Nways Multiprotocol Access Services

SC30-3885-00

Protocol Configuration and Monitoring Reference Volume 2
Version 1 Release 1

Nways Multiprotocol Access Services

SC30-3885-00

Protocol Configuration and Monitoring Reference Volume 2 Version 1 Release 1

Note

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

First Edition (March 1997)

This edition applies to Version 1 Release 1 of the IBM Nways Multiprotocol Access 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
USA

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

Contents

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

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

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

Trademarks

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

Advanced Peer-to-Peer Networking	IBM	RISC System/6000
AIX	Micro Channel	System/370
AIXwindows	NetView	VTAM
APPN	Nways	
BookManager	PS/2	

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

Preface

This manual contains the information you will need to configure bridging and routing functions on an Nways device. The manual describes all of the features and functions that are in the software. A specific Nways device might not support all of the features and functions described. If a feature or function is device-specific, a notice in the relevant chapter or section indicates that restriction.

This manual supports the IBM 2216 and refers to this product as either “the router” or “the device.” The examples in the manual represent the configuration of an IBM 2216 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.

To Get 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 diskette 1 of the configuration program diskettes. You can view the file with an ASCII text editor.

About the Software

IBM Nways Multiprotocol Access Services is the software that supports the IBM 2216 (licensed program number 5765-B87). 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 IBM Nways Multiprotocol Access 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 2216.
- The Configuration Program for IBM Nways Multiprotocol Access Services (*Configuration Program*), a graphical user interface that allows 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 preloaded at the factory; it is shipped separately from the device as part of the software order.

  You can also FTP the Configuration Program for IBM Nways Multiprotocol Access Services. See *Configuration Program User’s Guide for Nways Multiprotocol Access Services Version 1 Release 1,* 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 shown in the following example:

   rel**oad**

   In this example, you can enter either the whole command (reload) or its abbreviation (rel).

2. 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.

3. In information displayed in response to a command, defaults for an option are enclosed in brackets immediately following the option. For example:

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

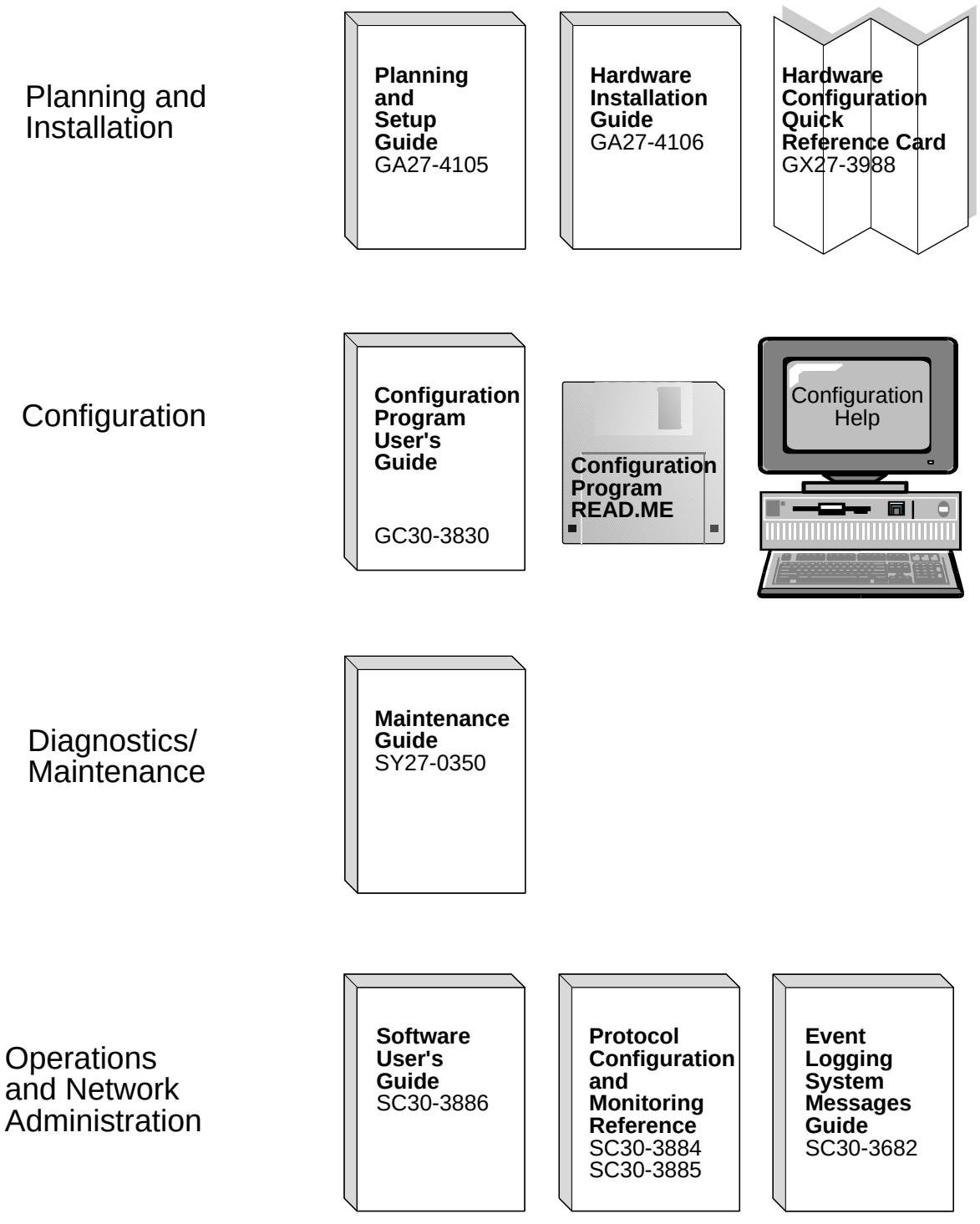
   In this example, the media defaults to UTP unless you specify STP.

4. Keyboard key combinations are indicated in text in the following ways:

   Ctrl-P

   Ctrl P

Common Tasks and the IBM 2216 Library



Library Overview

The following list shows the books in the IBM 2216 library, arranged according to tasks.

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 2216 home pages at:

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

Planning

GA27-4105 *IBM 2216 Multiaccess Connector Planning and Setup Guide*

This book is shipped with the IBM 2216. It explains how to prepare for installation and perform an initial configuration.

Installation

GA27-4106 *IBM 2216 Nways Multiaccess Connector Hardware Installation Guide*

This booklet is shipped with the IBM 2216. It explains how to install the IBM 2216 and verify its installation.

GX27-3988 *2216 Nways Multiaccess Connector 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 2216.

Diagnostics and Maintenance

SY27-0350 *2216 Nways Multiaccess Connector Maintenance Guide.*

This book is shipped with the IBM 2216 It provides instructions for diagnosing problems with and repairing the IBM 2216.

Operations and Network Management

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

SC30-3886 *Nways Multiprotocol Access Services Software User's Guide*

This book explains how to:

- Configure, monitor, and use the Nways Multiprotocol Access Services software.
- Use the Nways Multiprotocol Access Services command-line router user interface to configure and monitor the network interfaces and link-layer protocols shipped with the IBM 2216.

SC30-3884 *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 1*

SC30-3885 *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*

These books describe how to access and use the Nways Multiprotocol Access 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 *Nways 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*

This book discusses how to use the Nways Multiprotocol Access Services Configuration Program.

Safety

SD21-0030 *Caution: Safety Information—Read This First*

This book, shipped with the IBM 2216, provides translations of caution and danger notices applicable to the installation and maintenance of a IBM 2216.

Marketing

URL: **http://www.networking.ibm.com/216/216prod.html**

This IBM Web page provides product information through the World Wide Web.

Chapter 1. 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 1-15 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 predefining 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 1-1 on page 1-4. 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 1-15.

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 1-1. Implementation of APPN Network Node Functions on the IBM 2216

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
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		
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 or V.25 bis
   - Frame relay links running over ISDN
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 and token-ring ports only.

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:

1002 Adjacent Link Station name

1007 Parallel TGs

1012 LU name = CP name

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

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

Node performance tuning

Node service traces

Accounting and node statistics collection

High Performance Routing

HPR is an enhancement to APPN architecture that provides better performance over high speed, low error rate links using existing hardware. HPR replaces the normal APPN intermediate session routing (ISR) with a Network Control Layer (NCL) containing a new type of source routing function called automatic network routing (ANR). The complete HPR route is contained in the ANR packet allowing intermediate routing nodes to route the packets with less processing overhead and storage.

HPR also eliminates the error recovery and flow control (session-level pacing) procedures for each link between nodes and moves the error recovery and flow/congestion control procedures to the end-points of an HPR connection. A transport layer using a new error recovery procedure called Rapid Transport Protocol (RTP) is used by the endpoints of the HPR connection. HPR intermediate

nodes have no session or RTP connection awareness. This new transport layer features:

- Selective retransmission error recovery procedure
- Segmentation and reassembly
- Adaptive Rate-Based (ARB) flow and congestion control mechanism that meters data onto a route that allows efficient utilization of network resources while minimizing congestion. ARB uses a preventative rather than reactive approach to flow and congestion control.
- Nondisruptive 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 bridged frame format and the RFC 1490 routed frame format.

  – RFC 1490 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 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 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 routed frame format because there is no layer 2 protocol.

  – RFC 1490 Bridged format

    APPN HPR uses a SAP for traffic transferred using the RFC 1490 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 encapsulation, no SAP is used for HPR traffic.

Refer to Table 2-1 on page 2-1 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 2-1 on page 2-1 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. If the Border Node (either the same netid or different netid) is used, the DLUR can reside in a different (sub-)network than DLUS.

VTAM Considerations for DLUR

The following are example VTAM Switched Major Node definitions for DLUR. You should note that PATH statements are necessary only if VTAM is initiating the connection to the DSPU.

