RIP6>list all
RIP6
     Nets: -   0        RIP6: ENABLED
                            Send: static routes
                                  Poison reverse enabled.
                            Receive:  Not override default and static routes
                            RIP interface input metric: 1
                            RIP interface output metric: 0

    RIP6 default origination: BGP6(AS=10, net/prefix_len=1234::/64), cost = 1

    Import BGP6 routes: enabled -  AUTOTAG: enabled
```

Set

Use the **set** command to set RIP6 configuration parameters.

Syntax:
set import bgp6 routes
originating default
rip6-in-metric
rip6-out-metric

import bgp6 routes
This parameter specifies that routes learned by BGP6 will be imported into

the RIP6 routing network. Only routes that appear in the BGP6 input exchange tables will be imported. All routes are imported with their cost equal to their routing table cost.

Valid Values: Yes or No

Default Value: Yes

If the routes learned by BGP6 are imported into the RIP6 routing network, the following parameter can be configured:

Enable autotag
This parameter allows RIP6 to automatically generate tags for BGP6 routes. The tag value is the AS number from which the route is learned.

Valid Values: Yes or No

Default Value: Yes

Example:

```
RIP6 config>set import
Import BGP6 routes?? [Yes]:
Enable AUTOTAG? [Yes]:
AUTOTAG is updated dynamically
```

originating default
This following configuration parameters allow you to set RIP6 to advertise the router as a default router.

Always originate default route
Enabling this parameter allows RIP6 to advertise the router as a default router (called originating the default route). The default router performs routing for other routers on the Internet that have packets for an unknown network destination.

Valid Values: Yes or No

Default Value: No

Originate default dependent on BGP route availability
This field allows user to enable or disable a router running EGP/BGP to advertise itself as a default router via its IGP (RIP6 in this case.)

Valid Values: Yes or No

Default Value: No

From AS number
If you are configuring RIP6 to originate a default route when EGP routes are available, you can also configure it to originate the default only if EGP routes are received from a particular AS. For example, if you want a default route generated only if an EGP route is received from AS number 12, you would set this parameter to 12. Setting the AS number to 0 means “from any AS”.

Valid Values: 0 - 65535

Default Value: None

Destination prefix (or network number)
If you are originating a default route when EGP routes are available, you can also choose to originate the default only if a particular route is received through the EGP. For example, if you

want a default route generated only if a route to network N is received, you would set this parameter to N. Setting the network number to :: (zero) means “any route received”.

Valid Values: Any IPv6 unicast address, no multicast address, no loopback address, no linklocal address, no site local address, no IPv4-mapped address

Default Value: None

Prefix length
The length of the prefix. This parameter must be configured if **originate default if BGP routes available** is *yes*.

Valid Values: 8 - 128

Default Value:

Originate default if OSPF6 routes available
You can configure a router running OSPF6 to advertise itself as the default router (called originating the default route) via RIP6. When this parameter is enabled, the router advertises itself as the default router via RIP6 if it has OSPF6-derived routes in its routing table. The default router performs routing for other routers on the Internet that have packets for an unknown network destination.

Valid Values: Yes or No

Default Value: No

Originated default cost
This parameter specifies the cost that RIP will advertise with the default route that it originates. The cost is used to determine the shortest path for the default route to its neighbor router.

Valid Values: 1 - 16

Default Value: 1

Example:

```
RIP6 config>set originating
      Always originate default route? [No]: Yes
      Enter Originated default cost: between 1 and 15  [1]? 1
      Update RIP6 default origination dynamically: OK
      RIP6 config>
```

Example:

```
RIP6 config>set originating
      Always originate default route? [Yes]: no
      Originate default dependent on BGP6 route availability? [No]: yes
      From AS number [0]? 10
      Dest. prefix (or network number) [::]? 1234::0
      Prefix length must between 8 and 128 [64]? 64
      Enter Originated default cost: between 1 and 15  [1]? 1
      Update RIP6 default origination dynamically: OK
      RIP6 config>
```

rip6-in-metric
Sets the RIP6 metric on incoming RIP6 updates.

Change RIPng metric on which interface?
Specifies the interface number on which RIP6 input metric is to be set.

Valid Values: Any valid interface number

Default Value: 0

RIP6 input Metric
Specifies the value of the RIP6 metric used on incoming RIP6 updates.

Valid Values: 1 - 15

Default Value: 1

rip6-out-metric
Sets the RIP6 metric used on outgoing RIP6 updates.

Change RIPng metric on which interface?
Specifies the interface number on which RIP6 output metric is to be set.

Valid Values: Any valid interface number

Default Value: 0

RIP6 output Metric
Specifies the value of the metric used on outgoing RIP6 updates.

Valid Values: 0 - 15

Default Value: 0

Accessing the RIP6 Monitoring Environment

Use the following procedure to access the RIP6 monitoring commands. This process gives you access to the RIP6 monitoring process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to "The OPCON Process" in *Access Integration Services Software User's Guide*.) For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the + prompt, enter the **p rip6** command to get you to the `RIP6>` prompt.

   Example:

   ```
   + p rip6
   RIP6>
   ```

RIP6 Monitoring Commands

This section describes the RIP6 monitoring commands.

Table 114. RIP6 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 xxviii.
dump	Displays routing tables.
list	Displays the configuration.
ping6	Dynamically pings an IPv6 address.
reset	Dynamically resets RIP6.
traceroute6	Dynamically traces a route.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page xxviii.

Dump

See “Dump routing tables” on page 435 for information about the **dump** command.

List

Use the **list** command to display the configuration.

Syntax:
list

Example:

```
RIP6>list

RIP6                   In     Out
Intf    State          Metric Metric Send-Flags       Receive-Flags
 0         Enabled /UP    1      0      St,P

Send Flags: St=Static D=Default P=PoisonReverse
Recv Flags: OSt=Override-Static OD=Override-Default

RIP originates default with cost 1 under these conditions:
  BGP6 or OSPF6 External route 1234::/64 from AS 10 available
  Default origination conditions not satisfied
Import BGP6 routes: enabled - AUTOTAG: enabled
```

Ping6

See “Ping6” on page 414 for details about the **ping6** command.

Reset

Syntax:
reset

Example:

```
RIP6>reset
```

Traceroute6

See “Traceroute6” on page 414 for details about the **traceroute6** command.

RIP6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Routing Information Protocol for IPV6 (RIP6) supports the CONFIG (Talk 6) **delete interface** command with the following consideration:

All RIP6 configurations configured for this interface are deleted, too.

GWCON (Talk 5) Activate Interface

RIP6 supports the GWCON (Talk 5) **activate interface** command with the following consideration:

IPv6 must be configured for this interface

All RIP6 interface-specific commands are supported by the GWCON (Talk 5) **activate interface** command.

GWCON (Talk 5) Reset Interface

RIP6 supports the GWCON (Talk 5) **reset interface** command with the following consideration:

All RIP6 configurations for an interface change dynamically if there is an IPv6 address configured for this interface.

All RIP6 interface-specific commands are supported by the GWCON (Talk 5) **reset interface** command.

GWCON (Talk 5) Component Reset Commands

Routing Information Protocol for IPv6 (RIP6) supports the following RIP6-specific GWCON (Talk 5) **reset** commands:

GWCON, Protocol RIP6 Reset Interface (or All Interfaces) Command

Description:
Dynamically changes the policies or parameters of an RIP6 interface (all RIP6 interfaces.)

Network Effect:
Depending on the configuration changes, it will alter the sending or receiving policies of RIP6 routes on an interface.

Limitations:
None.

All RIP6 commands are supported by the **GWCON, protocol RIP6 reset interface (or all interfaces)** command.

CONFIG (Talk 6) Immediate Change Commands

RIP6 supports the following CONFIG commands that immediately change the operational state of the device. These changes are saved and are preserved if the device is reloaded, restarted, or you execute a dynamically reconfigurable command.

All RIP6 Talk 6 commands are dynamic.

Non-Dynamically Reconfigurable Commands

All RIP6 configuration parameters can be changed dynamically.

Chapter 17. Configuring and Monitoring BGP6

The BGP4 protocol with the addition of RFC 2283, *Multiprotocol Extensions for BGP4 (BGP4+)*, supports IPv6 routing information.

This chapter describes the BGP6 configuring and monitoring commands and includes the following sections:

Accessing the BGP6 Configuration Environment

To access the BGP6 configuration environment, enter the following command at the `Config>` prompt:

```
Config> protocol bgp6
BGP6 Config>
```

BGP6 Configuration Commands

This section describes the BGP6 configuration commands. These commands allow you to modify the BGP6 protocol behavior to meet your specific requirements. Some amount of configuration is necessary to produce a fully functional BGP6 router. Enter BGP6 configuration commands at the `BGP6 Config>` prompt.

Table 115. BGP6 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 xxviii.
Add	Add BGP6 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 BGP6 configuration information that had been entered with the **add** command.
Disable	Disables certain BGP6 features that have been turned on by the **enable** command.
Enable	Enables BGP6 speakers, BGP6 neighbors.
List	Displays BGP6 configuration items.
Move	Changes the order in which policies and aggregates are defined.
Set	Sets the IPv6-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 xxviii.

Add

Use the **add** command to add BGP6 information to your configuration.

Syntax:

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

aggregate *network prefix Prefix Length*

The **add aggregate** command causes the BGP6 speaker to aggregate a block of addresses, and advertise a single route to its BGP6 neighbors. You must specify the network prefix common to all the routes being aggregated and its prefix length. The following example illustrates how to aggregate a block of addresses.

1. The **network prefix** specifies the addresses being affected. The prefix is the first address in a range of addresses specified in a BGP6 policy.
   Valid Values: a valid IPv6 unicast address or IPv4 compatible address, excluding the following:
   - link-local addresses (FE80::)
   - site-local addresses (FEC0::)
   - loopback address (::1)
   - IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)

   Default Value: none
2. The **prefix length** applies to the address specified in Network Prefix to generate an address used in a BGP6 policy.
   Valid Values: 8 - 128
   Default Value: 64

Example:

```
add aggregate

Network Prefix []? 2000::
Prefix Length [64]? 16
```

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 address AS# init timer connect timer hold timer keep alive timer tcp segment size*

Use the **add neighbor** command to define a BGP6 neighbor. The neighbor can be internal to the BGP6 speaker’s AS, or external. To activate this neighbor dynamically use the **reset neighbor** command from BGP6 monitoring.

Neighbor address

The **neighbor address** is the IPv6 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 BGP6 speakers must share the same network. There is no such restriction for internal neighbors.

Valid Values: a valid IPv6 unicast address or IPv4 compatible address, excluding the following:

– link-local addresses (FE80::)
– site-local addresses (FEC0::)
– loopback address (::1)
– IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)
– zero address (::0)

Default Value: none

AS# The **AS#** 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 1 - 65535
Default Value: 1

Init timer
The **init timer** to specifies the amount of time the BGP6 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

Connect timer
The **connect timer** specifies the amount of time the BGP6 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 BGP6 speaker continues to listen for any connection that may be initiated by its neighbor.
Valid Values: 0 to 65535 seconds.
Default Value: 120 seconds

Hold timer
Enter the **hold timer** to specify the length of time the BGP6 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 BGP6 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 use 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

TCP segment size
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: 1 to 65535 bytes.

Default Value: 1220 bytes

Example:

add neighbor

```
Neighbor address []? 2002:9::6205
AS [1]? 2002
Init timer [12]?
Connect timer [120]?
Hold timer [90]?
TCP segment size [1220]?
```

no-receive *AS#*

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

The **AS#** has:

Valid Values: 1 to 65535

Default Value: 1

Example:

add no-receive

```
Enter AS: [1]? 2003
```

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

Use the **add originate-policy** command to specify the value to use in selecting routes for advertisement.

Exclusive

Exclusive policies prevent route information from being included in the BGP6 speaker's routing table.

Inclusive

Inclusive policies ensure that specific routes will be included in the BGP6 speaker's routing table.

Network prefix

This parameter specifies the network address affected by this policy.

Valid Values:a valid IPv6 unicast address or IPv4 compatible address, excluding the following:

– link-local addresses (FE80::)

– site-local addresses (FEC0::)

– loopback address (::1)

– IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)

Default Value: none

Prefix length

The **prefix length** applies to the address specified in Network Prefix to generate an address used in a BGP6 policy.

Valid Values: 0 - 128

Default Value: 0

Address match

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

Valid Values: Exact or Range

Default Value: Range

Tag The tag value represents the AS number from which the route is learned. The tag value is used for interacting with an IGP, like RIP6. See “Set” on page 453 for information on importing BGP6 routes and BGP6 autotag generation.

Valid Values: 0 - 65535

Default Value: 0

The following example includes all routes in the BGP6 speaker’s IGP routing table to be advertised.

Example:

```
add originate-policy inclusive

Network Prefix [::]?
Prefix length[0]?
Address Match (Exact/Range) [Range]?
Tag [0]?
```

policy-list

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

Name Specifies the name to be used to identify the group of policies.

Valid Values: A string of 1 - 15 ASCII characters

Default Value: None

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
```

receive-policy *(exclusive/ inclusive) network prefix Prefix Length address match originating AS# adjacent AS# igpmetric (inclusive only)*

Use the **add receive-policy** command to determine what routes will be imported to the BGP6 speaker’s routing table.