You should refer to *VTAM Resource Definition Reference*, SC31-6427, for details of the DLC parameter statements for the Switched Major Node definitions.

```
DABDLURX VBUILD TYPE=SWNET,MAXGRP=400,MAXNO=400,MAXDLUR=20
************************************************************************
*IN THE DLCADDR, THE 'SUBFIELD_ID' = CV SUBFIELD OF THE CV91           *
* MINUS 0X90.                                                          *
*FOR EXAMPLE, THE CV94 SUBFIELD IS CODED ON DLCADDR=(4,X,...           *
************************************************************************
************************************************************************
* Following are PU Statements for 2.0 and for 2.1
************************************************************************
************************************************************************
* 2.0 PU STATEMENT
************************************************************************
*PU20RT   PU   ADDR=05,PUTYPE=2,MAXPATH=8,ANS=CONT,USSTAB=AUSSTAB,
*              ISTATUS=ACTIVE,MAXDATA=521,IRETRY=YES,MAXOUT=7,
*              PASSLIM=5,IDBLK=017,IDNUM=00035,MODETAB=AMODETAB
*              LOGAPPL=ECHO71,DLOGMOD=M23278I 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 codings 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 codings 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

APPN Connection Network

When nodes are attached to a shared-access transport facility (SATF), any-to-any connectivity is possible. This any-to-any connectivity allows direct connections between any two nodes, eliminating routing through intermediate network nodes and the corresponding data traversing the SATF multiple times. To achieve this direct connectivity, however, TGs must be defined on each node for all the other possible partners.

Defining connections between all possible pairs of nodes attached to the SATF results in a large number of definitions (increasing on the order of the square of the number of nodes involved) and also a large number of topology database updates (TDUs) flowing in the APPN network. To alleviate these problems, APPN allows nodes to become members of a connection network to represent their attachment to an SATF. Session traffic between two nodes that have been defined as members of a connection network can be routed directly, without passing through a network node (achieves direct connectivity). To become a member of a connection network, an APPN node's port must be "attached" to a Connection Network by defining a connection network interface. When the port is defined, a Connection Network TG is created by the APPN component to identify the direct connection from the port to the SATF (i.e. the connection network). This TG is not a conventional TG as in the case of defined link stations, but rather represents the connection to the Connection Network in the topology database.

Note: TGs for end nodes are not contained in the network topology database, but are contained in the node's local topology database. TDUs do not flow through the network when a connection is established through a Connection Network or when an end node is made a member of a Connection Network.

Because the connectivity is represented by a TG from a given node to a Connection Network, normal topology and routing services (TRS) can be used for the network node server to calculate the direct path between any two nodes attached to the SATF (with TGs to the same Connection Network). DLC signaling information is returned from the destination node during the normal locate process to enable the origin node to establish a connection directly to the destination node.

Therefore, to achieve direct connectivity on an SATF, instead of each node on the SATF being defined (or connected) to each other, each node is connected to a Connection Network. The Connection Network is often visualized as a virtual node on the SATF to which all other nodes are attached. This model is frequently used and, in fact, the term Virtual Routing Node (VRN) is often interchanged with the term Connection Network.

When a connection network is defined, it is named. This name then becomes the CP name of the VRN and must follow all the requirements of any CP name. See Table 2-20 on page 2-79 for a list of these requirements.

Restrictions

- Connection networks defined on the router network node are only supported on token-ring and Ethernet LAN ports.
- 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.

- The same connection network can be defined on a maximum of five ports to the same LAN on the router network node.
- There is only one connection network TG from a given port to a given connection network's VRN.
- The same connection network TG characteristics apply for each port on which a given connection network is defined on this router network node. The TG characteristics could be different on a different node.
- 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.

Managing a Network Node

You can manage the router network node as an APPN entry point, which forwards APPN-related alerts to an APPN focal point, or as an SNMP-managed node.

The router supports MIBs for APPN, HPR, DLUR and SNANAU. The router network node sends alerts to a focal point. For additional information on APPN problem management services, refer to the *Protocol Configuration and Monitoring Reference Volume 1 for Nways Multiprotocol Access Services Version 1 Release 1*, Appendix A.

How the Network Node Functions as an Entry Point 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 the focal point node is not available to receive an alert from the router network node, the alert is “held” (stored) by CPMS. APPN on the router can hold up to 10 alerts.

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 is an explicit focal point.

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 that attempt fails, the router switches to the backup focal point. The primary focal point is then

responsible for reestablishing the focal-point-to-entry-point relationship with 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.

How the Network Node Functions as an SNMP-Managed Node

The router network node can function as an SNMP-managed node. 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.

As an SNMP-managed node, the router sends unsolicited status and error information to a focal point.

Chapter 2. Configuring Advanced Peer-to-Peer Networking (APPN)

This chapter describes the APPN configuration process and includes the following sections:

Supported DLCs

Table 2-1 shows the DLC ports supported by the router over APPN:

Table 2-1. Port Types Supported for APPN Routing

Port Type	Standard	HPR	ISR	DLUR*
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) **		Yes	Yes	Yes
Serial LAN bridging		NA	NA	NA
SDLC		No	Yes	Yes
X.25	CCITT X.25	No	Yes	Yes
DLSw (remote only) ***		No	Yes	Yes
APPN/PPP/ISDN		Yes	Yes	No
APPN/FR/ISDN		Yes	Yes	Yes
APPN/PPP/V.25 bis		Yes	Yes	No
LANE	Forum compliant	Yes	Yes	Yes

Notes:

1. * This column refers to the port providing the connection to the downstream PU (DSPU).
2. ** Use bridged format when you have two routers connected by frame relay and one of them does not have APPN. Otherwise, use routed format because of improved performance.
3. *** Since APPN runs over DLSw and DLSw runs over X.25, you can route APPN ISR traffic over X.25 by running APPN over DLSw.

Router Configuration Process

This section describes the router configuration process and includes details about parameters.

Configuration Changes That Require the APPN Function to Restart

- Network ID of the network node
- Control point name of the network node
- XID number (of network node) for subarea connection
- Adjacent node type (of link station)
- Any parameters under the following options:
  - High Performance Routing (HPR) at the node level
  - Dependent LU Requester (DLUR) at the node level
  - Connection network
  - Class of service
  - Node tuning
  - Node management
  - Mode name mappings

Configuration Requirements for APPN

APPN routing is configured on the individual adapters supporting the DLC desired. To use APPN routing, at least one of the following DLCs must be configured and enabled:

- 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
- DLSw

You can configure these APPN Network Node Features:

- High Performance Routing parameters (optional)
- Connection Networks for LAN ports (optional)
- Dependent LU Requester (optional)

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 2-4.

Use the following procedure for minimum configuration steps:

1. If you are configuring APPN using a DLSw port:
   a. Enable bridging on the node
   b. Enable DLSw on the node
   c. Define the DLSw port with a locally administered MAC address for DLSw.
2. Enable APPN routing on the port.

   Note: Since *Service Any* is enabled by default, the node accepts any request for a connection that it receives from another node.
3. Enable the APPN Network Node.
4. Configure the following parameters:
   - Network ID
   - Control point name
5. Define the XID number for subarea connections parameter for the APPN network node (optional).
6. Accept all other defaults.
7. Optionally do the following:
   - Modify High Performance Routing parameters
   - Configure Dependent LU Requester
   - Define Connection Networks
   - Define new COS names or mode name mappings
   - Tune the performance of this node
   - Perform node service trace diagnostics

- Collect statistics for this network node

Notes:

1. APPN routing must be defined and enabled on the specific ports you configure the router network node to use.
2. Bridging and DLSw must still be enabled on the specific adapter ports you desire the router 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 2-3.

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
   - DLSw
   - SDLC

3. Enable APPN routing on APPN ports with the *enable APPN routing on this port* parameter.

   Note: Since *Service Any* is enabled by default, the node accepts any request for a connection that it receives from another node.

4. Define APPN link stations on the selected DLC ports for the adjacent nodes to which this network node may initiate a connection.

   Note: Link stations do not have to be defined on every port, only those over which you want to initiate connections to adjacent nodes.

5. Enable the APPN network node.
6. Configure the following parameters for the APPN network node:
   - Network ID
   - Control point name
7. Define the XID number for subarea connections parameter for the APPN network node (optional).
8. Accept all other defaults
9. Optionally do the following:
   - Modify High Performance Routing parameters
   - Configure Dependent LU Requester
   - Define Connection Networks
   - Define new COS names or mode name mappings
   - Tune the performance of this node
   - Perform node service trace diagnostics
   - Collect statistics for this network node

Controlling Connections Configuration

This group of APPN configuration steps:

- Allows the network node to accept requests only from nodes that you specify.
- Enables the network node to initiate connections with other nodes that you specify, including LEN end nodes.

This configuration provides a higher level of security because you explicitly define which APPN nodes may communicate with this router network node. A connection request from an adjacent node will be accepted only if its fully qualified CP name parameter has been configured on this network node. This group of configuration steps optionally enables you to have a secure link with each adjacent node by configuring the session level security feature for each link.

Use the following procedure for the controlling connections configuration:

1. Select ports over which you desire to establish connections to adjacent nodes from the following DLC port types supported by APPN:
   - Token-ring LAN port
   - Ethernet LAN port
   - Frame-relay serial port
   - PPP serial port
   - X.25
   - DLSw
   - SDLC

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

High Performance Routing

See Chapter 2, “Configuring Advanced Peer-to-Peer Networking (APPN)” on page 2-1 for a list of ports that support HPR.

See “Configuration Requirements for APPN” on page 2-2 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 Chapter 2, “Configuring Advanced Peer-to-Peer Networking (APPN)” on page 2-1 for a list of ports that support DLUR.

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 APPN's behalf.

COS Options

You can use a template to create new user-defined COS names and associated definitions for TGs and nodes which can be used with new mode names or mapped to existing mode names.

In addition you can create new mode names that can be mapped to existing COS names.

Each COS definition file is identified by a COS name and contains an associated transmission priority and a table of ranges of acceptable TG and node characteristics that APPN compares against actual TG and node characteristics to determine weights for TGs and nodes from which APPN calculates the least weight route for the session. Using the Configuration Program you can:

- View a COS definition file:
  - View the transmission priority
  - View a list of node row references along with their corresponding weights
  - View a list of TG row references along with their corresponding weights
- Use a template 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:

- Define a new mode name and its mapping to a COS name.
- Change a mode name to COS name mapping:
  - Remap an IBM-defined mode name to a different COS name.

– Remap a previously specified user-defined mode name to a different COS name.

APPN Node Tuning

The performance of the router APPN network node can be tuned in two ways:

- By manually setting the values of the *maximum shared memory*, *percent of APPN shared memory to be used for buffers*, and the *maximum cached directory entries* tuning parameters using the **talk 6** option of the command line interface.
- By selecting values for the *maximum number of ISR sessions*, *maximum number of adjacent nodes* and other parameters shown in Table 2-7 on page 2-55, 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. The *maximum cached directory entries* parameter affects the amount of directory information that will be stored or cached to reduce the time it takes to locate a resource in the network.

In general, tuning the APPN network node involves a trade-off between node performance and storage usage. The better the performance, the more storage required.

Tuning Notes

1. The tuning parameter settings should reflect anticipated growth in your network.
2. If you define connection networks within your APPN network and you anticipate that most end nodes will initiate LU-LU sessions with other end nodes on the same connection network, you should set the *maximum number ISR sessions* parameter to a smaller value (1). Using connection networks in this manner reduces the shared memory requirements for the router network node because most LU-LU sessions will not flow through the APPN component in the router.
3. Because the *maximum shared memory* parameter affects storage allocation within the router, you should use care when explicitly defining this parameter. Use the defaults as a guide when increasing or reducing maximum shared memory manually.

Node Service (Traces)

The APPN Node Service (Traces) option allows you to start any APPN trace through **talk 6** or the Configuration Program. The traces are activated when the configuration file is applied to the router. The traces will continue to be active until they are stopped when a new configuration that stops the traces is applied to the router.

Note: Running traces on the router can affect its performance. Traces should be started only when needed for node service and should be stopped as soon as the required amount of trace information is gathered.

The APPN traces are grouped into the following 5 categories:

- Node-level traces specify traces concerning the overall APPN network node.

- Interprocess 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.

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).

You can enable or disable the *collect intermediate session information* using:

- Configuration Program
- Command line **talk 6**
- SNMP **SET** command

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 Nways Multiprotocol Access Services Version 1 Release 1* 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 nondisruptive 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 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 nondisruptive UNBIND:
  1. Wait for the amount of time specified by the *Delay before initiating retries* parameter. This delay allows time for an SSCP takeover, where the pipe would be reestablished by a new DLUS without action on the DLUR's part.
  2. Attempt to reach the primary DLUS.
  3. If unsuccessful, attempt to reach the backup DLUS.
  4. If the attempt to reach the backup DLUS is unsuccessful, DLUR will retry as described in steps 5 - 7 as long as the DSPU is requesting ACTPU.
  5. Wait for the amount of time specified by the *Long retry timer*.

     Note: If *Perform long retries to restore disrupted pipe* is No, no further retries will be attempted.
  6. Attempt to reach the primary DLUS.
  7. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS.
- For all other cases of pipe failure, DLUR will try the primary DLUS and then the backup DLUS immediately. If this fails, DLUR will:

1. Wait for the amount of time specified by the minimum of the *short retry timer* and the *Delay before initiating retries* parameters.
2. Attempt to reach the primary DLUS.
3. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS
4. If pipe activation continues to fail, DLUR will retry as described in steps 1 - 3 for the number of times specified in the *short retry count*.

   If the *short retry count* is exhausted, DLUR will retry as defined in steps 5 - 7 as long as the DSPU is requesting ACTPU.
5. Wait for the amount of time specified by the *Long retry timer*

   Note: If *Perform long retries to restore disrupted pipe* is No, no further retries will be attempted.
6. Attempt to reach the primary DLUS.
7. If the attempt to reach the primary DLUS is unsuccessful, attempt to reach the backup DLUS.

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 2-1. This support allows customers with DLSw configurations to migrate their networks to 2216.

Note: It is recommended to use APPN over direct DLCs when available instead of APPN over DLSw.

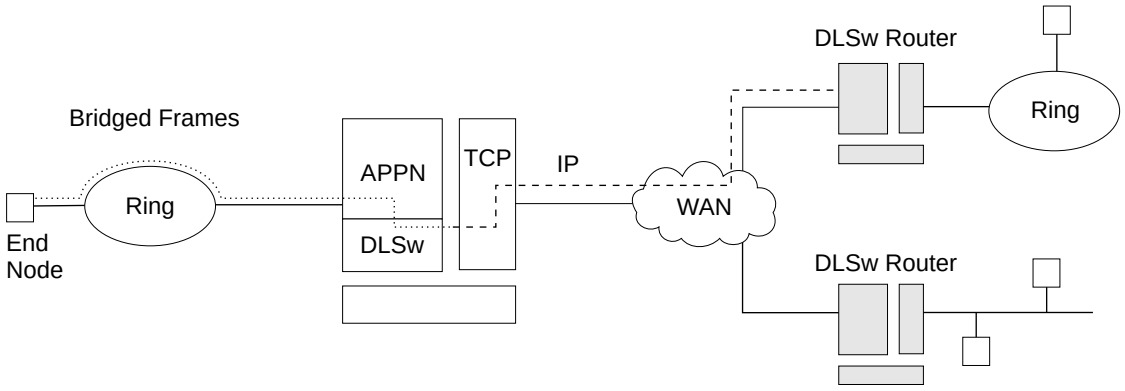


Figure 2-1. Data Flow in an APPN Configuration Using DLSw Port

APPN configuration restrictions using DLSw:

- Connectivity through remote DLSw partners only
- Only 1 DLSw port per router
- Use of a locally administered MAC address
- HPR is not supported on DLSw ports
- DLSw ports cannot be members of connection networks
- Parallel TGs are not supported on DLSw ports

See “Configuring the Router as an APPN Network Node” on page 2-2 to configure APPN using DLSw.

How APPN Uses DLSw ports to Transport Data

When APPN is configured on the router to use Data Link Switching (DLSw) port, DLSw is used to provide a connection-oriented interface (802.2 LLC type 2) between the APPN component in the router and APPN nodes and LEN end nodes attached to a remote DLSw partner.

When configuring a DLSw port for APPN on the router, you assign the network node a unique MAC and SAP address pair that enables it to communicate with DLSw. The MAC address for the network node is locally administered and must not correspond to any physical MAC address in the DLSw network.

Port Level Parameter Lists

Use the following tables to configure APPN ports:

- Port Configuration on page 2-69
- Port Definition on page 2-72
- Port Default TG Characteristics on page 2-73
- Port default LLC Characteristics on page 2-76

Link Level Parameter Lists

Use the following tables to configure APPN link stations:

- HPR Defaults on page 2-78
- Link Station - Detail on page 2-79
- Modify TG Characteristics on page 2-85
- Modify Dependent LU Server on page 2-87
- Modify LLC Characteristics on page 2-88
- Modify HPR Defaults on page 2-90

LU Parameter List

Use the following table to configure an LU:

- LEN End Node LU Name on page 2-91

Node Level Parameter Lists

Use the following tables to configure an APPN node:

- APPN Routing on page 2-47
- High Performance Routing (HPR) on page 2-49
- HPR Timer and Retry Options on page 2-49
- Dependent LU Requester on page 2-52
- Connection Network - Detail on page 2-92
- TG Characteristics (Connection Network) on page 2-93
- APPN COS - Additional port to Connection Network on page 2-96
- Node Level Traces on page 2-58
- Interprocess Signals Traces on page 2-61
- Module Entry and Exit Traces on page 2-63
- General Component Level Traces on page 2-64
- APPN Node Management on page 2-67

APPN Configuration Notes

The following examples show special parameters to consider when configuring various features to transport APPN traffic.

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
0d>li all

 Base net                       = 3
 Destination name               = 2216-01
 Circuit priority               = 8
Destination address: subaddress = 99199994301:

 Inbound destination name       = 2216-01
Inbound dst address: subaddress = 99199994301:

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

0d>ex

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

Config>n 6
Circuit configuration
0d>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
 ------------------------------ ------- ---------- ------- ------- -------
2216-21-i6          2             16     Permanent 64000    64000     0

  = circuit is required and belongs to a required PVC group
```

```
FR Config>
0d>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,
(S)DLC, (X)25, (D)LSw [  ] ? 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 ] ?
 Maximum number of link stations (1-976) [512 ] ?
 Percent of link stations reserved for incoming calls (0-100) [0 ] ?
 Percent of link stations reserved for 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

Refer to the *Software User's Guide for Nways Multiprotocol Access Services Version 1 Release 1* 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 re-establish 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 may want to configure this link so that CP-CP sessions do not use it. If you allow CP-CP sessions on this link, the link will not disconnect.
- 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.

```
*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
0d>li all

Base net                        = 6
Destination name                = 2216-15
Circuit priority                = 8

Inbound destination name        = 2216-15

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

0d>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,
(S)DLC, (X)25, (D)LSw [  ] ? 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 Nondisruptive 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 2 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 (2216-06) is going the be the destination of the Wan Reroute
**************************************************************************
Config>n 4
Circuit configuration
0d>li

 Base net                      = 3
 Destination name              = 2216-06  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,
(S)DLC, (X)25, (D)LSw [  ] ? 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 2216-22 so when NN22 calls into NN6,
*  it will map to interface 17
*
**************************************************************************
 11
Config> n 17
Circuit configuration
0d>fea      li all

Base net                        = 6
Destination name                = 2216-22
Circuit priority                = 8

Inbound destination name        = 2216-22

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

0d>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,
(S)DLC, (X)25, (D)LSw [  ] ? 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
0d>li al

Base net                        = 6
Destination name                = 2216-35
Circuit priority                = 8

Inbound destination name        = 2216-35

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

0d>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

V.25bis Configuration

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

```
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 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>
```

Notes:

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

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 Nways Multiprotocol Access Services Version 1 Release 1 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
```

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

Configuring APPN over X.25

This example shows APPN configuration for an X25 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,
(S)DLC, (X)25, (D)LSw[ ]? 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 (1-239)[239]?
        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>
```

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 2-2. APPN Configuration Command Summary

Command	Function
? (Help)	Lists all of the APPN configuration commands, or lists the options associated with specific commands.
Enable/Disable	Enables the following: • APPN • Dependent LU Requestor • Port *port name*
Set	Sets the following: • Node • Traces • HPR • DLUR • Management • Tuning
Add	Adds or updates the following: • Port *port name* • Link station *link station name* • LU_Name *LU name* • Connection Network *connection network name* • Additional port to connection network • Mode
Delete	Deletes the following: • Port *port name* • Link *link station name* • LU_Name *LU name* • Connection Network *connection network name* • Connection Networks Port Interface (CN PORTIF) *CN name* • Mode *mode name*
List	Lists the following from configuration memory: • All • Node • Traces • Management • HPR • DLUR • Port *port name* • Link *link name* • LU Name *LU name* • Mode Name *mode name* • Connection Network *connection network name*
Activate_new_config	Reads the configuration into non-volatile configuration memory.
Exit	Exits the APPN Configuration process and returns to the `Config>` prompt.

APPN Configuration Command Detail

Enable/Disable

Use the **enable/disable** command to enable (or disable):

Syntax: enable (or disable) appn
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 2-3 (Page 1 of 2). 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 2-3 (Page 2 of 2). Configuration Parameter List - APPN Routing

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	Route addition resistance
Valid Values	0 to 255
Default Value	128
Description	This parameter indicates the desirability of routing through this node. This parameter is used in the class of service based route calculation. Lower values indicate higher levels of desirability.
Parameter	XID number for subarea connection (see table notes)
Valid Values	A string of 5 hexadecimal digits
Default	X'00000'
Description	This parameter specifies a unique ID number (identifier) for the network node. The XID number is combined with an ID block number (which identifies a specific IBM product) to form an XID node identification. Node identifications are exchanged between adjacent nodes when the nodes are establishing a connection. The router network node automatically appends an ID block number to this parameter during the XID exchange to create an XID node identification. The ID number you assign to this node must be unique within the APPN network identified by Network ID parameter. Contact your network administrator to verify that the ID number is unique.

Note: Node identifications are normally exchanged between T2.1 nodes during CP-CP session establishment. If the network node is communicating with the IBM Virtual Telecommunications Access Method (VTAM) product through a T2.1 LEN node and the LEN node has a CP name defined for it, the XID number parameter is not required. If the adjacent LEN node is not a T2.1 node or does not have an explicitly defined CP name, the XID number parameter must be specified to establish a connection with the LEN node. VTAM versions prior to Version 3 Release 2 do not allow CP names to be defined for LEN nodes.

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 2-4. Configuration Parameter List - High Performance Routing (HPR)

Parameter Information	
Parameter	Maximum sessions for HPR connections
Valid Values	1 to 65535
Default Value	100
Description	This parameter specifies the maximum number of sessions allowed on an HPR connection. An HPR connection is defined by the class of service (COS), the physical path (TGs), and the network connection end points.

Table 2-5 (Page 1 of 3). Configuration Parameter List - HPR Timer and Retry Options

Parameter Information	
Low transmission priority traffic	
Parameter	RTP inactivity timer
Valid Values	1 to 60 minutes
Default Value	3 minutes
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 2-5 (Page 2 of 3). Configuration Parameter List - HPR Timer and Retry Options

Parameter Information	
Parameter	RTP inactivity timer
Valid Values	1 to 60 minutes
Default Value	3 minutes
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 60 minutes
Default Value	3 minutes
Description	This parameter specifies RTP's inactivity interval for HPR connections that carry traffic with *high* transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection.
Parameter	Maximum RTP retries
Valid Values	0 to 10
Default Value	6
Description	This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with high transmission priority.

Table 2-5 (Page 3 of 3). Configuration Parameter List - HPR Timer and Retry Options

Parameter Information	
Parameter	Path switch timer
Valid Values	0 to 7200 seconds
Default Value	180 seconds
Description	This parameter specifies the maximum amount of time that a path switch may be attempted on an HPR connection carrying traffic with high transmission priority. A value of zero indicates that the path switch function is to be disabled, and a path switch will not be performed.
Network transmission priority traffic	
Parameter	RTP inactivity timer
Valid Values	1 to 60 minutes
Default Value	3 minutes
Description	This parameter specifies RTP's inactivity interval for HPR connections that carry traffic with *network* transmission priority. This is an end-to-end version of the LLC inactivity timer, Ti. If no receptions occur during this interval, RTP transmits a poll. Idle periods are monitored to ensure the integrity of the connection.
Parameter	Maximum RTP retries
Valid Values	0 to 10
Default Value	6
Description	This parameter specifies the maximum number of retries before RTP initiates a path switch on an HPR connection that carries traffic with network transmission priority.
Parameter	Path switch timer
Valid Values	0 to 7200 seconds
Default Value	180 seconds
Description	This parameter specifies the maximum amount of time that a path switch may be attempted on an HPR connection carrying traffic with network transmission priority. A value of zero indicates that the path switch function is to be disabled, and a path switch will not be performed.

Syntax: set dlur

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 2-6 (Page 1 of 3). Configuration Parameter List - Dependent LU Requester

Parameter Information	
Parameter	Enable dependent LU requester (DLUR) on this network node
Valid Values	Yes, No
Default Value	No
Description	This parameter specifies whether a dependent LU requester is to be functionally enabled on this node.
Parameter	Default fully qualified CP name of primary DLUS (required when DLUR is enabled)
Valid Values	A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a CP name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names.
Default Value	None
Description	This parameter specifies the fully qualified control point (CP) name of the dependent LU server (DLUS) that is used by default. The default primary server may be overridden on a link station basis. The default server is used for incoming requests from downstream PUs when a primary DLUS has not been specified for the associated link station.
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 2-6 (Page 2 of 3). Configuration Parameter List - Dependent LU Requester

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 nondisruptive 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 2-11 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 nondisruptive 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 2-11 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 2-11 for a complete description of the retry algorithm.

Table 2-6 (Page 3 of 3). Configuration Parameter List - Dependent LU Requester

Parameter Information	
Parameter	Short retry timer
Valid Values	0 to 2756000 seconds
Default Value	120 seconds
Description	In all cases of pipe failure other than nondisruptive 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 2-11 for a complete description of the retry algorithm.
Parameter	Short retry count
Valid Values	0 to 65535
Default Value	5
Description	In all cases of pipe failure other than nondisruptive 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 2-11 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 2-11 for a complete description of the retry algorithm.
Parameter	Long retry timer
Valid Values	0 to 2756000 seconds
Default Value	300 seconds
Description	This parameter specifies the time DLUR will wait when performing long retries. See "DLUR Retry Algorithm" on page 2-11 for a complete description of the retry algorithm.

Syntax: set tuning

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Note: You will have to re-boot in order for the changes you specify to take place.

Table 2-7 (Page 1 of 3). Configuration Parameter List - APPN Node Tuning

Parameter Information	
Parameter	Maximum number of adjacent nodes
Valid Values	1 to 2800
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 8000
Default	50
Description	This parameter is an estimate of the maximum number of nodes that you expect in the sub-network (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 64000
Default	3 times the value of the *maximum number of network nodes in the sub-network*.
Description	This parameter is an estimate of the maximum number of TGs connecting network nodes in the sub-network (that is, in the topology known by this node). This parameter is configurable using the Configuration Program only.
Parameter	Maximum number of ISR sessions
Valid Values	10 to 7500
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.

Table 2-7 (Page 2 of 3). Configuration Parameter List - APPN Node Tuning

Parameter Information	
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.
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 2-7 (Page 3 of 3). Configuration Parameter List - APPN Node Tuning

Parameter Information	
Parameter	Override tuning algorithm
Valid Values	Yes, No
Default Value	No
Description	When enabled, this parameter overrides the tuning calculations generated by the Command Line and enables you to specify explicit values for the Maximum shared memory parameter and the Maximum cached directory entries parameter. This parameter is configurable using the Configuration Program only.
Parameter	Maximum shared memory
Valid Values	1280 - 26000 KB
Default Value	5108
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. This parameter is configurable using the Configuration Program and from **talk 6**
Parameter	Percent of APPN shared memory to be used for buffers
Valid Values	10 to 50
Default	10% or 512 Kilobytes, whichever is larger.
Description	This parameter specifies the amount of shared memory that APPN will use for buffers. This parameter is configurable using the Configuration Program and from **talk 6**
Parameter	Maximum cached directory entries
Valid Values	0 to 65535
Default	4000
Description	This parameter specifies the number of directory entries to be stored or cached by the router network node. If a directory entry for a node is cached, the router does not need to broadcast a search request to locate the node. This reduces the time it takes to initiate sessions with the node. This parameter is configurable using the Configuration Program and from **talk 6**

Syntax: set traces

You will be prompted to enter values for the following parameters. The parameter range will be shown in parentheses ( ). The parameter default will be shown in square brackets [ ].

Table 2-8 (Page 1 of 3). Configuration Parameter List - Node Level Traces

Parameter Information	
Parameter	Process management
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the management of processes within the APPN network node, including the creation and termination of processes, processes entering a wait state, and the posting of processes.
Parameter	Process to process communication
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about messages exchanged between processes in the APPN network node, including the queuing and receipt of such messages.
Parameter	Locking
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about locks that were obtained and released on processes in the APPN network node.
Parameter	Miscellaneous tower activities
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about miscellaneous activities within the APPN network node.
Parameter	I/O to and from the system
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the flow of messages entering and exiting the APPN network node.
Parameter	Storage management
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about any shared memory that was obtained and released by the APPN network node.

Table 2-8 (Page 2 of 3). Configuration Parameter List - Node Level Traces

Parameter Information	
Parameter	Queue data type management
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls in the APPN network node that manage general purpose queues.
Parameter	Table data type management
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls in the APPN network node that manage general purpose tables, including calls to add table entries and calls to query tables for specific entries.
Parameter	Buffer management
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about buffers in the APPN network node that were obtained and released.
Parameter	Configuration control
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the activities of the configuration control component of the APPN network node. The configuration control component manages information about node resources.
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.

Table 2-8 (Page 3 of 3). Configuration Parameter List - Node Level Traces

Parameter Information	
Parameter	Interprocess message segmenting
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the buffer transfer and freeing of chained messages within the APPN network node.
Parameter	Control of processes outside scope of this tower
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about the definition and activation of processes external to this APPN network node, such as when the node operator facility (NOF) defines the external process configuration control.
Parameter	Monitoring existence of processes, services, towers
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about requests that start or stop the monitoring of processes or services within the APPN network node.
Parameter	Distributed environment control
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about requests within the APPN network node that define subsystems and create environments.
Parameter	Process to service dialogs
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this trace option causes the router trace facility to gather data about all calls within the APPN network node that open, close, or send data on a dialog.
Parameter	AVL Tree Support
Valid Values	Yes, No
Default	No
Description	This parameter enables or disables this APPN trace option. When enabled, the trace option causes the router trace facility to gather data about all calls that manage AVL trees.

Table 2-9 (Page 1 of 3). Configuration Parameter List - Interprocess 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 interprocess 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 interprocess 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 interprocess signals from the configuration services component.
Parameter	Dependent LU requester
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about interprocess 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 interprocess 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 interprocess 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 interprocess signals from the HPR path control component.

Table 2-9 (Page 2 of 3). Configuration Parameter List - Interprocess Signals Traces

Parameter Information	
Parameter	Management Services
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about interprocess 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 interprocess 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 interprocess signals from the path control component.
Parameter	Presentation Services
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about interprocess 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 interprocess 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 interprocess 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 interprocess signals from the session connector component.

Table 2-9 (Page 3 of 3). Configuration Parameter List - Interprocess Signals Traces

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 interprocess 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 interprocess 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 interprocess signals from the topology and routing services component.

Table 2-10 (Page 1 of 2). Configuration Parameter List - Module Entry and Exit Traces

Parameter Information	
Parameter	Attach manager
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the attach manager component.
Parameter	Half session
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the half session component.
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.

Table 2-10 (Page 2 of 2). Configuration Parameter List - Module Entry and Exit Traces

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 module entry and exit information from the presentation services component.
Parameter	Rapid transport protocol
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about module entry and exit information from the rapid transport control component.
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 2-11 (Page 1 of 4). Configuration Parameter List - General Component Level Traces

Parameter Information	
Parameter	Accounting services
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the accounting services component.
Parameter	Address space manager
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the address space manager component.

Table 2-11 (Page 2 of 4). Configuration Parameter List - General Component Level Traces

Parameter Information	
Parameter	Architected transaction programs
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the architected transaction programs component.
Parameter	Configuration services
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the configuration services component.
Parameter	Dependent LU requester
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the dependent LU requester component.
Parameter	Directory services
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the directory services component.
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	Management services
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the management services component.
Parameter	Node operator facility
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the node operator facility component.

Table 2-11 (Page 3 of 4). Configuration Parameter List - General Component Level Traces

Parameter Information	
Parameter	Path control
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the path control component.
Parameter	Problem determination services
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the problem determination component.
Parameter	Rapid transport protocol
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the rapid transport control component.
Parameter	Session connector manager
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the session connector manager component.
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 2-11 (Page 4 of 4). Configuration Parameter List - General Component Level Traces

Parameter Information	
Parameter	Topology and routing services
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables this APPN trace option. When enabled, this parameter informs the trace facility to include trace data about general information from the topology and routing services component.

Table 2-12. 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.

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 2-13 (Page 1 of 2). 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 2-13 (Page 2 of 2). Configuration Parameter List - APPN Node Management

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.

Table 2-14 (Page 1 of 2). Configuration Parameter List - APPN ISR Recording Media

Parameter Information	
Memory Parameters	
Parameter	Memory (see table notes)
Valid Values	Yes, No
Default Value	No
Description	This parameter enables or disables the collection of intermediate session data in the router's local memory.
Parameter	Maximum memory buffers
Valid Values	0 to 1
Default Value	1
Description	This parameter specifies the number of buffers to be allocated in the router's local memory for storing intermediate session records.
Parameter	Maximum memory records per buffer
Valid Values	0 to 2000
Default Value	100
Description	This parameter specifies the maximum number of intermediate session records that may be stored in the memory buffer on the router.
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 2-14 (Page 2 of 2). Configuration Parameter List - APPN ISR Recording Media

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. If Yes is specified, the router will save topology information once a day during garbage collection.

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 2-13 on page 2-67) has been enabled.
- Intermediate session data can be stored in router memory.

Add

Use the **add** command to add:

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 2-15 (Page 1 of 3). Configuration Parameter List - Port Configuration

Parameter Information	
Parameter	Link type
Valid Values	PPP (P) Frame relay (F) Ethernet (E) Token ring (T) SDLC (S) X.25 (X) DLSw (D)
Default Value	None
Description	This parameter specifies the type of link associated with this port.
Parameter	Interface number
Valid Values	0 to 253
Default Value	0
Description	This parameter defines the physical interface number of the hardware interface to which this device is attached.

Table 2-15 (Page 2 of 3). Configuration Parameter List - Port Configuration

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) • FR (frame relay) • X25 (X.25) • DLS (DLSw) • SDLC (SDLC) • PPP (point-to-point) 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	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.

Table 2-15 (Page 3 of 3). Configuration Parameter List - Port Configuration

Parameter Information	
Parameter	High performance routing (HPR) supported
Valid Values	Yes, No
Default Value	Yes for token-ring, Ethernet, frame relay, and PPP ports. Disabled for all other port types (Cannot be changed).
Description	This parameter indicates whether link stations on this port will support HPR. This value may be overridden on the link station definition.
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 2-16 (Page 1 of 2). Configuration Parameter List - Port Definition

Parameter Information	
Parameter	Maximum BTU size
Valid Values	768 to 1289 bytes for Ethernet 768 to 2063 bytes for token-ring 768 to 2048 bytes for frame relay or PPP 768 to 2044 bytes for frame relay or PPP over ISDN and V.25bis 768 to 2048 bytes for all other ports X.25 will take value from network level
Default Value	1289 bytes for Ethernet 2048 bytes for token-ring 2048 bytes for frame relay or PPP 2044 bytes for frame relay or PPP over ISDN and V.25bis 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.
Parameter	Maximum number of link stations
Valid Values	1 to 239 for X.25 ports 1 to 127 for SDLC ports 1 to 976 for all other ports (cannot be configured for PPP ports)
Default Value	1 for PPP ports (cannot be changed) 239 for X.25 ports If SDLC is configured as multipoint and primary, then this parameter defaults to 127. Otherwise, it is set to 1 and is not configurable. 512 for all other ports
Description	This parameter specifies the maximum number of link stations that will be allowed to use this port. This parameter allows the resources for the APPN node and this port to be constrained.
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.

Table 2-16 (Page 2 of 2). Configuration Parameter List - Port Definition

Parameter Information	
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	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.

Table 2-17 (Page 1 of 4). Configuration Parameter List - Port Default TG Characteristics

Parameter Information	
Parameter	Cost per connect time
Valid Values	0 to 255
Default Value	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 nonswitched facilities). Higher values represent higher costs.

Table 2-17 (Page 2 of 4). Configuration Parameter List - Port Default TG Characteristics

Parameter Information	
Parameter	Cost per byte
Valid Values	0 to 255
Default Value	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.
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 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.
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 token-ring and Ethernet/802.3 ports: LAN For frame-relay ports: Packet switched For all other ports: Telephone
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 2-17 (Page 3 of 4). Configuration Parameter List - Port Default TG Characteristics

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
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.
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.

Table 2-17 (Page 4 of 4). Configuration Parameter List - Port Default TG Characteristics

Parameter Information	
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 2-18 (Page 1 of 3). Configuration Parameter List - Port default LLC Characteristics

Parameter Information	
Parameter	Remote APPN SAP
Valid Values	Multiples of four in the hexadecimal range of X'04' to X'EC'
Default Value	X'04'
Description	This parameter specifies the SAP associated with an adjacent node's APPN link station.
Parameter	Maximum number of outstanding I-format LPDUs (TW)
Valid Values	1 to 127
Default Value	26
Description	This parameter specifies the LLC maximum number of outstanding I-format LPDUs (TW) for all link stations on this port. The maximum number of outstanding I-format LPDUs defines the transmit Command Line option (TW) which is the maximum number of sequentially numbered I-format LPDUs that the link station may have unacknowledged at any given time.
Parameter	Receive window size
Valid Values	1 to 127
Default Value	26
Description	This parameter specifies the LLC receive Command Line option size (RW) for all link stations on this port. The RW parameter specifies the maximum number of unacknowledged sequentially numbered I-format LPDUs that the link station can receive from the remote link station. RW is advertised in SNA XID frames and IEEE 802.2 XID frames. The XID receiver should set its effective TW to a value less than or equal to the value of the received RW to avoid overruns.

Table 2-18 (Page 2 of 3). Configuration Parameter List - Port default LLC Characteristics

Parameter Information	
Parameter	Inactivity timer (Ti)
Valid Values	1 to 254 seconds
Default Value	30 seconds
Description	This parameter specifies the LLC inactivity timer (Ti) for all link stations on this port. An LLC link station uses Ti to detect an inoperative condition in either the remote link station or in the transmission media. If an LPDU is not received in the time interval specified by Ti, an S-format command LPDU with the poll bit set is transmitted to solicit remote link station status. Recovery is then based on the reply timer (T1).
Parameter	Reply timer (T1)
Valid Values	1 to 254 half-seconds
Default Value	2 half-seconds
Description	This parameter specifies the LLC reply timer (T1) for all link stations on this port. An LLC link station uses T1 to detect a failure to receive a required acknowledgement 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 acknowledgement timer (T2)
Valid Values	1 to 254 half-seconds
Default Value	1 half-second
Description	This parameter specifies the LLC receiver acknowledgement timer (T2) for all link stations on this port. The T2 parameter may be used with the N3 counter to reduce acknowledgement traffic. A link station uses T2 to delay the sending of an acknowledgement for a received I-format LPDU. T2 is started when an I-format LPDU is received, and reset when an acknowledgement is sent in an I-format or S-format LPDU. If T2 expires, the link station must send an acknowledgement 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 acknowledgement before its T1 expires.

Table 2-18 (Page 3 of 3). Configuration Parameter List - Port default LLC Characteristics

Parameter Information	
Parameter	Acknowledgements 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 tranmitted 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 2-19. 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 half-seconds
Default Value	2 half-seconds
Description	This parameter specifies the LLC reply timer (HPR T1) that is to be used for all link stations on this port supporting HPR when the HPR supported parameter is enabled on this port. This default overrides the value of the default LLC reply timer (T1) parameter specified on the default LLC characteristics parameter.
Parameter	Maximum number of retransmissions for HPR (HPR N2)
Valid Values	1 to 254
Default Value	3
Description	This parameter specifies the LLC maximum number of retransmissions (HPR N2) that is to be used for all link stations on this port supporting HPR when the HPR supported parameter is enabled on this port. This default overrides the value of the default LLC maximum number of retransmissions (N2) parameter specified on the default LLC Characteristics parameter.

Syntax: add link

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 2-20 (Page 1 of 6). Configuration Parameter List - Link Station - Detail

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) • FR (frame relay) • X25 (X.25) • DLS (DLSw) • SDLC (SDLC) • PPP (point-to-point) 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 2-20 (Page 2 of 6). Configuration Parameter List - Link Station - Detail

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.

Table 2-20 (Page 3 of 6). Configuration Parameter List - Link Station - Detail

Parameter Information	
Parameter	Adjacent node type
Valid Values	APPN network node APPN end node LEN end node PU 2.0 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 or a PU 2.0 node supported by the DLUR function. 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. The *PU 2.0* option is valid only when DLUR is enabled on the router APPN network node. 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.

Table 2-20 (Page 4 of 6). Configuration Parameter List - Link Station - Detail

Parameter Information	
Parameter	Fully qualified CP name of adjacent node
Valid Values	A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a control point name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully qualified CP name, using the special characters @, $, and from the character set A, continues to be supported; however, these characters should not be used for new CP names.
Default Value	None
Description	This parameter specifies the fully qualified CP name of the adjacent node. For the cases where this parameter is not required, the adjacent node's CP name may be learned dynamically during XID exchange; however, if a CP name is specified, it must match the adjacent node's definition for the link to be successfully activated. **Note:** This parameter is required when any of the following occur: • The *Service any node* parameter is set to Disable. • The *Adjacent node type* parameter is set to LEN end node. • The *CP-CP session level security* parameter is set to Enable. • The link is a limited resource.
Parameter	Activate link automatically If limited resource, then this parameter is set to No and is not configurable.
Valid Values	Yes, No
Default Value	Yes
Description	When this parameter is enabled, the router network node automatically activates the link to the adjacent node and initiates a connection.