Exclusive policies prevent route information from being included in the BGP6 speaker’s routing table.

Inclusive policies ensure that specific routes will be included in the BGP6 speaker’s routing table.

Network prefix

Specifies the addresses being affected.

Valid Values: a valid IPv6 unicast address or IPv4 compatible address, excluding the following:

- link-local addresses (FE80::)
- site-local addresses (FEC0::)
- loopback address (::1)
- IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)

Default Value: none

Prefix Length

The **prefix length** applies to the address specified in **network prefix** to generate an address used in a BGP6 policy.

Valid Values: 0 - 128

Default Value: 0

Address match
The **address match** is a range of addresses or an exact address.
Valid Values: Exact or Range
Default Value: Range

Originating AS#
An **originating AS#** has:
Valid Values: 0 to 65535
Default Value: 0

Adjacent AS#
The **adjacent AS#** specifies the neighboring AS number.
Valid Values: 0 to 65535
Default Value: 0

IGP metric
The **IGP metric**(for inclusive receive-policies only) specifies the metric value with which the accepted routes are imported into the speaker's IGP routing table. If the IGP metric is -1, these routes will not be imported into the IGP; thus, these routes are not re-advertiseable.
Valid Values: -1 to 65535
Default Value: 0

Example:

add receive-policy exclusive

```
Network Prefix [::]? 2003::
Prefix length[0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]? 168
Adjacent AS# [0]? 165
```

Example:

add receive-policy inclusive

```
Network Prefix [::]? 2000:: Prefix Length [0]? 64
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Adjacent AS# [0]?
IGP-metric [0]?
```

send-policy *(exclusive/ inclusive) network prefix Prefix Length address match tag adjacent AS#*

Use the **add send-policy** command to create policies that determine which of the BGP6 speaker's learned routes will be readvertised. These routes could be internal or external to the BGP6 speaker's AS.

Exclusive policies prevent route information in the BGP6 speaker's routing table from being advertised to BGP6 neighbors.

Inclusive policies ensure that specific routes in the BGP6 speaker's routing table will be advertised to BGP6 neighbors.

Network prefix
The **network prefix** is for the addresses being affected.
Valid Values: a valid IPv6 unicast address or IPv4 compatible address, excluding the following:
- link-local addresses (FE80::)
- site-local addresses (FEC0::)
- loopback address (::1)
- IPv4 mapped IPv6 addresses (::FFFF:<IPv4 address>)

Default Value: none

Prefix length
The **prefix length** applies to the address specified in Network Prefix to generate an address used in a BGP6 policy.
Valid Values: 0 - 128
Default Value: 0

Address match
The **Address match** is a range of addresses or an exact address.
Valid Values: Exact or Range
Default Value: Range

Tag The tag value represents the AS number from which the route is learned. The tag value is used for interacting with an IGP, like RIP6. See “Set” on page 453 for information on importing BGP6 routes and BGP6 autotag generation.
Valid Values: 0 to 65535
Default Value: 0

Adjacent AS#
The **adjacent AS#** specifies the neighboring AS number.
Valid Values: 0 to 65535
Default Value: 0

Example:

`add send exclusive`

```
Network Prefix []? 2003::
Prefix length[0]? 16
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]?
```

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 [::]? 2003::
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)[]?
```

Change

Use the **change** command to change a BGP6 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 Prefix Length*

This example changes the current aggregate (aggregate 1).

Example:

```
change aggregate 1

Network Prefix [2000::]? 2001::
Prefix Length [16]?
```

neighbor *neighbor IPv6 address AS# init timer connect timer hold timer keep alive timer tcp segment size*

Use this command to change the configuration parameter values for an existing neighbor. This command may not be used to change the address for an existing neighbor.

To reactivate the neighbor dynamically use the **reset neighbor** command from BGP6 monitoring.

The **neighbor address** to be modified has:

Valid Values: Any currently configured neighbor address
Default Value: none

The following example changes the value of the hold timer to zero for neighbor 2002:0::6205.

Example:

```
change neighbor 2002:0::6205

AS [2002]?
Init timer [12]?
Connect timer [60]?
Hold timer [12]? 0
TCP segment size [1220]?
```

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

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

This example alters the BGP6 speaker's originate policy.

Example:

```
change originate-policy

Enter index of originate-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [2003::]? 2004::
Prefix Length [16]? 16
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]? 2003::
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 Prefix Length 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 BGP6 speaker's receive-policy. Rather than import route information from every BGP6 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 [2003::]?
Prefix Length [16]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Adjacent AS# [0]? 165
```

send-policy *index# (exclusive/ inclusive) network prefix Prefix Length 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 BGP6 speaker's send policy.

Example:

```
change send-policy

Enter index of send-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0::0]? 2004:6::6205
Prefix Length [16]? 16
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]? 165
```

Delete

Use the **delete** command to delete a BGP6 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.

Example: `delete aggregate 1`

neighbor *neighbor IPv6 address*

Use this command to delete a BGP6 neighbor. You must specify the neighbor's network address.

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

Valid Values: Any currently configured neighbor address

Default Value: none

To deactivate this neighbor dynamically use the **reset neighbor** command from BGP6 monitoring.

Example: **`delete neighbor 2002:9::6024`**

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#** has:

Valid Values: 1 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 []? 2009:9::6205
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 BGP6 neighbor or speaker. Note that neighbors are implicitly enabled whenever added with the **add** command.

Syntax:

disable	BGP6 speaker
	compare-med-from-diff-AS
	neighbor . . .

BGP6 speaker
Use the **disable BGP6 speaker** command to disable the BGP6 protocol.

Example: `disable BGP6 speaker`

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 IPv6 address*
Use this command to disable a currently configured neighbor. The **neighbor address** has:
Valid Values: Any valid IPv6 address
Default Value: none

Example: `disable neighbor 2002:9::6205`

Enable

Use the **enable** command to activate the BGP6 features, capabilities, and information added to your BGP6 configuration.

Syntax:

enable	BGP6 speaker
	compare-med-from-diff-AS
	neighbor . . .

BGP6 speaker *AS# tcp segment size*
Use the **enable BGP6 speaker** command to enable the BGP6 protocol.

1. The **AS#** is associated with this collection of routers and nodes.
   Valid Values: 1 to 65535
   Default Value: 1
2. Enter the **TCP segment size** to specify the maximum segment size that BGP6 should use for passive TCP connections.
   Valid Values: 1 to 65535 bytes.
   Default Value: 1220 bytes

Example:

```
enable BGP6 speaker

AS [0]? 165
TCP segment size [1220]?
```

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

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

neighbor *neighbor IPv6 address*
Use this command to enable a BGP6 neighbor.

The **neighbor address** has:
Valid Values: Any currently configured neighbor address
Default Value: none

Example: `enable neighbor 2002:9::6205`

List

Use the **list** command to display various pieces of the BGP6 configuration data, depending on the particular subcommand invoked.

Syntax:

list aggregate

all

BGP6 speaker

neighbor

no-receive

originate-policy

policy-list . . .

policy-to-neighbor

receive-policy

send-policy

aggregate

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

Example: `list aggregate`

```
Aggregation:
Index    Prefix/Prefix length
1        2000::/16
```

all Use the **list all** command to list the BGP6 neighbors, policies, aggregated routes, and no-receive-as records in the current BGP6 configuration.

Example: `list all`

```
                BGP6 Protocol:          Enabled
                AS:                    710
                TCP-Segment Size:      1220

Neighbors and their AS:
                                                     Init  Conn  Hold  TCPSEG
Address                                 State  AS    Timer Timer Timer Size
2003:7:8:2::820                         ENABLD 820   12    120   90    1220

2002:9::6205                            ENABLD 2002  12    120   90    1220


Receive-Policies:
Index Type Prefix/Prefix length                       Match OrgAS AdjAS IGPmet
1     INCL ::/0                                       Range 0     0     0

2     EXCL 2003::/16                                  Range 0     0

Send-Policies:
Index  Type  Prefix/Prefix length                       Match Tag   AdjAS
1      INCL  ::/0                                       Range 0     0

2      EXCL  2003::/16                                  Range 0     0


Originate-Policies:
Index  Type  Prefix/Prefix Length                       Match  Tag
1      INCL  ::/0                                       Range  0
2      EXCL  2003::/16                                  Range  0

Aggregation:
Index  Prefix/Prefix Length
1      2000::/16

AS-PATH with following ASs will be discarded:
AS 2003
compare-med-from-diff-as is enabled.
IPv6-route-table-scan-timer value is 2 seconds.
```

BGP6 speaker

Use the **list BGP6 speaker** command to derive information on the BGP6 speaker. The information provided is as follows:

Example:

list BGP6 speaker

```
BGP6 Protocol:         Enabled
AS:                    165
TCP-Segment Size:      1220
```

neighbor

Use the **list neighbor** command to derive information on BGP6 neighbors.

Example: list neighbor

```
Neighbors and their AS along with attached policy-list name(s):
                                                   Init  Conn  Hold  TCPSEG
Address                                 State  AS    Timer Timer Timer Size
2003:7:8:2::820                         ENABLD 820   12    120   90    1220

2002:9::6205                            ENABLD 2002  12    120   90    1220
```

no-receive

Use the **list no-receive** command to derive information on no-receive-AS definitions that have been added to the BGP6 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 BGP6 configuration.

Example: list originate-policy

```
Originate-Policies:
Index  Type  Prefix/Prefix Length                         Match  Tag
1      INCL  ::/0                                         Range  0
2      EXCL  2003::/16                                    Range  0
```

policy-list

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

Example: list policy-list

```
BGP6 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 address                         Receive          Send
2002:9::6205                             rec1             send1
```

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 BGP6 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/Prefix length                         Match OrgAS AdjAS IGPmet
1     INCL ::/0                                         Range 0     0     0

2     EXCL 2003::/16                                    Range 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/Prefix length                        Match Tag   AdjAS
1      INCL  ::/0                                        Range 0     0

2      EXCL  2003::/16                                   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 IPv6-route-table-scan-timer. The IPv6-route-table-scan-timer value is used to set the IPv6 forwarding table scanning time interval for BGP6 updates.

Syntax:

set	ipv6-route-table-scan-timer **Valid Values**: 1 to 10 **Default Value**: 1

Example:

```
set ipv6-route-table-scan-timer
Timer Value in seconds [1]? 2
```

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 or send policies within the **update** command.

Example: Adding a receive policy

```
BGP6 Config>add POLICY-LIST
Policy-list name []? rec1
Policy Type (Receive/Send) [Receive]?
BGP6 Config>UPDATE POLICY-LIST
Policy-list name []? rec1
Policy-list rec1:Receive Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]?
Network Prefix [::]? 1234::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
Policy-list rec1:Receive Config>list
Receive Policy list for rec1:
Idx T Prefix/Length/Match                         OrgAS AnyAS MED   Weight
LP    IGPm
1   E 1234::/16/R                                 0     0

Policy-list rec1:Receive Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]? inc
Network Prefix [::]? 5678::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Local-pref [0]?
Weight [0]?
IGP-metric [0]?
Policy-list rec1:Receive Config>list
Receive Policy list for rec1:
Idx T Prefix/Length/Match                         OrgAS AnyAS MED   Weight
LP    IGPm
1   E 1234::/16/R                                 0     0
2   I 5678::/16/R                                 0     0     0     0
```

Example: Adding a send policy

```
BGP6 Config>add POLICY-LIST
Policy-list name []? send1
Policy Type (Receive/Send)
[Receive]?  send
BGP6 Config>UPDATE POLICY-LIST
Policy-list name []? send1
Policy-list send1:Send Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]? i
Network Prefix [::]? 1234::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
Tag [0]?
MED [0]?
# of AS padding [0]?
Policy-list send1:Send Config>list
Send Policy list for send1:
Idx T Prefix/Length/Match                         OrgAS AnyAS Tag   MED
 ASpad
1   I 1234::/16/R                                 0     0     0     0
```

Notes:

1. There will be no prompting for *MED*, *Local-pref*, *Weight*, and *IGP-metric* parameters for exclusive receive policy. *MED*, *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.
2. Prompting for *MED* and *# of AS padding* parameter values occurs only for inclusive send policies.

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 rec1:
Idx T Prefix/Length/Match                          OrgAS AnyAS MED   Weight
LP    IGPm
1   E 1234::/16/R                                  0     0
2   I 5678::/16/R                                  0     0     0     0
```

Send Policy Example:

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

Accessing the BGP6 Monitoring Environment

To access the BGP6 monitoring environment, enter the following command at the + prompt:

```
+ protocol bgp6
BGP6>
```

BGP6 Monitoring Commands

This section describes the BGP6 monitoring commands. These commands allow you to modify the BGP6 protocol behavior to meet your specific requirements. Some amount of configuration is necessary to produce a fully functional BGP6 router. Enter BGP6 monitoring commands at the `BGP6>` monitoring prompt.