Table 2-20 (Page 5 of 6). Configuration Parameter List - Link Station - Detail

Parameter Information	
Parameter	Allow CP-CP sessions on this link
Valid Values	Yes, No
Default Value	Yes, if adjacent node type is APPN network node or APPN end node Disable for all other adjacent node types
Description	This parameter specifies whether sessions between control points are to be activated over this link station. This parameter allows control of CP-CP session establishment between adjacent network nodes so that the overhead associated with topology database updates (TDUs) may be constrained. **Note:** Every APPN network node must have at least one CP-CP session established to another APPN network node in order to maintain the minimum connectivity necessary to update the topology database. In addition, more than minimum connectivity could be desired to eliminate single points of failure and to improve network dynamics.
Parameter	CP-CP session level security
Valid Values	Yes, No
Default Value	No
Description	This parameter specifies whether session level security is enforced for CP-CP sessions established over this link station. When session level security is enabled, encrypted data is exchanged and compared during the BIND flows (which includes the BIND, the BIND response, and an FMH-12 Security RU). To successfully establish a CP-CP session with session level security enabled, both partners must be configured with the same encryption key. Currently, session level security support is limited to the basic LU-LU verification protocol.
Parameter	Encryption key
Valid Values	Up to 16 hexadecimal digits. If fewer than 16 digits are specified, the value is padded on the right with zeros.
Default Value	None
Description	This parameter is used to encrypt data exchanged during BIND flows. Both partners must be configured with the same key to establish a CP-CP session.
Parameter	Use enhanced session security (If security is enabled)
Valid Values	Yes, No
Default Value	No

Table 2-20 (Page 6 of 6). Configuration Parameter List - Link Station - Detail

Parameter Information	
Parameter	High performance routing (HPR) supported
Valid Values	Yes, No
Default Value	APPN network node, APPN end node or LEN end node: the value specified in the default HPR supported parameter for this port All other adjacent node types: No
Description	This parameter indicates whether this link station supports HPR. The user should disable HPR support if the underlying link is unreliable. An HPR connection will not be established unless both link stations advertise HPR support during XID exchange.
Parameter	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	If the *link type* is PPP or FR, the default will be taken from the *limited resource* parameter for the associated port. If the *link type is X.25*, the default is No
Description	This parameter specifies whether the TG for this link station is a limited resource.
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.
Default Value	If *limited resource* is Yes, default is 1. If *limited resource* is No, default is 0.
Description	This parameter uniquely identifies a TG between adjacent nodes.

Table 2-21 (Page 1 of 2). 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 nonswitched 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 2-21 (Page 2 of 2). Configuration Parameter List - Modify TG Characteristics

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.
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 2-22. Configuration Parameter List - Modify Dependent LU Server

Parameter Information	
Parameter	Fully qualified CP name of primary DLUS
Valid Values	A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a control point name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names.
Default Value	The value specified in the default fully qualified CP name of primary dependent LU server parameter.
Description	This parameter specifies the fully qualified CP name of the dependent LU server (DLUS) that is to be used for incoming requests from the downstream PU associated with this link station.
Parameter	Fully qualified CP name for backup DLUS
Valid Values	A string of up to 17 characters in the form of *netID.CPname*, where: • *netID* is a network ID from 1 to 8 characters • *CPname* is a control point name from 1 to 8 characters Each name must conform to the following rules: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing fully qualified CP name, using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new CP names.
Default Value	The value specified in the default fully qualified CP name of backup dependent LU server parameter.
Description	This parameter specifies the fully qualified CP name of the dependent LU server (DLUS) that is to be used as a backup for the downstream PU associated with this link station. This parameter allows the default backup server to be overridden. A backup is not required, and the NULL value indicates the absence of a backup server. Note that NULL can be specified even when a default backup server has been defined (by erasing the default value that appears for this parameter).

Table 2-23 (Page 1 of 2). Configuration Parameter List - Modify LLC Characteristics

Parameter Information	
Parameter	Remote APPN SAP
Valid Values	Multiples of four in the hexadecimal range of X'04' to X'EC'.
Default Value	Default value is taken from the associated port parameter.
Description	This parameter specifies the Destination SAP (DSAP) address on the destination node to which data will be sent. This DSAP address value will appear in the LLC frame to identify the service access point (SAP) address associated with the adjacent node's APPN link station.
Parameter	Maximum number of outstanding I-format LPDUs (TW)
Valid Values	1 to 127
Default Value	Default value is taken from the associated port parameter.
Description	This parameter specifies the transmit Command Line option which is the maximum number of sequentially numbered I-format LPDUs that the link station may have unacknowledged at any given time.
Parameter	Receive window size
Valid Values	1 to 127
Default Value	Default value is taken from the associated port parameter.
Description	This parameter specifies the maximum number of unacknowledged sequentially numbered I-format LPDUs that the LLC link station can receive from the remote link station. RW is advertised in SNA XID frames and IEEE 802.2 XID frames. The XID receiver should set its effective TW to a value less than or equal to the value of the received RW to avoid overruns.
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 2-23 (Page 2 of 2). Configuration Parameter List - Modify LLC Characteristics

Parameter Information	
Parameter	Reply timer (T1)
Valid Values	1 to 254 half-seconds
Default Value	Default value is taken from the associated port parameter.
Description	A link station uses T1 to detect a failure to receive a required acknowledgement 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 acknowledgement timer (T2)
Valid Values	1 to 254 half-seconds
Default Value	Default value is taken from the associated port parameter.
Description	This parameter may be used in conjunction with the N3 counter to reduce acknowledgement traffic. A link station uses T2 to delay the sending of an acknowledgement for a received I-format LPDU. T2 is started when an I-format LPDU is received, and reset when an acknowledgement is sent in an I-format or S-format LPDU. If T2 expires, the link station must send an acknowledgement 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 acknowledgement before its T1 expires.
Parameter	Acknowledgement needed to increment working window
Valid Values	0 to 127 acknowledgements
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 tranmitted 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 2-24. 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 half-seconds
Default Value	Default value is taken from the associated port parameter.
Description	This parameter specifies the HPR override LLC reply timer (HPR T1) that is to be used when HPR is supported by this link station. This parameter overrides the value taken from the default reply timer override for HPR parameter specified on HPR Defaults. This parameter supersedes the value of the LLC reply timer (T1) parameter specified on the Modify Logical Link Control (LLC) Characteristics parameter when HPR is supported.
Parameter	Maximum number retransmission (HPR N2)
Valid Values	1 to 2160000
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	1-216000 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 2-25. 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 2-26. 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
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.
Parameter	Port name (required)
Valid Values	Name of port on which APPN routing has been enabled.
Default Value	None
Description	This parameter specifies the name of a port providing connectivity to the shared access transport facility (SATF) for the connection network being defined. All ports defined for a given connection network must be the same type and have the same characteristics.
Parameter	Limited Resource Timer
Valid Values	1-216000 seconds
Default Value	180
Description	This parameter specifies the timer value associated with a limited resource.

Table 2-27 (Page 1 of 2). 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 nonswitched facilities). Higher values represent higher costs.
Parameter	Cost per byte
Valid Values	0 to 255
Default Value	0
Description	This parameter expresses the relative cost of transmitting a byte over the associated TG. The units are user-defined and the assigned value should reflect the actual expenses incurred for transmitting over the TG relative to all other TGs in the network. A value of zero means that bytes may be transmitted over the TG at no additional cost. Higher values represent higher costs.
Parameter	Security
Valid Values	Nonsecure - all else (for example, satellite-connected, or located in a nonsecure country). Public switched network - secure in the sense that route is not predetermined. Underground cable - located in secure country (as determined by the network administrator). Secure conduit - Not guarded, (for example, pressurized pipe). Guarded conduit - protected against physical tapping. Encrypted - link-level encryption is provided. Guarded radiation - guarded conduit containing the transmission medium; protected against physical and radiation tapping.
Default Value	Nonsecure
Description	This parameter indicates the level of security protection associated with the TG. If security attributes other than the architecturally-defined ones are needed, one of the user-defined TG characteristics may be used to specify additional values.

Table 2-27 (Page 2 of 2). Configuration Parameter List - TG Characteristics (Connection Network)

Parameter Information	
Parameter	Propagation delay
Valid Values	Minimum LAN - less than 480 microseconds Telephone - between .48 and 49.152 milliseconds Packet switched - between 49.152 and 245.76 milliseconds Satellite - greater than 245.76 milliseconds Maximum
Default Value	LAN
Description	This parameter specifies the approximate range for the length of time that it takes for a signal to propagate from one end of the TG to the other.
Parameter	Effective capacity
Valid Values	2 hexadecimal digits in the range X'00' to X'FF'
Default Value	X'75'
Description	This parameter specifies the effective maximum bit transmission rate for this connection network TG. Effective capacity specifies the maximum effective rate for both physical links and logical links. The effective capacity is encoded as a single-byte representation. The values X'00' and X'FF' are special cases used to denote minimum and maximum capacities. The range of the encoding is very large; however, only 256 values in the range may be specified.
Parameter	First user-defined characteristic
Valid Values	0 to 255
Default Value	128
Description	This parameter specifies the first of three additional characteristics that users may define to describe the TGs in the network. The default value of 128 allows a subset of TGs to be defined as more or less desirable than the rest without defining values for all TGs.
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 2-28. 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.
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 2-29. Configuration Parameter List - APPN Additional port to Connection Network

Parameter Information	
Parameter	Connection network name (fully-qualified) (required for each connection network defined)
Valid Values	A string of 1 to 8 characters: • First character: A to Z • Second to eighth characters: A to Z, 0 to 9 **Note:** An existing connection network of which this node desires to become a member, named using the special characters @, $, and # from the character set A, continues to be supported; however, these characters should not be used for new connection network names.
Default Value	None
Description	This parameter specifies the name of the connection network being defined on this router network node. Since this name becomes the CP name of the virtual routing node (VRN), the name must be unique among all CP and LU names in the APPN network (same as in the local Control Point Name). All nodes that are members of a given connection network must use the same VRN Name. The fully-qualified VRN Name (CP name of VRN) has the form: *NetworkID.ConnectionNetworkName* where *NetworkID* is this router network node's network identifier.
Parameter	Port name
Valid Values	A unique unqualified name that is automatically generated by the Command Line. The name will consist of: • TR (token-ring) • EN (Ethernet)
Default Value	Unqualified name generated by the Command Line.
Description	This parameter specifies the name representing this port.

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*

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*

Exit

Use the **exit** command to exit the APPN configuration process and return to the CONFIG> prompt.

Syntax: exit

Chapter 3. Monitoring APPN

This chapter describes how to monitor APPN. It includes the following sections:

- "Accessing the APPN Console Commands"
- "APPN Console Commands"

Accessing the APPN Console Commands

Use the following procedure to access the APPN console 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 console. If the prompt does not appear when you first enter configuration, press **Return** again.

Enter **protocol APPN** For example:

```
* talk 5
+
+ protocol APPN
```

APPN Console Commands

This section summarizes the APPN console commands for monitoring APPN interfaces. Enter the commands at the APPN> prompt.

Table 3-1. APPN Console Command Summary

Command	Function
? (Help)	Lists all of the APPN configuration commands, or lists the options associated with specific commands.
Dump	Creates an APPN dump file
Stop	Stops APPN
Restart	Restarts APPN
List	Lists: • CP-CP_sessions - displays information on active CP-CP sessions • Dump - displays dump information • ISR_sessions - displays information on active ISR sessions • Link_information - displays information on all links unless a particular interface is requested. • Port_information - displays information on all ports unless a particular interface is requested. • RTP_sessions - displays information on active RTP sessions • Session_information - If *Save RSCV information for intermediate nodes* is Yes, displays origin CP Name, primary LU Name, and secondary LU Name.
Memory	Obtains and displays APPN memory usage information.
Transmit	Transmits a dump from the hardfile to a workstation in the network using tftp.
Exit	Exits the APPN Monitoring process and returns to the + prompt.

? (Help)

Syntax: help

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter a ? after a specific command name to list its options.

Dump

Syntax: dump

Use the **Dump** command to create an APPN dump on the hardfile. The hardfile will hold up to 5 dumps. Each dump is numbered in sequence and has a timestamp. Use the **List** command to display the dump information.

Transmit

Syntax: transmit dump-number

Use the **Transmit** command to transmit an APPN dump from the hardfile to a workstation in the network using tftp.

Stop

Syntax: stop

Use the **Stop** command to cause APPN to stop.

Restart

Syntax: restart

Use the **Restart** command to restart APPN after it has been stopped.

List

Syntax: list *name*

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

List config	Displays the APPN configuration values.
List cp	Displays a table of all defined cp sessions.
List dump	Displays information about the dumps saved on the hard file.
List isr	Displays a table of all defined isr links.
List port	Displays a table of all defined ports.
List port	*port name* Displays a information about the requested port.
List link	Displays a table of all defined links.
List link	*station name* Displays a information about the requested link station.
List rtp	Displays a table of all defined rtp links.
List session_info	Displays origin CP Name, primary LU Name and secondary LU Name if *Save RSCV information for intermediate sessions* is Yes.

Exit

Use the **Exit** command to exit the APPN monitoring process and return to the + prompt.

Chapter 4. Configuring DVMRP

This chapter describes how to configure DVMRP (Distance Vector Multicast Routing Protocol) using the DVMRP configuration commands. It includes the following sections:

- "Accessing the DVMRP Configuration Environment"
- "DVMRP Configuration Commands"

Accessing the DVMRP Configuration Environment

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

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

DVMRP Configuration Commands

This section summarizes and explains the DVMRP configuration commands. The commands are entered at the `DVMRP Config>` prompt. To activate the commands, you must restart the router.

Table 4-1. DVMRP Configuration Commands Summary

Command	Function
? (Help)	Lists all of the DVMRP configuration commands or lists the options associated with specific commands.
DVMRP	Enables or disables DVMRP.
List	Displays the current DVMRP configuration.
MOSPF	Sets the metric and threshold for the DVMRP interface running over MOSPF. This command also disables the MOSPF VIF.
Phyint	Sets the metric and threshold for LAN interfaces associated with DVMRP. This command also deletes LAN interfaces associated with DVMRP
Tunnel	Adds or deletes tunnels in a MOSPF/DVMRP configuration.
Exit	Exits the DVMRP configuration process and returns to the CONFIG environment.

? (Help)

Use the **? (help)** command to list the available commands from the current prompt level. You can also enter a ? after a specific command name to list its options.

Syntax: ?

Example: **?**

or

add ?

DVMRP

Use the **dvmrp** command to enable or disable DVMRP on the bridging router.

Syntax: dvmrp on
off

on

Enables DVMRP on the bridging router. When enabled, DVMRP interfaces will automatically be assigned to all LAN interfaces that are NOT running MOSPF.

Example: `dvmrp on`

off

Disables DVMRP on the router.

Example: `dvmrp off`

List

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

Syntax: list

Example: **`list`**

```
DVMRP enabled
tunnel 0.0.0.0 0.0.0.0 1 1
MOSPF 1 1
```

MOSPF

Use the **mospf** command to set the metric and threshold for the DVMRP interface running over MOSPF. This command also disables the MOSPF VIF.

Syntax: mospf *metric threshold*
delete

metric threshold

Sets the metric and threshold for the MOSPF VIF. Default value for the metric and threshold parameters is 1.

When using a MOSPF domain to join DVMRP tunnels, DVMRP is actually run over MOSPF. When this occurs a DVMRP interface named “MOSPF VIF” (VIF or virtual interface) is automatically created. DVMRP tries to run over MOSPF automatically using the MOSPF VIF.

Example: `mospf 1 1`

delete

Disables the MOSPF VIF. When MOSPF is enabled, DVMRP tries to run over MOSPF automatically using the MOSPF VIF.

Example: `mospf delete`

Phyint

Use the **phyint** command to set the metric and threshold for LAN interfaces associated with DVMRP. This command also deletes LAN interfaces associated with DVMRP.

Syntax: phyint *intrfc_address metric threshold*
intrfc_address delete

intfc_address metric threshold
Sets the metric and threshold for LAN interfaces (specified by the *intrfc_address* parameter) associated with DVMRP. Default values for the metric and threshold parameters are 1.

Example: `phyint XXXXX 1 1`

off
Deletes LAN interfaces associated with DVMRP.

Example: `phyint XXXXX delete`

Tunnel

Use the **tunnel** command to add tunnels or delete tunnels in a MOSPF/DVMRP configuration.

Syntax: tunnel *source-adr destination-addr metric threshold*
source-addr destination-addr delete

source-adr destination-addr metric threshold
Adds a tunnel to a MOSPF/DVMRP configuration.

Example: `tunnel XXX XXX 1 1`

source-addr destination-addr delete
Deletes a tunnel from a MOSPF/DVMRP configuration.