Table 116. BGP6 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 xxviii.
Disable neighbor	Disables a particular neighbor or all neighbors.
Dump routing tables	Lists the contents of the IPv6 routing table.
List	Lists all BGP routing table entries.
Enable neighbor	Enables a particular neighbor or all neighbors.

Table 116. BGP6 Monitoring Command Summary (continued)

Command	Function
Neighbors	Displays currently active neighbors.
Parameter	Displays installed BGP6 globals in the BGP6 system.
Paths	Displays all available paths in the database.
Ping6	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.
Reset neighbor	Resets a particular neighbor.
Traceroute6	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 xxviii.

Disable Neighbor

Use the **disable neighbor** command to disable a particular neighbor or all neighbors that have been enabled. This command brings down the BGP6 session and removes the routes learned from that neighbor.

Syntax:

disable neighbor *IPv6 neighbor address*

Example: **`disable neighbor`**

```
Enter a Neighbor address or :: for all neighbors []? ::
neighbor 2003:1::6105 disabled
```

Dump Routing Tables

For a complete explanation of the **dump routing tables** command, refer to the **Dump Routing Tables** command on page "Dump routing tables" on page 410.

Example:

```
Type   Dest net/Prefix                            Cost Age  Next hop(s)/Net

BGPR   2001:6::/64                                0     193  IP64/0
BGPR   2001:7::/64                                0     187  IP64/0
BGPR   2001:9::/64                                0     200  IP64/0
BGPR   2001:17::/64                               0     200  IP64/0
 Dir*  2002:2::/64                                1     7889 Eth/1
RIP6   2002:5::/64                                3     10   FE80::220:35FF:FE45:2488
 Eth/1
RIP6   2002:6::/64                                2     10   FE80::220:35FF:FE45:2488
 Eth/1
RIP6   2002:9::/64                                2     10   FE80::220:35FF:FE45:2488
 Eth/1
RIP6   2002:99::/64                               3     10   FE80::220:35FF:FE45:2488
 Eth/1
RIP6   2002:1111::/64                             3     10   FE80::220:35FF:FE45:2488
 Eth/1
 Dir*  2003:1::/64                                1     7889 IP64/0

IPV6 Routing table size: 768 nets (79872 bytes), 11 nets known
                      0 nets hidden, 0 nets deleted, 1 nets inactive
                      0 routes used internally, 756 routes free
```

Enable Neighbor

Use the **enable neighbor** command to enable a particular neighbor or enable all neighbors that have been disabled. This command starts the BGP6 session with neighbor.

Syntax:

enable neighbor *IPv6 neighbor address*

Example:

```
Enter a Neighbor address or :: for all neighbors []? ::
neighbor 2003:1::6105 enabled
```

List

Use the **list** command to dump all BGP6 routing table entries, or to display information on routes advertised to, or received from, specified BGP6 neighbor addresses (destinations).

Syntax:

list all
dst_network *network address*
rt_rcved_from_nbr *network address*
rt_sent_to_nbr *network address*

all

Example:

```
BGP6> list all

MED   Weight LPref AAG AGRAS ORG AS-Path

0     0      0     No  0     IGP seq[2001]
Network/Prefixlen: 2001:6::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0      0     No  0     IGP seq[2001]
Network/Prefixlen: 2001:7::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0      0     No  0     IGP seq[2001]
Network/Prefixlen: 2001:9::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0      0     No  0     IGP seq[2001]
Network/Prefixlen: 2001:17::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0      0     No  0     IGP
Network/Prefixlen: 2002:2::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:5::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:6::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:9::/64
```

```
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:99::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:1111::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::
```

dst_network *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:

```
BGP6>list dst_network
Destination network prefix []? 2002:1111::
Do you want specify prefix len? [No]: y
Prefix len (0-128) [64]?

Destination: 2002:1111::/64
             Age:30, Upd#:4, LastSent: 0002:10:17

Eligible paths: 1
PathID: 0 - (Best Path)
        ASpath:
        Origin: IGP, Pref: 0, LocalPref: 0
        Metric: 0, Weight: 0, MED: 0
        NextHop:     2002:2::6202
        NextHop LLA: ::
        Neighbor:    2002:2::6202
        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.

rt_rcved_from_nbr *net address*

Lists all routes received from the specified BGP neighbor.

Example:

```
BGP6>list rt_rcved_from_nbr
BGP6 neighbor address []? 2003:1::6105

        Destinations obtained from BGP6 neighbor 2003:1::6105

MED   Weight LPref AAG AGRAS ORG AS-Path

0     0      0     No  0     IGP seq[2001]
Network/Prefixlen: 2001:9::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0      0     No  0     IGP seq[2001]
Network/Prefixlen: 2001:7::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0      0     No  0     IGP seq[2001]
Network/Prefixlen: 2001:17::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0      0     No  0     IGP seq[2001]
Network/Prefixlen: 2001:6::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B
```

rt_sent_to_nbr *net address*

Lists all routes advertised to the specified BGP neighbor.

Example:

```
BGP6>list rt_sent_to_nbr
BGP6 neighbor address []? 2003:1::6105

        Destinations advertised to BGP6 neighbor 2003:1::6105

MED   Weight LPref AAG AGRAS ORG AS-Path

0     0      0     No  0     IGP
Network/Prefixlen: 2002:9::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:5::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:99::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:1111::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0      0     No  0     IGP
Network/Prefixlen: 2002:6::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::
```

Neighbors

Use the **neighbors** command to display information on all active BGP6 neighbors.

Syntax:

neighbors *IPv6 neighbor address*

Example:

```
BGP6>neighbors

                                     Status State       DAY-HH:MM:SS   AS   Upd#
Address: 2003:1::6105
bgp6-ID: 20.1.7.5                    ENABLD Established 000-00:03:42   2001 11
```

IPv6-Address

Specifies the IPv6 address of the BGP6 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 BGP6 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 BGP6 connection has been successfully established, and can now start to exchange UPDATE messages.

BGP-ID
Specifies the neighbor's BGP6 Identification number.

AS Specifies the neighbor's AS number.

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

IPv6 neighbor address
Use the **neighbor** command to display detailed data on a particular BGP6 neighbor.

Example:

```
BGP6>neighbors 2000::662:0
Active Conn: None
Passve Conn: Sprt:179   Dprt:1026  State: Established KeepAlive/Hold Time: 30/90
TCP connection errors: 1          TCP state transitions: 1

BGP6 Messages:    Sent       Received                      Sent       Received
Open:             2          2          Update:            2          2
Notification:     1          0          KeepAlive:         2          2
Total Messages:   7          6

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:             1          0
```

Parameter

Use the BGP6 **parameter** command to display installed BGP6 globals in the BGP6 system.

Syntax:

parameter

Example:

```
compare-med-from-diff-as is disabled.
IPv6-route-table-scan-timer value is 1 seconds.
```

Paths

Use the BGP6 **paths** command to display the paths stored in the path description data base.

Syntax:

paths

Example:

```
paths
PathId MED   AAG AGRAS RefCnt ORG AS_PATH

0      0     No  0     6      IGP
Next Hop:     2002:2::6202
Next Hop LLA: ::

1      0     No  0     2      IGP seq[2001]
Next Hop:     2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

2      0     No  0     2      IGP seq[2001]
Next Hop:     2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B
```

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 BGP6 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.

Ping6

For an explanation of the **ping6** command, see “Ping6” on page 414.

Policy-List

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

Example:

```
BGP6>policy-list
Destination network prefix []? 2003:1::6105
Policy Type (Receive/Send/Origin) [All]?

Receive policy list for all neighbors:
Idx T Match OrgAS AdjAS IGPmet Usage  Prefix
1   I Range 0     0     0      5      2001::/16

AS-PATH with following ASs will be discarded:


Send policy list for all neighbor:
Idx T Match TAG   AdjAS Usage  Prefix
1   I Range 0     0     11     2002::/16

Origin policy list for all neighbor:
Idx T Match Tag   Usage  Prefix
1   I Range 0     6      2002::/16
BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? r

Receive policy list for neighbor '2000::1' :
Idx T Match OrgAS AnyAS MED   Weight LPref IGPmet Usage  Prefix
1   I Range 0     0     10    0      100   0      0      ::/0

BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? s

Send policy list for neighbor '2000::1' :
Idx T Match OrgAS AnyAS Tag   MED   ASpad Usage  Prefix
1   I Range 0     0     0     30    0     0      ::/0

BGP6>policy-list
Neighbor address []? 2000::1
Policy Type (Receive/Send/Origin) [All]? o

Origin policy list for all neighbor:
Idx T Match Tag   Usage  Prefix
1   I Range 0     2      ::/0
```

Reset Neighbor

Use the **reset neighbor** command to reset the specified BGP6 neighbor, based on the neighbor configuration parameters stored in the configuration memory.

Syntax:

reset neighbor *IPv6 neighbor address*

Example: **reset neighbor**

```
Enter a Neighbor address:  []? 2003:1::6105
resetting neighbor 2003:1::6105
```

Sizes

Use the BGP6 **sizes** command to display the number of entries stored in the various data bases.

Syntax:

sizes

Example:

```
sizes

        # Paths:                               10
        # Path descriptors:                    3
          Update sequence#:                    11
        # Routing tbl entries (allocated):     10
        # Current tbl entries (not imported):  0
        # Current tbl entries (imported to IGP): 4
```

Paths Total number of eligible paths for all the routes in the BGP6 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 BGP6 routing table.

Current tbl entries (not imported)
Indicates the number of BGP6 routes not imported into IGP.

Current tbl entries(imported to IGP)
Indicates the number of BGP6 routes imported into IGP.

Traceroute6

For an explanation of the **traceroute6** command, see “Traceroute6” on page 414.

BGP6 Dynamic Reconfiguration Support

This section describes dynamic reconfiguration (DR) as it affects Talk 6 and Talk 5 commands.

CONFIG (Talk 6) Delete Interface

Border Gateway Protocol for IPv6 (BGP6) supports the CONFIG (Talk 6) **delete interface** command with the following consideration:

> Deletes configured BGP6 external neighbors if the neighbor address has a common IPv6 prefix with an IPv6 address deleted on that interface.

GWCON (Talk 5) Activate Interface

The GWCON (Talk 5) **activate interface** command is not applicable for BGP6. BGP6 has no SRAM records associated with an interface.

GWCON (Talk 5) Reset Interface

The GWCON (Talk 5) **reset interface** command is not applicable for BGP6. BGP6 has no SRAM records associated with an interface.

GWCON (Talk 5) Component Reset Commands

BGP6 supports the following BGP6-specific GWCON (Talk 5) **reset** commands:

GWCON, Protocol Bgp6, Reset Neighbor Command

Description:
Adds or deletes a BGP6 neighbor. Changes neighbor parameters & policies.

Network Effect:
BGP6 neighbor connection and learned routes are updated based on configuration change.

Limitations:
None.

The following table summarizes the BGP6 configuration changes that are activated when the **GWCON, protocol bgp6, reset neighbor** command is invoked:

Commands whose changes are activated by the GWCON, protocol bgp6, reset neighbor command
CONFIG, protocol BGP6, add neighbor
CONFIG, protocol BGP6, change neighbor
CONFIG, protocol BGP6, delete neighbor
CONFIG, protocol BGP6, attach policy-to-neighbor
CONFIG, protocol BGP6, change policy-to-neighbor
CONFIG, protocol BGP6, delete policy-to-neighbor
CONFIG, protocol BGP6, add policy-list
CONFIG, protocol BGP6, update policy-list

GWCON (Talk 5) Temporary Change Commands

BGP6 supports the following GWCON commands that temporarily change the operational state of the device. These changes are lost whenever the device is reloaded, restarted, or you execute any dynamically reconfigurable command.

Commands
GWCON, protocol BGP6, enable neighbor
GWCON, protocol BGP6, disable neighbor

Non-Dynamically Reconfigurable Commands

The following table describes the BGP6 configuration commands that cannot be dynamically changed. To activate these commands, you need to reload or restart the device.

Commands
CONFIG, protocol BGP6, enable bgp6
CONFIG, protocol BGP6, disable bgp6
CONFIG, protocol BGP6, add no-receive
CONFIG, protocol BGP6, delete no-receive
CONFIG, protocol BGP6, add/change/delete/move aggregate
CONFIG, protocol BGP6, add/change/delete/move originate-policy
CONFIG, protocol BGP6, add/change/delete/move receive-policy
CONFIG, protocol BGP6, add/change/delete/move send-policy
CONFIG, protocol BGP6, enable compare-med-from-diff-as
CONFIG, protocol BGP6, set ipv6-route-table-scan-timer

Appendix. Packet Sizes

This appendix discusses the sizes of packets for the various networks and protocols supported. Included are the following sections:

- General Issues
- Network-Specific Size Limits
- Protocol-Specific Size Limits
- Changing Maximum Packet Sizes

General Issues

For the purposes of this discussion, the packets that the routers handle consist of user data and header information.

The amount of user data within a packet is limited by the amount of header information on the packet. The amount of header information depends on (at least):

- The network-types over which the packet must travel.
- The protocols in use on these networks.

The following factors affect the size of the packet contents:

- Length of the Data-Link header information that the current network type and interface require the packet to have.
- Length of the trailer information (if any) that the current network type and interface require the packet to have.

On any given network, the sum of the maximum data size together with header and trailer sizes will equal the network's maximum packet size. When routing between networks of different maximum packet size, fragmentation of the packet may result.

Network-Specific Size Limits

Given the information in the previous section, the maximum amount of network layer data supported by each data link layer (network interface) can be determined. Table 117 lists the default maximum packet sizes for common interface types.

Table 117. Default Network-Specific Maximum Packet Size

Network Type (Data Link)	Network Layer max packet size (bytes)	Length of Network Header	Information Trailer
Token-Ring 4-Mbps	2052	22	0
Token-Ring 16-Mbps	2052	22	0
Ethernet	1500	18	4
PPP	2046	2	0
Frame Relay	2048 (see notes)	variable	2

Note: For Frame Relay interfaces, you configure the maximum frame size not the network layer maximum packet size. To determine the maximum network layer packet size for a protocol, see the description of the **set frame-size** command in the chapter entitled Configuring and Monitoring Frame Relay Interfaces in *Access Integration Services Software User's Guide*.

4.

Packet Sizes

Note: You can change the maximum packet size for interfaces other than Ethernet. Use the **network** command from the `Config>` prompt to access the interface's configuration commands.

The maximum packet size is the maximum amount of data the protocol forwarder can pass to the device.

Note: These numbers correspond to the MTUs in 4.2 BSD UNIX.

For an IP packet, this includes the IP header, the UDP or TCP header, and all data.

The packet size in use is displayed when the router's GWCON memory command is used. The "Pkt" size is the Network layer packet size. The Hdr (header) and Tlr (trailer) sizes depend on the networks and their network interfaces.

Protocol-Specific Size Limits

This section explains the protocol-specific size limits.

IP Packet Lengths

The IP protocol specifications do not require a host IP implementation to accept IP packets of more than 576 octets; however, router IP implementations must accommodate IP packets of any length up to the limits imposed by the network-specific packets in use.

Furthermore, router IP performs transparent fragmentation and reassembly of packets that would otherwise exceed network-specific length restrictions, as required by the IP specification.

Packet size mismatches do not cause connectivity problems. However, fragment reassembly does pose a performance penalty, so fragmentation should be avoided whenever possible.

Changing Maximum Packet Sizes

Normally, the router automatically sets the maximum network layer packet size to the size of the largest possible packet on all the connected networks. It then adds any headers and trailers required by the networks to determine the internal buffer size, which is larger than the network layer size.

Some networks (Token-Ring 4 Mbps and Token-Ring 16 Mbps) allow you to configure maximum packet sizes. Configuring maximum packet sizes affects the size of buffers used on the router and this in turn affects the number of buffers available for a given memory size. Routers automatically determine what size buffer it is going to need. You can change the maximum Network layer packet size that the router handles by using the set packet-size command; however, do not use this command unless specifically directed to by Customer Service.

List of Abbreviations

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/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

ATP AppleTalk Transaction Protocol

AUI attachment unit interface

ayt are you there

BAN Boundary Access Node

BBCM Bridging Broadcast Manager

BECN backward explicit congestion notification

BGP Border Gateway Protocol

BNC bayonet Niell-Concelman

BNCP Bridging Network Control Protocol

BOOTP BOOT protocol

BPDU bridge protocol data unit

bps bits per second

BR bridging/routing

BRS bandwidth reservation

BSD Berkeley software distribution

BTP BOOTP relay agent

BTU basic transmission unit

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

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

E&M Ear & Mouth

E1 2.048 Mbps transmission rate

EDEL end delimiter

EDI error detected indicator

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

ELAN Emulated LAN

ELAP EtherTalk Link Access Protocol

ELS Event Logging System

ELSCon
Secondary ELS Console

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

FXO Foreign Exchange Office

FXS Foreign Exchange Station

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

HPR high-performance routing

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

Ifc# interface number

IGP interior gateway protocol

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

LCS LAN Channel Station

LCP Link Control Protocol

LED light-emitting diode

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

LSA Link Services Architecture

LSB least significant bit

LSI LAN 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

MOSDBG
Micro Operating System Debugging Tool

MOSPF
Open Shortest Path First with multicast extensions

MPC Multi-Path Channel

MPC+ High performance data transfer (HPDT) Multi-Path Channel

MSB most significant bit

MSDU MAC service data unit

MRU maximum receive unit

MTU maximum transmission unit

nak not acknowledged

NAS Nways Switch Administration station

NBMA Non-Broadcast Multiple Access

NBP Name Binding Protocol

NBR neighbor

NCP Network Control Protocol

NCP Network Core Protocol

NDPS non-disruptive path switching

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

OOS Out of Service

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

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

s second

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

seqno sequence number

SGID sever group id

SGMP Simple Gateway Monitoring Protocol

SL serial line

SMP standby monitor present

SMTP Simple Mail Transfer Protocol

SNA Systems Network Architecture

SNAP Subnetwork Access Protocol

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

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

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

UTP unshielded twisted pair

VCC Virtual Channel Connection

VINES VIrtual NEtworking System

VIR variable information rate

VL virtual link

VNI Virtual Network Interface

VoFR Voice over Frame Relay

VR virtual route

WAN wide area network

WRS WAN restoral/reroute

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

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. (1) Operational. (2) Pertaining to a node or device that is connected or is available for connection to another node or device.

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.

agent. A system that assumes an agent role.

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)

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

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).

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)