Example: `tunnel XXX XXX delete`

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: `exit`

Chapter 5. Monitoring DVMRP

This chapter describes how to monitor DVMRP protocol activity and how to use the DVMRP console commands. It includes the following sections:

- "Accessing the DVMRP Console Environment"
- "DVMRP Console Commands"

Accessing the DVMRP Console Environment

To access the DVMRP console environment, enter the following command at the * (GWCON) prompt:

```
* talk 5
+ protocol dvmrp
DVMRP>
```

DVMRP Console Commands

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

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

Table 5-1. DVMRP Console Command Summary

Command	Function
? (Help)	Lists all the DVMRP console commands or lists the options associated with specific commands.
Dump routing tables	Displays the OSPF routes contained in the routing table.
Interface summary	Displays OSPF interface statistics and parameters.
Join	Configures the router to belong to one or more multicast groups.
Leave	Removes the router from membership in multicast groups.
Mcache	Displays a list of currently active multicast forwarding cache entries.
Mgroups	Displays the group membership of the router's attached interfaces.
Mstats	Displays various multicast routing statistics.
Exit	Exits the DVMRP console process and returns to the GWCON environment.

? (Help)

Use the ? (help) command to list the commands that are available from the current prompt level. You can also enter a ? after a specific command name to list its options.

Syntax: ?

Example: **?**

```
DUMP routing tables
EXIT
INTERFACE summary
JOIN
LEAVE
MCACHE
MGROUPS
MSTATS
```

Dump Routing Tables

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

Syntax: dump

Example: **dump**

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

Type	Displays the type of multicast sources (i.e., DVMRP)
Origin-Subnet	Displays the IP address of the originating subnet.
From-Gateway	Displays the IP address of the gateway from which the entry came.
Metric	Displays the associated cost of that route.
Age	Displays the age of routing table entry as the number of seconds since the routing table entry was refreshed.
In	Displays the DVMRP VIF that multicast datagram from the source must be received on.
Out-Vifs	Displays those VIFs that will send the multicast datagrams. VIFs marked with an asterisk indicate that a datagram will only be forwarded if there are group members on the attached network.

Interface Summary

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

Syntax: interface *interface-ip-address*

Example: **`interface`**

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

Vif	Displays the number assigned to DVMRP interfaces (or VIFs) command. Each VIF is assigned a number, which is used to identify the VIF in other commands
Local Address	Displays the local IP address of the DVMRP interface.
Metric	The associated cost of the route.
Threshold	Reflects the ability of a network to control external flow of multicast packets outside of the network. Multicast packets to be forwarded on the interface must have a time-to-live (TTL) value greater than the configured threshold.
Flags	Displays whether the VIF is down or that the router is the querier (i.e., sender of IGMP Host Membership Queries) on the interface.

Join

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

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

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

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

Syntax: join *multicast-group-address*

Example: **`join 224.185.00.00`**

Leave

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

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

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

Syntax: leave *multicast-group-address*

Example: **`leave 224.185.00.00`**

Mcache

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

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

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

Syntax: mcache

Example: **`mcache`**

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

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

Source	Source network/subnet of matching datagrams.
Destination	Destination group of matching datagrams.
Count	Displays the number of entries processed for that multicast group.

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

Downstream — Displays the total number of downstream interfaces/neighbors to which the datagram will be forwarded. When this is 0, the datagram will not be forwarded.

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

Example: **`mcache 128.185.182.9 224.0.1.2`**

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

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

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

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

Mgroups

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

Syntax: mgroups

Example: **`mgroups`**

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

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

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

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

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

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

Mstat

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

Syntax: mstats

Example: **`mstats`**

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

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

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

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

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

DVMRP forwarding — Displays whether the router will forward IP multicast datagrams between Autonomous Systems.

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

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

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

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

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

No matching rcv interface	Displays the count of those datagrams that were received by a non-inter-AS multicast forwarder on a non-MOSPF interface.
Unreachable source	Displays a count of those datagrams whose source address was unreachable.
Unallocated cache entries	Displays a count of those datagrams whose cache entries could not be created due to resource shortages.
Off multicast tree	Displays a count of those datagrams that were not forwarded either because there was no upstream neighbor or no downstream interfaces/neighbors in the matching cache entry.
Unexpected DL multicast	Displays a count of those datagrams that were received as datalink multicasts on those interfaces that have been configured for datalink unicast.
Buffer alloc failure	Displays a count of those datagrams that could not be replicated because of buffer shortages.
TTL scoping	Indicates those datagrams that were not forwarded because their TTL indicated that they could never reach a group member.
DVMRP routing entries:	Displays the number of DVMRP routing entries.
DVMRP entries freed:	Indicates the number of DVMRP entries that have been freed. The size will be the number of routing entries minus the number of entries freed.
# fwd cache alloc	Indicates the number of cache entries allocated. The current forwarding cache size is the number of entries allocated (“# fwd cache alloc”) minus the number of cache entries freed (“# fwd cache freed”).
# fwd cache freed	Indicates the number of cache entries freed. The current forwarding cache size is the number of entries allocated (“# fwd cache alloc”) minus the number of cache entries freed (“# fwd cache freed”).
# fwd cache GC	Indicates the number of cache entries were cleared because they were not recently used and the cache overflowed.
# local group DB alloc	Indicates the number of local group database entries allocated. The number allocated (“# local group DB alloc”) minus the number freed (“# local group DB free”) equals the current size of the local group database.
# local group DB free	Indicates the number of local group database entries freed. The number allocated (“# local group DB alloc”) minus the number freed (“# local group DB free”) equals the current size of the local group database.

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

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: `exit`

Chapter 6. Using and Configuring AppleTalk Phase 2

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

Basic Configuration Procedures

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

Enabling Router Parameters

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

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

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

Setting Network Parameters

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

- Set the Network Range for Seed Routers - Coordinating network ranges and zone lists for all routers on a network is simplified by having specific routers designated as seed routers. Seed routers are configured with the network range and zone list while all other routers are given null values. Null values indicate that the router should query the network for values from the seed routers. For every network (segment) of your interconnected AppleTalk internet, at least one router interface must be configured as the seed router for that network. There are usually several seed routers on a network in case one of them fails. Also, a router can be a seed router for some or all of its network interfaces. Use the **set net-range** command to assign the network range in seed routers.
- Set the Starting Node Number - Use the **set node** command to assign the starting node number for the router. The router will AARP for this node, but if it is already in use, a new node will be chosen.
- Add a Zone Name - You can add one or more zone names for each network in the internetwork. You can add a zone name for a given network in any router connected to that network; however, only the seed router needs to contain the zone name information for a connected network. Attached routers dynamically acquire the zone name from adjacent routers using the ZIP protocol. Apple recommends that, for a given network, you choose the same seed router for the network number and the zone name. The zone name cannot be configured for a network unless the network number is also configured. To add a zone name for each network number, use the AppleTalk Phase 2 configuration **add zone** *name* command.

AppleTalk 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

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

General Information

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

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

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

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

Why ZoneName Filters?

When the typical AppleTalk end station wants to use a service (printer, file server) on the Apple Internet, it first looks at all available Zones and selects one. It then chooses a service type and requests a list of all names advertising the type in the chosen Zone. Several problems arise from this mechanism.

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

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

How Do You Add Filters?

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

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

  Use similar commands to create network number filters.

Other Commands:

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

Sample Configuration Procedures

This section covers the steps required to get AP2 up and running. For information on how to make further configuration changes, see “AppleTalk Phase 2 Configuration Commands” on page 6-8. 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 6-1 on page 6-6.

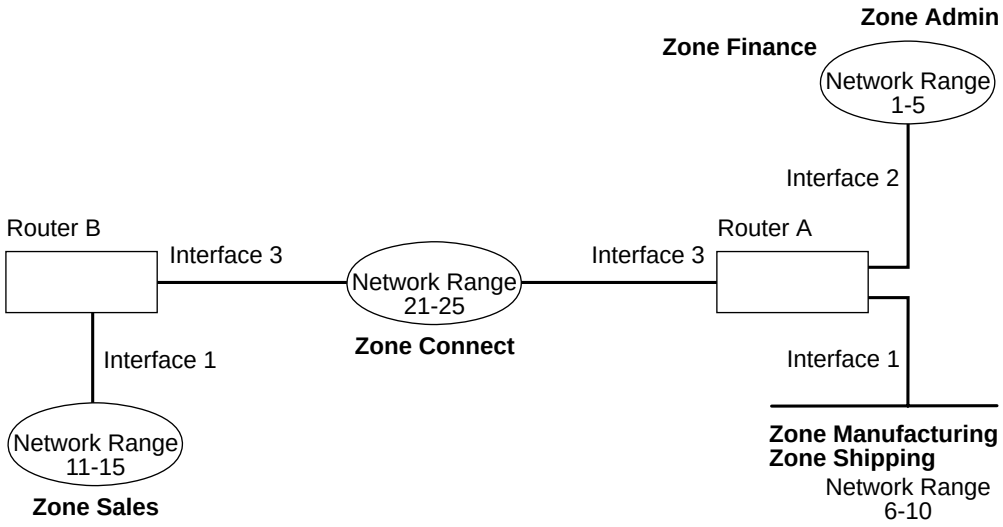


Figure 6-1. Example of Zone Filtering

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 shown Figure 6-2.

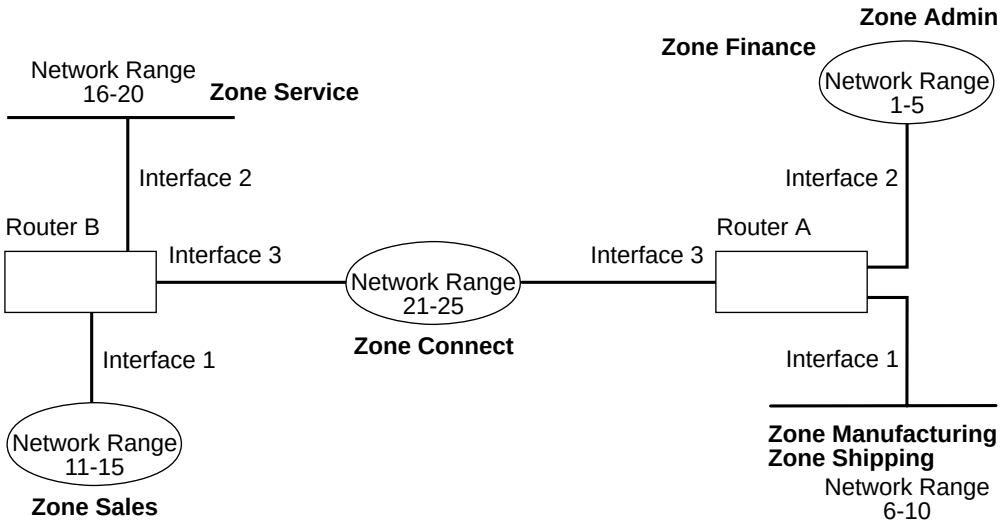


Figure 6-2. Example of Network Filtering

Example

The following example shows how to filter Network 6-10 so that it is not visible to Network 16-20 as shown in Figure 6-2 on page 6-7.

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.

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 summarizes and then explains 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 6-1 on page 6-9 shows the commands.

Table 6-1. AppleTalk Phase 2 Configuration Commands Summary

Command	Function
? (Help)	Lists the AppleTalk Phase 2 configuration commands or lists the options associated with specific commands.
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	Exits the AppleTalk Phase 2 configuration process and returns to the CONFIG environment.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter a ? after a specific command name to list its options.

Syntax: ?

Example: **`?`** OR **`disable ?`**

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: **`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: 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: 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: 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: 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: 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: `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: `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: `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: `delete zfilter 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: `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: `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: `disable checksum`

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

Example: `disable interface 2`

nfilter in *interface#*
Disables, but does not delete, the input network filters on this interface.

Example: `disable nfilter in`

```
Interface # [0]? 2
```

nfilter out *interface#*
Disables, but does not delete, the output network filters on this interface.

Example: `disable nfilter out`

```
Interface # [0]? 2
```

zfilter in *interface#*
Disables, but does not delete, the input zone filters on this interface.

Example: `disable zfilter in`

```
Interface # [0]? 1
```

zfilter out *interface#*
Disables, but does not delete, the output zone filters on this interface.

Example: `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: `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 oout . . .
split-horizon-routing . . .
zfilter . . .

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

Example: `enable ap2`

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

Example: **`enable checksum`**

interface *interface#*

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

Example: **`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: **`enable nfilter 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: **`enable nfilter out exc`**

```
Interface # [0]? 1
```

split-horizon-routing *interface #*

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

Example: **`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: **`enable zfilter in inc`**

```
Interface # [0]?
```

Example: **`enable zfilter out exc`**

```
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 and an unseeded router on interface 2. Interface 2 will learn the network number and zone name from a seed router.

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

Syntax: list

Example: **`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 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 nodes to simultaneously communicate through the router and still use fastpath. If the number of 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: `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 2216 to an IBM 6611 using a PPP interface, set the 2216 for “half-router” mode which is the *only* mode of operation supported by the IBM 6611 for AppleTalk communications over a PPP interface.

Example: `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: `set node 2 2`

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: `exit`

Chapter 7. Monitoring AppleTalk Phase 2

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

- "Accessing the AppleTalk Phase 2 Console Environment"
- "AppleTalk Phase 2 Monitoring Commands"

Accessing the AppleTalk Phase 2 Console Environment

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

```
+ protocol ap2
AP2>
```

AppleTalk Phase 2 Monitoring Commands

This section summarizes and then explains the AppleTalk Phase 2 console commands which allow you to view the parameters and statistics of the interfaces and networks that transmit AppleTalk Phase 2 packets. Console 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 console commands at the AP2> prompt. Table 7-1 shows the commands.

Table 7-1. AppleTalk Phase 2 Console Command Summary

Command	Function
? (Help)	Lists all the AppleTalk Phase 2 console commands or lists the options associated with specific commands.
Atecho	Sends echo requests and watches for responses.
Cache	Displays the cache table entries.
Clear Counters	Clears all cache usage counters and packet overflow counters.
Counters	Displays the overflow count of AP2 packets for each interface.
Dump	Displays the current state of the routing table for all networks in the internet and their associated zone names.
Interface	Displays the current addresses of the interfaces.
Exit	Exits the AppleTalk Phase 2 console process and returns to the GWCON environment.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter a ? after a specific command name to list its options.

Syntax: ?

Example: ?

```
atecho
cache
clear-counters
counters
dump
interface
exit
```

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*

Example: **`atecho 1 27`**

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

Example: **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:

Dir - indicates that the interface is connected directly to the destination network, the interface is enabled, and the network number is known. (The interface is used to retrieve the routing table.)

Good - indicates that an RTMP packet containing a good tuple for this network was heard in the last 20 seconds.

Suspct - indicates that no RTMP tuple was received for this network in the last 20 seconds.

Bad - indicates that no RTMP tuple was received for this network in the last 40 seconds. RTMP packets with tuples listing this network as unreachable will be sent for 20 seconds, then the network will be deleted from the RTMP routing table. (For more information, refer to the RTMP chapter in *Inside AppleTalk Second Edition* by Gursharan S. Sidhu.)

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

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

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: **`exit`**

Chapter 8. Using and Configuring 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 2216 has a configurable network address. This address identifies the router as a service network node for Vines. Banyan has assigned the range 30900000 to 3097FFFF to IBM for use in its routers.

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.

In the VINES addressing scheme, client nodes on the same physical network can have different network addresses. This can occur when a physical network has two service nodes and two network addresses. In this instance, the client node is assigned the network address of the service node that responds first to the client node's address assignment request.

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 8-4. Distributes topological information to support the routing services provided by VINES IP.
- "Internet Control Protocol (ICP)" on page 8-6. 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 8-6. 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 8-1 on page 8-3 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 8-1. Vines IP Header Fields Summary

VINES IP Header Field	# of Bytes	Description
Checksum	2	Detects bit-error corruption of a packet.
Packet Length	2	Indicates the number of bytes in the packet including the VINES IP header and data.
Transport Control	1	Consists of the following five subfields: **Class** Determines the type of nodes to which VINES IP broadcast packets are sent. **Error** If the error bit is set, an exception notification packet is sent to the transport layer protocol entity when a packet cannot be routed to a service or client node. **Metric** Requests that the service node of the destination client node return to the source a routing cost from the service node to the destination client node. **Redirect** Indicates whether the packet contains an RTP message specifying a better route to use. **Hop Count** Specifies the range a packet can travel. The hop count can range from 0x0 to 0xf.
Protocol Type	1	Specifies the VINES network layer protocol of the packet as VINES IP, RTP, ICP, or VINES ARP.
Destination Network Number	4	A 4-byte network number in the VINES IP address of the destination.
Destination Subnetwork Number	2	A 2-byte subnetwork number in the VINES IP address of the destination.
Source Network Number	4	A 4-byte network number in the VINES IP address of the source.
Source Subnetwork Number	2	A 2-byte subnetwork number in the VINES IP address of the source.

Routing Update Protocol (RTP)

RTP gathers and distributes routing information that VINES IP uses to compute routes throughout the network. RTP enables each router to periodically broadcast routing tables to all of its neighbors. The router then determines the destination neighbor it will use to route the packet.

Service nodes maintain two tables: a routing table and a neighbor table. Both of these tables have timers that age their contents to eliminate out-of-date entries. Routing updates for X.25 interfaces occur when there is a change in the routing database, for example, when a node goes up/down or the metric changes.

Routing Table

The routing table contains information about the service nodes. Figure 8-1 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 8-1. 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 8-2 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 8-2. Sample Neighbor Table

Neighbor Table Field Description

Nbr Address The address of the neighbor node. In Figure 8-2, 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 8-2 summarizes the states the service and client nodes enter during VINES ARP implementation.

Table 8-2. Client and Service Node VINES ARP States

Client Node States	
Initialization	The client node is initializing.
Query	The client node is transmitting a query request packet.
Request	The client node received a query response packet from a service node and is transmitting an assignment request packet to the service node it heard from.
Assigned	The client node received an assignment response packet containing the VINES network and subnetwork addresses.
Service Node States	
Initialization	The VINES ARP protocol is initializing.
Listen	The service node is waiting for query request packets from the client nodes.
Service	The service node received a query request packet and sent a query response packet.
Assignment	The service node issues an assignment response packet containing the VINES network and subnetwork addresses.

Basic Configuration Procedures

The steps to initially configure each router that sends and receives VINES packets are as follow:

1. Assign a unique 32-bit hexadecimal address to each router in the VINES network. Using the **set network-address** *hex #* command, enter a network address from 30900000 to 3097FFFF. This range of addresses has been reserved for IBM by Banyan. 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.

To enable a new configuration, enter the **restart** command after the OPCON prompt (*) and answer **yes** to the following prompt:

```
Are you sure you want to restart 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 **2216s**:

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 (i.e., 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.

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 8-3. VINES Configuration Commands Summary

Command	Function
? (Help)	Lists all the VINES configuration commands and their options.
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 to the previous prompt level.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: ?

Example: ?

```
ADD X.25 ADDRESS
DELETE X.25 ADDRESS
ENABLE
DISABLE
SET
LIST
EXIT

VINES config>
```

Example: `disable ?`

```
VINES
INTERFACE
CHECKSUMMING

VINES config>
```

Add

Adds an X.25 address translation.

Syntax: add interface ...

interface # *remote-X.25-addr handle*
Adds an X.25 address translation. *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* is a 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 ...

interface # *remote-X.25-addr*
Deletes an X.25 address translation. If the specified interface has not been configured using the VINES **add interface** command, the console 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 2216s 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 2216s 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`

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: `exit`

Chapter 9. Monitoring VINES

This chapter describes the VINES console commands and includes the following sections:

- "Accessing the VINES Console Environment"
- "VINES Console Commands"

Accessing the VINES Console Environment

To access the VINES console environment, enter the following command at the * prompt:

```
* t 5
```

Then, enter the following command at the + prompt:

```
+ protocol vin
VINES>
```

VINES Console Commands

This section summarizes and then explains the VINES console commands. Enter these commands at the VINES> prompt.

Table 9-1. VINES Console Command Summary

Command	Function
? (Help)	Lists the VINES console commands and their options.
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 to the previous prompt level.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: ?

Example: ?

```
COUNTERS
ROUTE given address
DUMP
EXIT
```

Example: dump ?

```
NEIGHBOR-TABLES
ROUTING-TABLES
```

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 holdown 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 holdown state.

P: After initialization, the X.25 interface enters permanent state for 4 and 1/2 minutes. After 4 and 1/2 minutes, the neighbor enters the permanent state and its age stays at 0 while in this state. If the X.25 interface goes down, the entry is removed from the routing table.

Next Hop Nbr Addr The address of the neighbor service node that is the next hop on the least-cost path to the network.

Nbr Intf The medium to which the next hop neighbor service node is attached.

Metric An estimated cost, in 200-milliseconds, to route the VINES packet to the destination service node.

Age (secs) The current age, in seconds, for the entry. If a router does not receive a routing update about a service node that is in the routing table at least every 360 seconds (6 minutes), the router removes the entry for that service node from the routing table.

Route

Use the **route** command to view an entry from the routing table. *Given address* is the network address of the service node.

Syntax: route *given address*

Example: **`route 30622222`**

```
Net Address   Next Hop Nbr Addr  Nbr Intf   Metric  Age (secs)

30622222      30622222:0001       Eth/0       2       30
```

Exit

Use the **exit** command to return to the previous prompt.

Syntax: exit

Example: **`exit`**

Chapter 10. Using, Configuring, and Monitoring 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 since 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 discussion 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.

Note: When configuring DNA IV to run over ATM LAN Emulation, the AMA must be used.

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 endnodes know to use it as their default gateway. Any endnode 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 endnodes 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.

Endnodes 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 endnodes one hop away from this endnode
- 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 allows 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" on page 10-6
  - Provides additional security by limiting access within routers in the network.
- "Managing Traffic Using Area Routing Filters" on page 10-9
  - 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 10-13.

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 allows 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

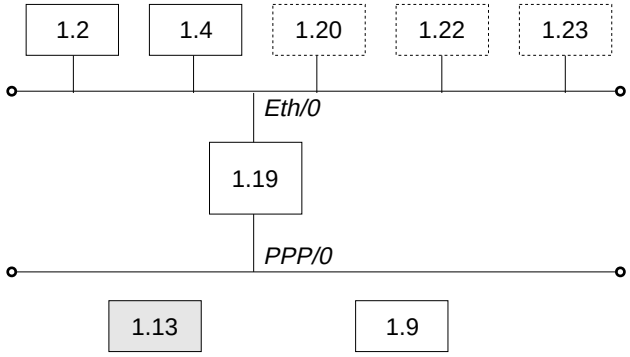
Access control limits access to a particular host or group of hosts. You must assign access control to all routes to that host, not just the preferred route. Otherwise, access control functions when the primary route is up, but fails when the secondary route is in use.

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 10-1, 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 10-1 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 10-1



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 10-1. Example of Inclusive Access Control

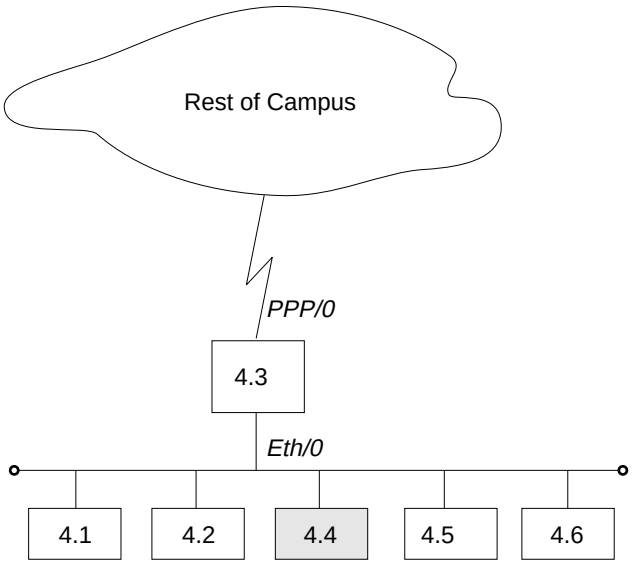
The first and second entries of the inclusive filter information shown in Figure 10-1 allow nodes 1.2 and 1.4 to send packets to node 1.13. The third entry allows any node to send to node 1.9 (you are not trying to secure node 1.9).

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 10-2 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 10-2. 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 10-2. To configure the example given for router 4.3 in Figure 10-2, 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 10-3 on page 10-10, 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 10-3, 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
```

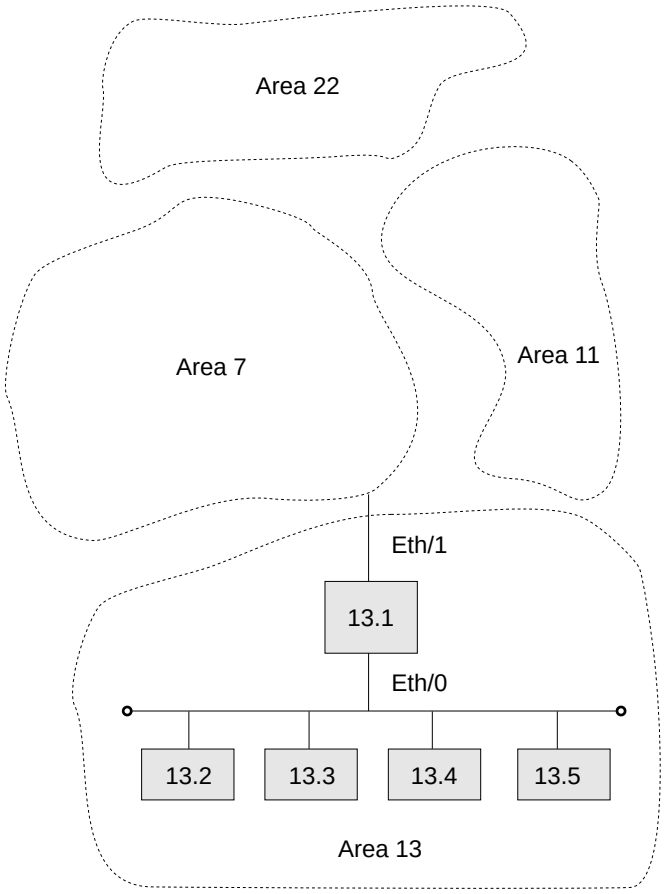


Figure 10-3. Example of Area Routing Filter for Security

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 multi-level 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 10-4 on page 10-13 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 10-4 on page 10-13, 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
```

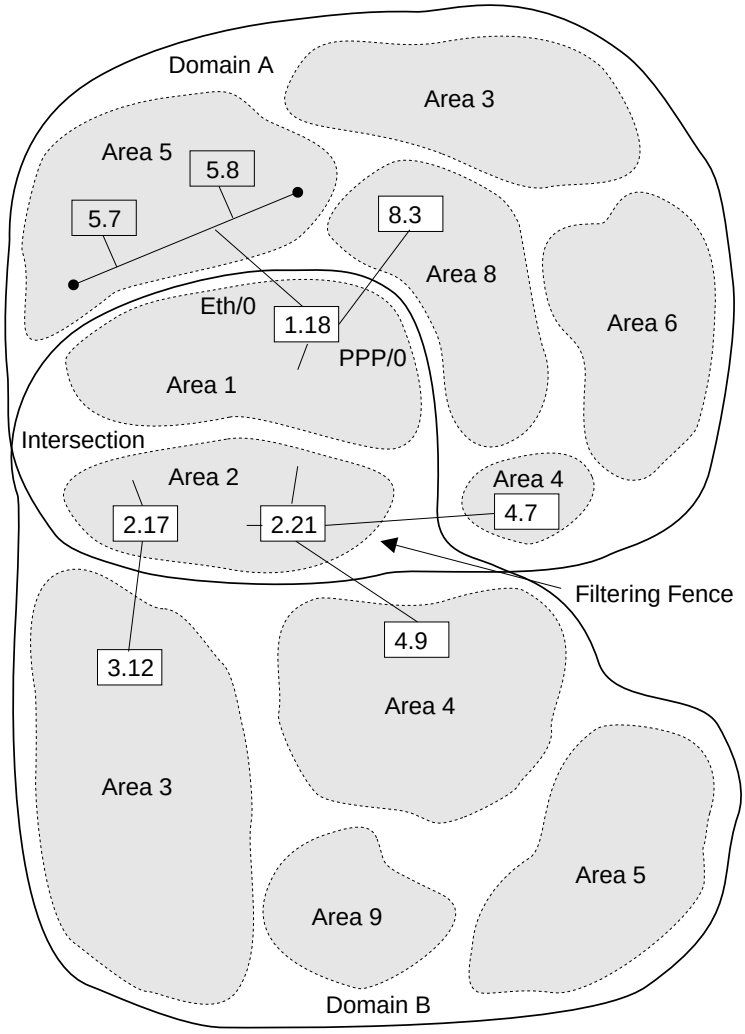


Figure 10-4. Example of Blending DECnet Domains

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 (TKR), Frame Relay, Ethernet, PPP, and X.25 interfaces. The following sections discuss the procedures for configuring the DNA IV protocol to work over these 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 (Table 10-1).

Table 10-1. 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 **show** command to verify that each Token-Ring circuit is working.

```
NCP> show circuits tkr/0 characteristics

Circuit Volatile Characteristics

Circuit=TKR/0

State                          = ON
Designated Router              = 62.412
Cost                           = 4
Router priority                = 10
Hello timer                    = 15
Maximum routers                = 16
Routing type                   = Standard
Adjacent node                  = 62.590
Listen time                    = 90
```

7. Exit NCP.

```
NCP> exit
Config>
```

8. Use the **update version** command only when updating to a new release of software.

9. Check the routing type field in the Circuit Volatile characteristics display. For bilingual or Phase IV support, you need to change the routing type from the default (standard) to either AMA or bilingual. For example:

```
NCP> define circuit tkr/0 router type AMA

                    –or–

NCP> define circuit tkr/0 router type bilingual
```

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
```

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 2216 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**

DNA IV Commands

This section summarizes and explains 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 10-2. NCP Configuration and Monitoring Commands

Command	Function
? (help)	Lists all the NCP commands or lists the options associated with specific commands.
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 to the previous prompt.

Note the following information about the commands:

1. **define** commands do not take effect until the next time the router is started.
2. **list, define,** and **purge** 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. **show** and **list** commands are the most useful for monitoring the DNA IV protocol.
4. **set, show**, and **zero** modify, display, or clear data in the volatile database.
5. **zero** clears statistics saved in the volatile database, but does ***not*** clear the argument settings made with set or define commands.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: **?**

Example: **?**