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)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems.

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*.

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)

CCITT. International Telegraph and Telephone Consultative Committee. This was an organization of the International Telecommunication Union (ITU). On 1 March 1993 the ITU was reorganized, and responsibilities for standardization were placed in a subordinate organization named the Telecommunication Standardization Sector of the Telecommunication Union (ITU-TS). "CCITT" continues to be used for recommendations that were approved before the reorganization.

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)*.

channelization. The process of breaking the bandwidth on a communication line into a number of channels, possibly of different size. Also called ***time division multiplexing*** (TDM).

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.

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 database (CDB). A database that stores the configuration parameters of one or several devices. It is prepared and updated using the configuration program.

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*.

connection. In data communication, an association established between functional units for conveying information. (I) (A)

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)

dependent LU requester (DLUR). An APPN end node or an APPN network node that owns dependent LUs, but requests that a dependent LU server provide the SSCP services for those dependent LUs.

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.

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.

EIA unit. A unit of measure, established by the Electronic Industries Association, equal to 44.45 millimeters (1.75 inches).

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.

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. An example of an EGP is the Border Gateway Protocol (BGP). Contrast with Interior Gateway Protocol (IGP).

F

fax. Hardcopy received from a facsimile machine. Synonymous with ***telecopy.***

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.

flash memory. A data storage device that is programmable, erasable, and does not require continuous power. The chief advantage of flash memory over other programmable and erasable data storage devices is that it can be reprogrammed without being removed from the circuit board.

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.

front-end processor. A processor such as the IBM 3745 or 3174, that relieves a main frame from the communication control tasks.

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.

high-performance routing (HPR). An addition to the Advanced Peer-to-Peer Networking (APPN) architecture that enhances data routing performance and reliability, especially when using high-speed links.

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.

hub (intelligent). A wiring concentrator, such as the IBM 8260, that provides bridging and routing functions for LANs with different cables and protocols.

hysteresis. The amount the temperature must change past the set alert threshold before the alert condition is cleared.

I

I-frame. Information frame.

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 Digital Network Exchange (IDNX). A processor integrating voice, data, and image applications. It also manages the transmission resources, and connects to multiplexers and network management support systems. It allows integration of equipment from different vendors.

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).

interleaving. (1) The alternating of two or more operations or functions through the overlapped use of a computer facility. (2) In data transmission, the alternating of packets from one data stream with packets from another.

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.

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)*.

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.

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.

IPPN. The interface that other protocols can use to transport data over IP.

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).

J

jitter. (1) Short-term non-cumulative variations of the significant instants of a digital signal from their ideal positions in time. (2) Undesirable variations of a transmitted digital signal. (3) Variations in the network delay.

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 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.

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)*.

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. (1) MIB module. (2) Management Information Base.

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.

module. In the Nways Switch, a packaged functional hardware unit containing logic cards, connectors, and lights. The modules are used to package adapters, line interface couplers, voice server extensions, and other components. All modules are ***hot pluggable*** in the logic subracks.

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.

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.

multipath channel (MPC). A channel protocol that uses multiple unidirectional subchannels for VTAM-to-VTAM bidirectional communication.

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 Access Server (NAS). A device providing temporary, on-demand network access to users. This access is point-to-point using PSTN or ISDN lines.

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*.

network support station. The processor used to locally operate and service the Nways Switch. It is used by the Nways Switch administrator or service personnel.

network user address (NUA). In X.25 communications, the X.121 address containing up to 15 binary code digits.

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*.

Non-Return-to-Zero Changes-on-Ones Recording (NRZ-1). A recording method in which the ones are represented by a change in the condition of magnetization, and zeros are represented by the absence of change. Only the one signals are explicitly recorded. (Previously called ***non-return-to-zero inverted***, NRZI, recording.)

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.

Nways Switch. Synonymous with IBM 2220 Nways BroadBand Switch.

Nways Switch configuration station. A dedicated OS/2 station running a stand-alone version of the Nways Switch Configuration Tool (NCT). It is used to generate a network configuration database and should be installed as a remote console.

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 loss ratio. The probability that a packet will not reach its destination or not reach it within a specified time.

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.

private branch exchange (PBX). A private telephone exchange for transmission of calls to and from the public telephone network.

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)

| **pulse code modulation (PCM).** A standard adopted for the digitalization of an analog voice signal. In PCM, the voice is sampled at a rate of eight kHz and each sample is coded in an 8-bit frame.

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.

real-time processing. The manipulation of data that are required, or generated, by some process while the process is in operation. Usually the results are used to influence the process, and perhaps related processes, while it is occurring.

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 console. A station running OS/2, TCP/IP, and the remote Nways Switch Resource Control program. It can be connected to any network support station to operate and service the Nways Switch remotely.

The connection may be through:
- A switched line using a modem

Any network support station can be used as a remote console of another network support station.

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.

resource. In the Nways Switch, an hardware element or a logical entity created by the Control Program. For example, the adapters, LICs, and lines are physical resources. The control points and connections are logical resources.

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

SAP. See service access point.

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.

Serial Line Internet Protocol (SLIP). A protocol used over a point-to-point connection between two IP hosts over a serial line, for example, a serial cable or an RS232 connection into a modem, over a telephone line.

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 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).

SNA management services (SNA/MS). The services provided to assist in management of SNA networks.

socket. (1) An endpoint for communication between processes or application programs. (2) The abstraction provided by the University of California's Berkeley Software Distribution (commonly called Berkeley UNIX or BSD UNIX) that serves as an endpoint for communication between processes or applications.

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 mask. Synonym for *address mask*.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

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)*.

synchronous optical network (SONET). A US standard for transmitting digital information over optical interfaces. It is closely related to the synchronous digital hierarchy (SDH) recommendation.

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. In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions. (I) (A)

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

TCP/IP. (1) Transmission Control Protocol/Internet Protocol. (2) A UNIX-like/Ethernet-based system-interconnect protocol originally developed by the US Department of Defense. TCP/IP facilitated ARPANET (Advanced Research Projects Agency Network), a packet-switched research network for which Layer 4 was TCP and Layer 3, IP.

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 division multiplexing (TDM). See ***channelization***.

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.

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) 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.

trunk line. A high-speed line connecting two Nways Switches. It can be a coaxial cable, fiber cable, or radio wave, for example, and may be leased from telecommunication companies.

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.

U

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.34. An ITU-T Recommendation for modem communication over standard commercially available voice-grade 33.6-Kbps (and slower) channels.

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.

version. A separately licensed program that usually has significant new code or new function.

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 connection. In frame relay, the return path of a potential connection.

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 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

E

M

N

O

P

U

V

W

Readers' Comments — We'd Like to Hear from You

Access Integration Services
Protocol Configuration and Monitoring
Reference Volume 2
Version 3.4

Publication No. SC30-3991-02

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
SC30-3991-02

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

SC30-3991-02

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC30-3991-02

Spine information:

Access Integration Services

AIS V3.4 Protocol Reference V2