```
Define
List
Purge
Set
Show
Zero
Exit
```

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 . . .
executor . . .
module access-control . . .
module routing-filter . . .
node . . .

Set can be used for volatile RAM (immediate change, no reboot).

Syntax: set circuit . . .
executor . . .
node . . .

circuit *circuit-specifier argument*

The **define** command sets or changes circuit arguments in the permanent database.

The **set** command sets or changes circuit arguments in the volatile database. The circuits must be in the off state to modify numeric arguments in the volatile database.

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`

Example: `set 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 re-establish 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 endnodes 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 endnodes 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 endnode 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 endnodes. (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 endnodes that can be adjacent (one hop away) to this router. This is the sum over all broadcast circuits. If there are more endnodes, some of those endnodes 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 10-19.

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 endnodes 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. Endnodes 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 endnode 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 endnodes 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`**

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: `exit`

Example: **`exit`**

Chapter 11. Using and Configuring 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 11-1.

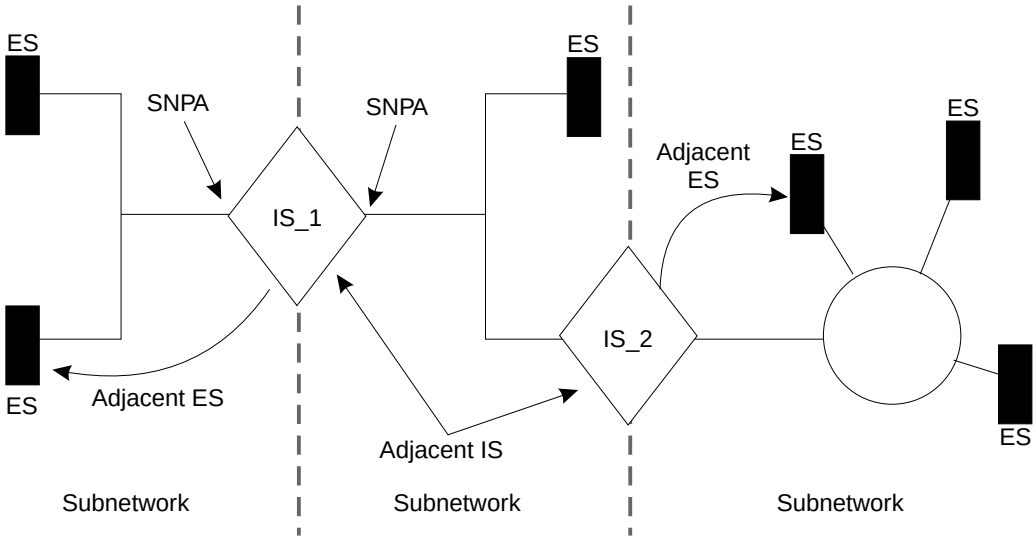


Figure 11-1. OSI Network

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 allows 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 allows 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 11-2.

Figure 11-2. 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 11-3). 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.

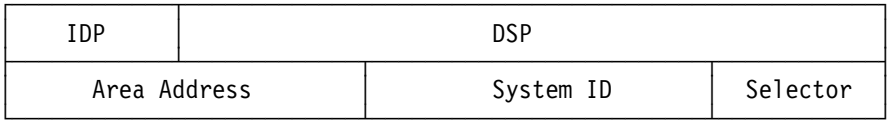


Figure 11-3. IS-IS NSAP Addressing Interpretation

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 11-4 on page 11-4. 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 11-4. 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 11-1 lists the multicast addresses for Ethernet and Token-Ring LANs.

Table 11-1. IS-IS Multicast Addresses

Destination	Ethernet 802.3	Token-Ring 802.5	ProNET10	Address Description
All ESs	09002B000004	C00000004000	FFFFFFFFFFFF	For all end systems on the subnetwork.
All ISs	09002B000005	C00000008000	FFFFFFFFFFFF	For all intermediate systems on the subnetwork.
All L2 ISs	0180C2000015	C00000008000	FFFFFFFFFFFF	For all L2 intermediate systems on the subnetwork.
All L1 ISs	0180C2000014	C00000008000	FFFFFFFFFFFF	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 11-9.

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 metrics.
- All devices use the same routing protocol, such as IS-IS.

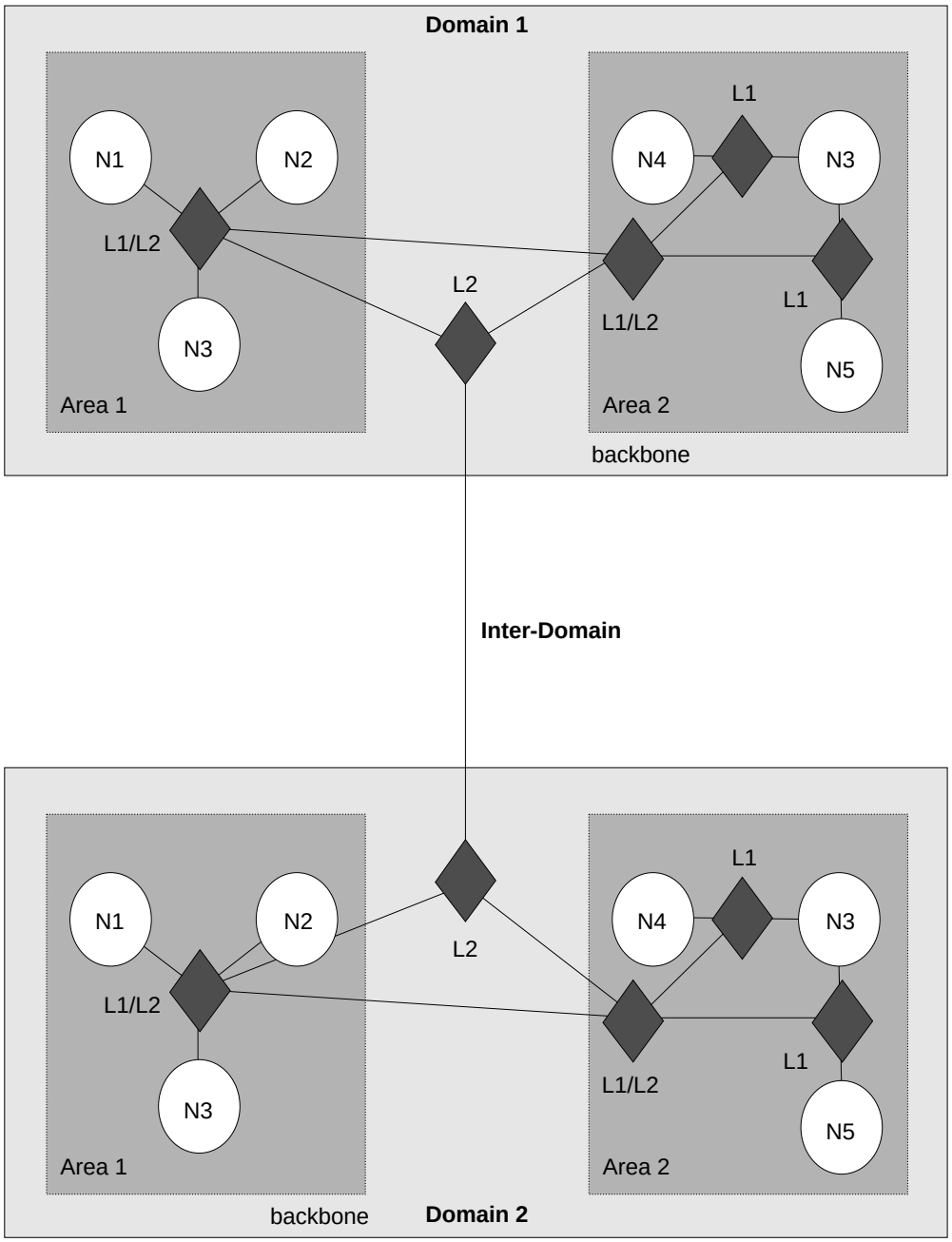


Figure 11-5. OSI Domain

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 11-6 on page 11-7, Area 1 and Area 2 are synonymous areas to each other and Areas 3 and 4 are also synonymous to each other.

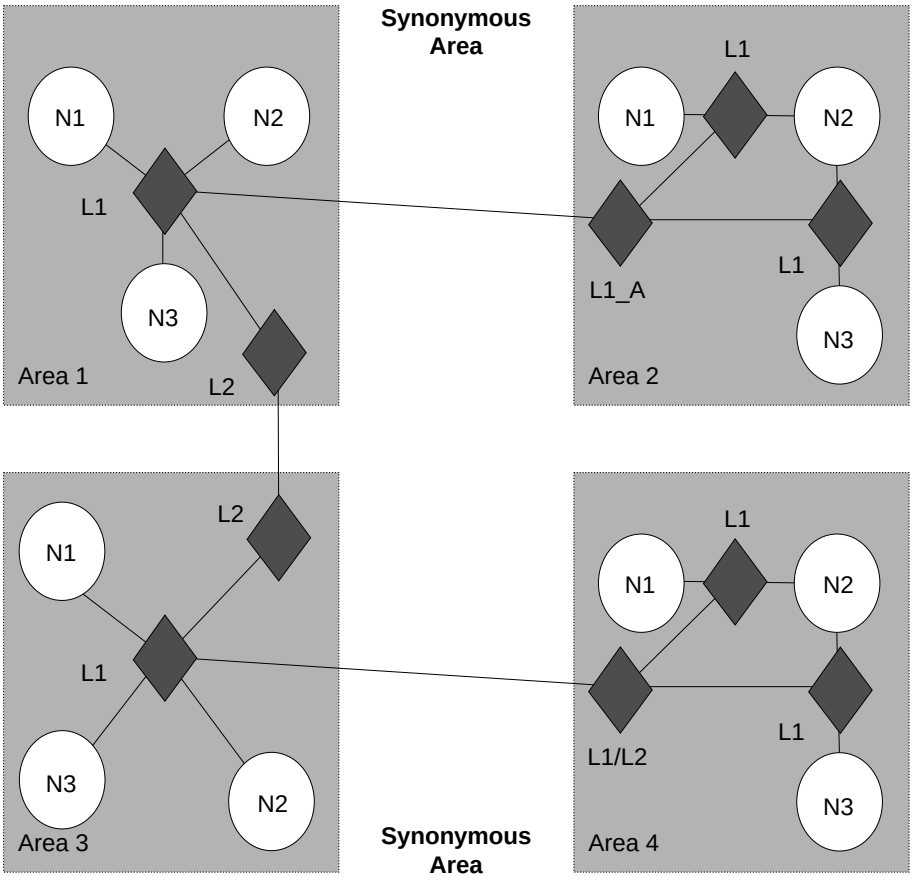


Figure 11-6. Synonymous Areas

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 allows 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” 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 11-7 on page 11-12). 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.

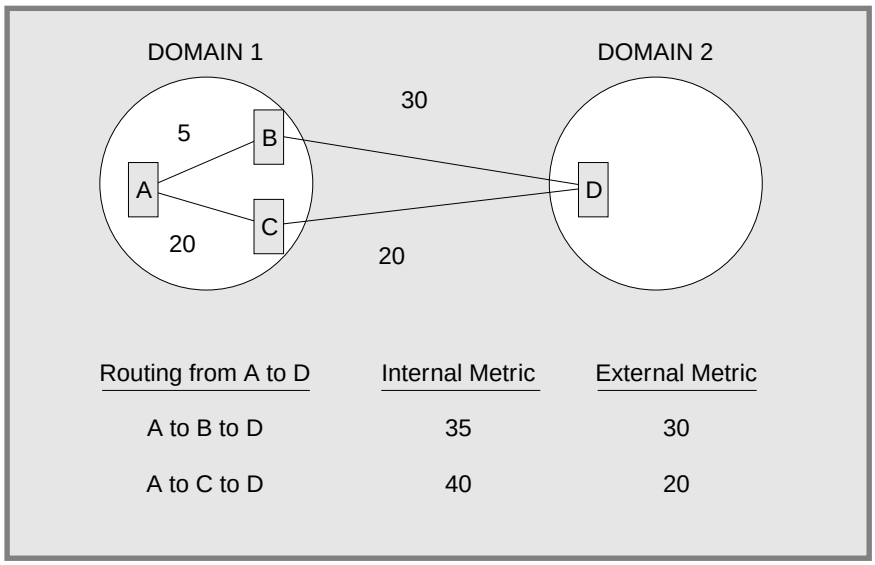


Figure 11-7. Internal and External Routing Metrics

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 since 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), since 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 allows 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 allows 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 X25, 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 10, "Using, Configuring, and Monitoring DNA IV." 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 and token-ring). 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.

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 *Software User's Guide*.

DECnet V/OSI Configuration Commands

This section summarizes and then explains the OSI configuration commands. The OSI configuration commands allow 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 11-2. OSI Configuration Commands Summary

Command	Function
? (Help)	Lists the configuration commands or lists any parameters associated with that command
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	Exits the OSI configuration and returns to the CONFIG environment

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter a **?** after a specific command name to list its options.

Syntax: ?

Example: **?**

```
LIST
ADD
CHANGE
DELETE
ENABLE
DISABLE
SET
CLEAR
EXIT
```

Example: **list ?**

```
GLOBALS
SUBNETS
ADJACENCIES
PASSWORD
PREFIXADDRESSES
ALIAS
ALGORITHM
PHASEIVPFX
TIMERS
```

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 console.

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: **`add 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]?
```

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.

Warning: 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.

Example: **`disable osi`**

routing-circuit *routing-circuit-name*
Disables the specified routing circuit.

Use the **add routing-circuit** command to set up routing-circuits.

Example: **`disable routing-circuit p_system2`**

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.

Example: `enable osi`

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).

```
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 2216 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 allows 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: `set subnet`

X.25 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.

Exit

Use the exit command to return to the previous prompt level.

Syntax: exit

Example: `exit`

Chapter 12. Monitoring OSI/DECnet V

This chapter describes the OSI/DECnet V console commands and includes the following:

- "Accessing the OSI/DECnet V Console Environment"
- "OSI/DECnet V Console Commands"

Accessing the OSI/DECnet V Console Environment

For information on how to access the OSI/DECnet V console environment, refer to *Getting Started (Introduction to the User Interface)* in the *Software User's Guide*.

OSI/DECnet V Console Commands

This section summarizes and then explains the OSI/DECnet V Console commands. Use these commands to gather information from the database.

The monitoring commands either display or modify the volatile database.

Table 12-1 (Page 1 of 2). OSI/DECnet V Console Commands Summary

Command	Function
? (Help)	Displays all the OSI/DECnet V console commands or any options associated with a specific command.
Addresses	Displays the router's NET and area addresses.
Change Metric	Modifies the cost of a circuit.
CLNP-Stats	Displays OSI CLNP statistics.
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.
ESIS-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.

Table 12-1 (Page 2 of 2). OSI/DECnet V Console Commands Summary

Command	Function
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 2216-style router.
Exit	Exits the OSI console command process.

? (Help)

Use the **?** (help) command to list the commands that are available from the current prompt level. You can also enter a ? after a specific command name to list its options.

Syntax: ?

Example: **?**

```
Addresses
Subnets
Designated-router
ES-adjacencies
IS-adjacencies
L1-routes
L2-routes
L1-summary
L2-summary
L1-update
L2-update
CLNP-stats
ESIS-stats
ISIS-stats
Change Metric
Send echo packet
Traceroute address
Route Nsap
Toggle alias/noalias
DNAV-info
```

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
IS0 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 **esis-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.

ISIS-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 psuedonode 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-psuedonode update. 01–FF represents a psuedonode 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 CNLP 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 console. 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      5 ms      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.

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: **`exit`**

Chapter 13. Using and Configuring BGP4

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

This chapter contains the following sections:

Border Gateway Protocol Overview

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

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

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

- Exhaustion of Class B address space
- Routing table growth

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

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

How BGP4 Works

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

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

at this well-known address. The router also opens active TCP connections to enabled BGP neighbors. This TCP connection enables BGP routers to share and update reachability information with neighbors in the same or other autonomous systems.

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

A single AS may have one or many BGP connections to outside autonomous systems. Figure 13-1 shows two autonomous systems. The BGP speaker in AS1 is attempting to establish a TCP connection with its neighbor in AS2. Once this connection is established, the routers will be able to share reachability information.

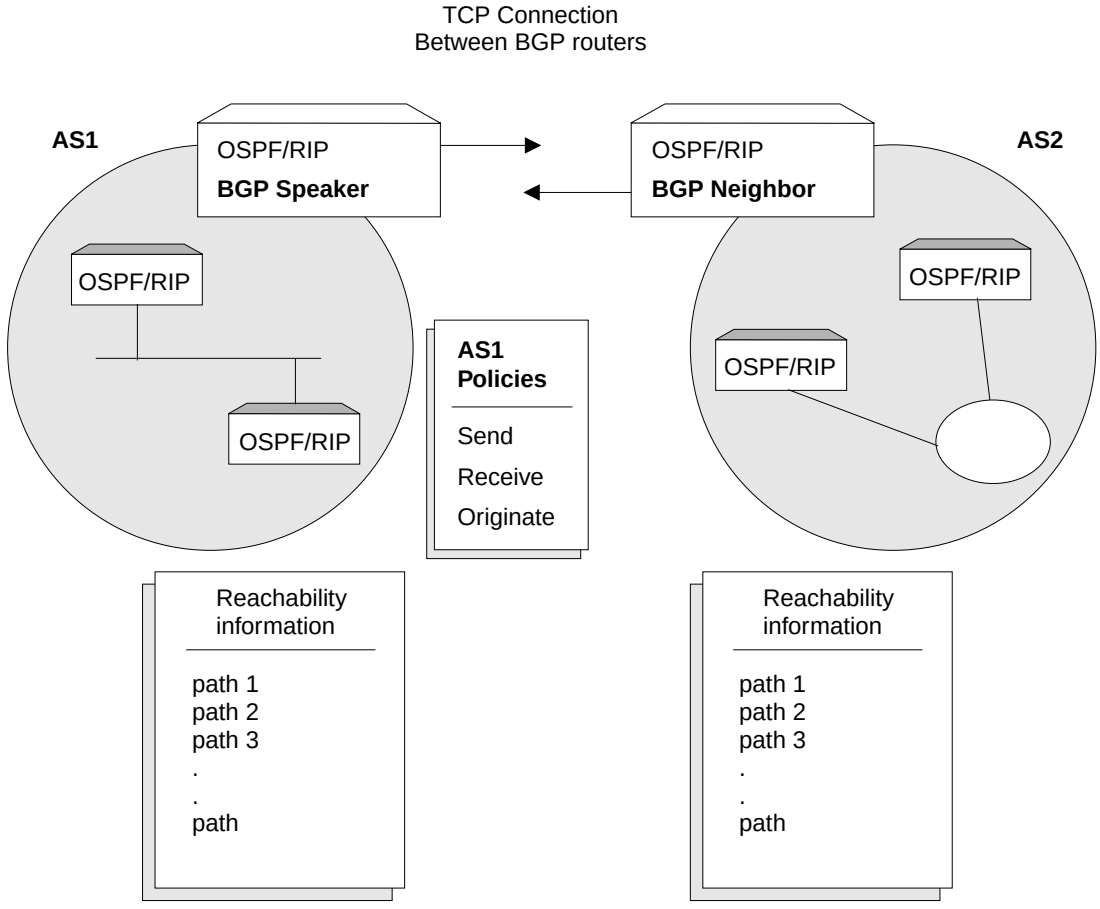


Figure 13-1. BGP Connections between Two Autonomous Systems. Once the BGP speaker in AS1 establishes a TCP connection with its BGP neighbor in AS2, the two routers can selectively exchange reachability information. The information each router sends or accepts is determined by policies defined for each router.

While the autonomous systems shown in Figure 13-1 have only one BGP router, each could have multiple connections to other autonomous systems. As an example of this, Figure 13-2 on page 13-3 shows three interconnected autonomous systems. AS1 has three BGP connections to outside autonomous systems: one to AS2, one to AS3 and one to ASx. Similarly, AS3 has connections to AS1, AS2 and to ASy.

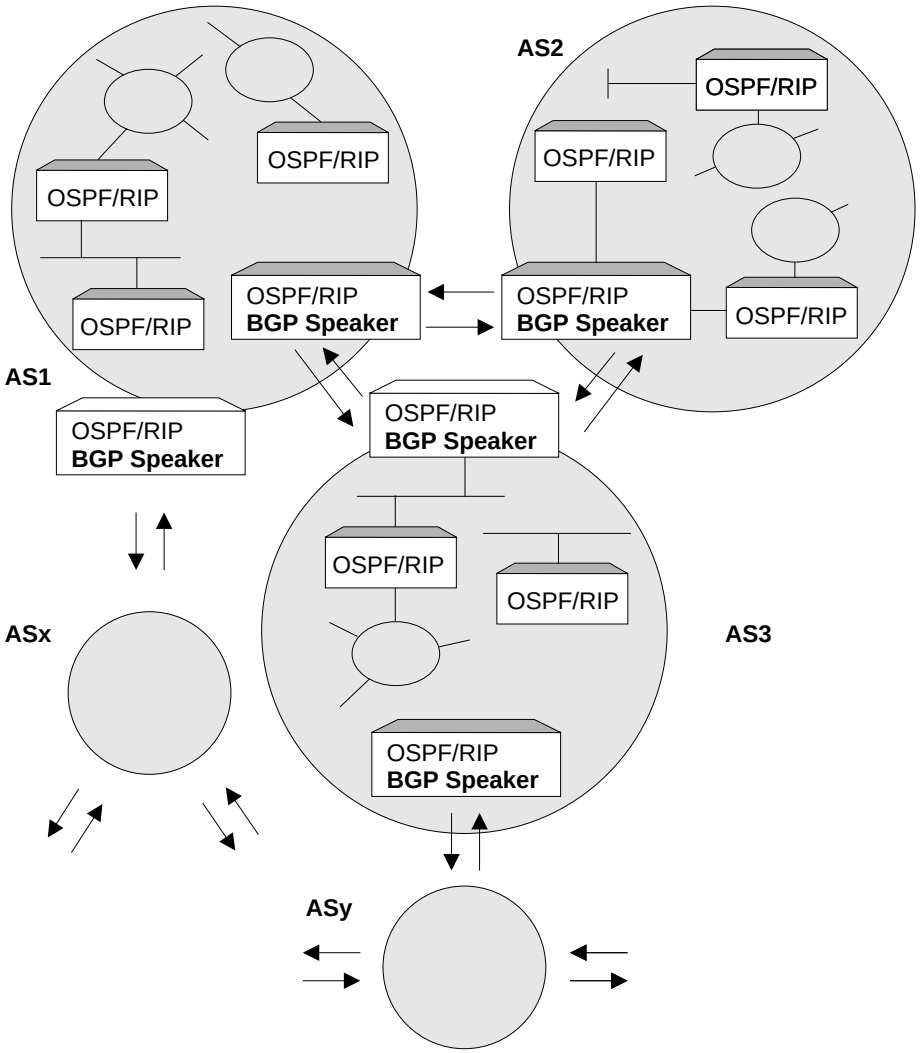


Figure 13-2. BGP Connections among Three Autonomous Systems. Note that AS1 and AS3 have two BGP speakers.

Originate, Send, and Receive Policies

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

- Originate Policies
- Send Policies
- Receive Policies

Once a TCP connection is established, the BGP speaker shown in Figure 13-1 on page 13-2 can send its entire routing table to its BGP neighbor in AS2. However, for security or other reasons, it may not be desirable to send reachability information on each network to AS2. Similarly, it may not be desirable for AS2 to receive reachability information on each network in AS1.

BGP Messages

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

OPEN

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

KEEP ALIVE

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

UPDATE

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

NOTIFICATION

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

Setting Up BGP4

Setting up BGP involves three basic steps:

1. Enabling BGP.

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

2. Defining BGP Neighbors.

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

3. Adding Policies.

   The *policies* you establish determine which routes will be imported and exported by the BGP speaker. You can set up policies for different purposes. See "Sample Policy Definitions" on page 13-5 for more information.

Enabling BGP

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

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

The *AS number* must be in the range 0 to 65535. The *TCP segment* size must be in the range 1 to 65535. The default value for *TCP segment* is 1024. This number represents the maximum segment size BGP will use for passive TCP connections.

Defining BGP Neighbors

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

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

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

Adding a BGP neighbor automatically enables it, causing the BGP speaker to send out a connection request to the neighbor.

Adding Policies

IBM's BGP implementation supports three policy commands:

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

Sample Policy Definitions

This section provides a set of examples of some specific policies you can set up for a BGP speaker. All policies are defined using the BGP **add** command. See "Add" on page 13-8 for the syntax of the **add** command.

Originate Policy Examples

Include All Routes for Advertisement

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

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

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

Exclude a Range of Routes

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

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

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

The tag is the received RIP information. You can select networks based on a particular tag value for advertisement. See the description of the **Set** command in "Using and Configuring IP" in *Protocol Configuration and Monitoring Reference Volume 1 for Nways Multiprotocol Access Services Version 1 Release 1* for information on setting the tag value.

Receive Policy Examples

Import all Routes from All BGP Neighbors

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

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

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

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

Block Specific Routes from a Transit AS

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

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

Block Specific AS-path.

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

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

Send Policy Examples

Restrict Route Advertisement to a Specific AS

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

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

Advertise All Known Routes

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

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

Accessing the BGP4 Console Environment

For information on how to access the BGP console environment, see “Getting Started (Introduction to the User Interface)” in the Software User’s Guide for Nways Multiprotocol Access Services Version 1 Release 1.

BGP4 Configuration Commands

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

Table 13-1. BGP Command Summary

Command	Function
? (Help)	Lists the configuration commands or lists the actions associated with specific commands.
Add	Add BGP neighbors.
Change	Modifies information that was originally entered with the **add** command.
Delete	Deletes BGP configuration information that had been entered with the **add** command.
Disable	Disables certain BGP features that have been turned on by the **enable** command.
Enable	Enables BGP speakers or BGP neighbors.
List	Displays BGP configuration items.
Move	Changes the order in which policies and aggregates are defined.
Exit	Exits the process.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter **?** after a specific command name to list its options.

Syntax: ?
Example: **?**

```
ADD
CHANGE
DELETE
DISABLE
ENABLE
LIST
MOVE
EXIT
```

Add

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

Syntax: add aggregate . . .
neighbor . . .
no-receive asnum . . .
originate-policy . . .
receive-policy . . .
send-policy. . .

aggregate *network prefix* *network mask*

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

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

   Valid Values: Any valid IP address.

Default Value: none

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

   Valid Values: Any valid IP address.

   Default Value: none

Example: **`add aggregate`**

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

When you add an aggregate definition, remember to define a policy to block the aggregated routes from being exported. If you do not, the router will support both the individual routes and the aggregate you have defined.

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

Use the **add neighbor** command to define a BGP neighbor. The neighbor can be internal to the BGP speaker's AS, or external. An internal neighbor must exist on the same network as the speaker.

1. The IP *address of the neighbor* has:

   Valid Values: Any valid IP address.

   Default Value: none

2. The *AS number* of the neighbor has:

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

   Default Value: none

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

   Valid Values: 0 to 65535 seconds.

   Default Value: 12 seconds

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

   Valid Values: 0 to 65535 seconds.

   Default Value: 120 seconds

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

   Once neighbors have established BGP connection, they exchange Keep-alive messages at frequent intervals to ensure that the connection is still alive and the neighbors are reachable. The Keep-Alive timer interval

is calculated to be one-third of the negotiated hold timer value. Hence the hold timer value must be either zero or at least three seconds.

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

Valid Values: 0 to 65535 seconds.

Default Value: 90 seconds

6. The *TCP segment size* specifies the maximum data size that may be exchanged on the TCP connection with a neighbor.

   Valid Values: 0 to 65535 bytes.

   Default Value: 1024 bytes

Example: **`add neighbor`**

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

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

AS
: Your own autonomous system number for internal neighbor or neighbor's autonomous system number.

Init Timer
: Specifies the amount of time the BGP speaker waits to initialize resources and reinitiate transport connection with the neighbor in case the speaker has previously transitioned to IDLE state due to an error. If the error persists, this timer increases exponentially. The default is 12 seconds.

Connect Timer
: The amount of time the BGP speaker waits to reinitiate transport connection to its neighbor if the TCP connection fails while in either CONNECT or ACTIVE state. In the meantime, the BGP speaker continues to listen for any connection that may be initiated by its neighbor. The default is 120 seconds.

Hold Timer
: The length of time the BGP speaker waits before assuming that the neighbor is unreachable. Both neighbors exchange the configured information in OPEN message and choose the smaller of the two timers as their negotiated Hold Timer value. The default is 90 seconds. Once neighbors have established BGP connection, they exchange Keep-alive 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 3 seconds. Note that, on switched lines, you may wish to have the Hold Timer value of zero to

save bandwidth by not sending Keep-Alive messages at frequent intervals.

TCP Segment Size
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. It defaults to 1024, but can be set up in the range 1 to 65535.

no-receive *asnum*

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

The *AS number* has:

Valid Values: 0 to 65535

Default Value: none

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

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

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

Exclusive	Exclusive policies prevent route information from being included in the BGP speaker's routing table.
Inclusive	Inclusive policies ensure that specific routes will be included in the BGP speaker's routing table.
Network prefix	The network prefix for the addresses being affected.
Address match	The address, or range of addresses, that will be affected by the policy statement.
Tag	The value that has been set for a particular AS. All tag values match that of the AS from which they were learned.

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

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

   Valid Values: Any valid IP address.

   Default Value: none

2. Enter the *Network Mask* to be applied to the address specified in Network Prefix to generate an address used in a BGP policy.

   Valid Values: Any valid IP address.

   Default Value: none

3. Select whether the *Address match* is to be a range of addresses or an exact address.

4. A *TAG* is the value that has been set for a particular AS. Tag values match that of the AS from which they were learned.

   Valid Values: 0 to 65535

Default Value: none

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

Example: **add originate-policy exclusive**

```
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

See "Originate Policy Examples" on page 13-5 for detailed examples of this policy command.

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

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

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

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

   Valid Values: Any valid IP address.

   Default Value: none

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

   Valid Values: Any valid IP mask.

   Default Value: none

3. The *Address match* is a range of addresses or an exact address.

4. An *Originating AS#* has:

   Valid Values: 0 to 65535

   Default Value: none

5. The *Adjacent AS#* to specifies the neighboring AS number.

   Valid Values: 0 to 65535

   Default Value: none

Example: **add receive-policy exclusive**

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

See "Receive Policy Examples" on page 13-6 for detailed examples of this policy command.

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

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

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

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

   Valid Values: Any valid IP address.

   Default Value: none

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

   Valid Values: Any valid IP address.

   Default Value: none

3. The *Address match* is a range of addresses or an exact address.

4. A *TAG*. is the value that has been set for a particular AS. Tag values match that of the AS from which they were learned.

   Valid Values: 0 to 65535

   Default Value: none

5. The *Adjacent AS#* specifies the neighboring AS number.

   Valid Values: 0 to 65535

   Default Value: none

Example: **`add send exclusive`**

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

See "Send Policy Examples" on page 13-7 for detailed examples of this policy command.

Change

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

Syntax: change aggregate . . .
neighbor . . .
originate-policy . . .
receive-policy . . .
send-policy. . .

aggregate *index# network prefix network mask*

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

Example: **`change aggregate 1`**

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

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

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

The *neighbor address* to be modified has:

Valid Values: Any valid IP address.

Default Value: none

Example: **change neighbor 192.0.251.165**

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

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

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

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

Example: **change originate-policy**

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

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

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

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

Example: **change receive-policy**

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

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

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

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

Example: **change send-policy**

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

Delete

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

Syntax: delete aggregate . . .
neighbor . . .
no-receive . . .
originate-policy . . .
receive-policy . . .
send-policy. . .

aggregate *index#*

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

Example: **delete aggregate 1**

neighbor *neighbor IP address*

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

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

Valid Values: Any valid IP address.

Default Value: none

Example: **delete neighbor 192.0.251.165**

no-receive *as*

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

The *AS number* has:

Valid Values: 0 to 65535

Default Value: none

Example: **delete no-receive 168**

originate-policy *index#*

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

Example: **delete originate-policy 2**

receive-policy *index#*

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

Example: **delete receive-policy**

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

send-policy *index#*

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

Example: `delete send-policy 4`

Disable

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

Syntax: disable BGP speaker
neighbor . . .

disable bgp speaker

Example: `disable bgp speaker`

disable neighbor *neighbor IP address*

The *neighbor address* has:

Valid Values: Any valid IP address.

Default Value: none

Example: `disable neighbor 192.0.190.178`

Enable

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

Syntax: enable BGP speaker
neighbor . . .

bgp speaker *as# tcp segment size*

Use the enable bgp speaker command to enable the BGP protocol.

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

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

   Valid Values: 0 to 65535

   Default Value: none

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

   Valid Values: 0 to 65535 bytes.

   Default Value: 1024 bytes

Example:

```
enable bgp speaker
AS [0]? 165
TCP segment size [1024]?
```

neighbor *neighbor IP address*

Use this command to enable a BGP neighbor.

The *neighbor address* has:

Valid Values: Any valid IP address.

Default Value: none

Example: **`enable neighbor 192.0.190.178`**

List

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

Syntax: list aggregate
all
BGP speaker
neighbor
no-receive
originate-policy
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              Mask
1         194.10.16.0        255.255.240.0
```

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

Example: **`list all`**

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

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

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

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

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

Aggregation:

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

bgp speaker

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

Example: **`list BGP speaker`**

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

neighbor

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

Example: `list neighbor`

```
Neighbors and their AS:

                                    Init    Conn    Hold    TCPSEG
Address            State     AS     Timer   Timer   Timer   Size

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

no-receive

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

Example: `list no-receive`

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

originate-policy *all* *index* *prefix*

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

Example: `list originate-policy`

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

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

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

Example: `list receive-policy`

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

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

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

Example: `list send-policy`

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

Move

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

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

Example: **move originate-policy**

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

Exit

Use the **exit** command to leave the BGP configuration module and return to the `Config>` prompt.

Syntax: exit

Example: **exit**

Chapter 14. Monitoring BGP4

This chapter describes the BGP console commands and includes the following sections:

- "Accessing the BGP Console Environment"
- "BGP4 Console Commands"

Accessing the BGP Console Environment

For information on how to access the BGP console environment, see "Getting Started (Introduction to the User Interface)" in the Software User's Guide for Nways Multiprotocol Access Services Version 1 Release 1.

BGP4 Console Commands

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

Table 14-1. BGP Command Summary

Command	Function
? (Help)	Lists the monitoring commands or lists the actions associated with specific commands.
Destinations	Displays all entries in the BGP routing table.
Dump routing tables	Lists the contents of the IP routing table.
Neighbors	Displays currently active neighbors.
Paths	Displays all available paths in the database.
Ping	Sends ICMP Echo Requests to another host once a second and watch for a response. This command can be used to isolate trouble in an internetwork environment.
Sizes	Displays the number of entries in various databases.
Traceroute	Displays the complete path (hop-by-hop) to a particular destination.
Exit	Exits the process.

? (Help)

Use the **? (help)** command to list the commands that are available from the current prompt level. You can also enter **?** after a specific command name to list its options.

Syntax: ?
Example: **?**

```
DESTINATIONS
NEIGHBORS
PATHS
SIZES
EXIT
```

Destinations

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

Syntax: destinations *net address/net address net mask*
advertised-to *network address*
received-from *network address*

Example: `destinations`

```
Network         Mask       NextHop          MED AAG AGRAS ORG ASPath
128.185.0.0     FFFF0000   192.0.251.165    0   No  0     IGP
142.4.0.0       FFFF0000   192.0.190.178    0   No  0     IGP seq[178]
143.116.0.0     FFFF0000   128.185.252.168  0   No  0     IGP seq[168]
192.0.190.0     FFFFFF00   192.0.251.165    0   No  0     IGP
192.0.251.0     FFFFFF00   192.0.251.165    0   No  0     IGP
194.10.16.0     FFFFF000   192.0.251.167    0   No  167   IGP seq[167]
```

destinations *net address*

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

Example: `destinations 142.4.0.0`

```
Network         Mask     NextHop         MED AAG AGRAS ORG ASPath
142.4.0.0       FFFF0000 192.0.251.165   0   No  0     IGP
seq[165-178]Dest:142.4.0.0, Mask:FFFF0000, Age:180, Upd#:13,
LastSent:0001:53:32 Eligible paths: 2

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

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

ASpath Enumeration of autonomous systems along the path.

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

-set: Set of autonomous systems in the path.

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

LocalPref The originating router's degree of preference for the destination.

Metric The path metric with which the route is imported.

Weight The path weight.

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

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

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

destinations *net address net mask*

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

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

Example: destinations 194.10.16.0 255.255.240.0

```
Dest:194.10.16.0, Mask:FFFFF000, Age:0, Upd#:3, LastSent:0002:00:00

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

destinations advertised-to *net address*

Lists all routes advertised to the specified BGP neighbor.

Example: destinations advertised-to

```
BGP neighbor address [0.0.0.0]? 192.0.251.165

        Destinations advertised to BGP neighbor 192.0.251.165

Network       Mask     NextHop         MED AAG AGRAS ORG ASPath
194.10.16.0   FFFFF000 194.10.16.167   0   No  167   IGP
192.0.190.0   FFFFFF00 192.0.251.165   0   No  0     IGP seq [165]
142.4.0.0     FFFF0000 192.0.251.165   0   No  0     IGP seq [165-178]
143.116.0.0   FFFF0000 128.185.250.168 0   No  0     IGP seq [168]
```

destinations received-from *net address*

Lists all routes received from the specified BGP neighbor.

Example: destinations received-from

```
BGP neighbor address [0.0.0.0]? 128.185.250.167

        Destinations obtained from BGP neighbor 128.185.250.167

Network     Mask     NextHop         MED AAG AGRAS ORG ASPath
194.10.16.0 FFFFF000 128.185.250.167 0   No  167   IGP seq[167]
192.0.190.0 FFFFFF00 128.185.250.167 0   No  0     IGP seq[167-165]
142.4.0.0   FFFF0000 128.185.250.167 0   No  0     IGP seq[167-165-178]
```

Dump Routing Tables

For a complete explanation of the **dump routing tables** command, refer to “Dump Routing Table” in the “Monitoring IP” chapter of *Protocol Configuration and Monitoring Reference Volume 1 for Nways Multiprotocol Access Services Version 1 Release 1*.

Neighbors

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

Syntax: neighbors *internet address*

Example: **neighbors**

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

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

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

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

- Connect — Waiting for the TCP connection to the neighbor to be completed.
- Active — In the event of TCP connection failure, the state is changed to Active, and the attempt to acquire the neighbor continues.
- OpenSent — In this state OPEN has been sent, and BGP waits for an OPEN message from the neighbor.
- OpenConfirm — In this state a KEEPALIVE has been sent in response to neighbor’s OPEN, and waits for a KEEPALIVE/NOTIFICATION from the neighbor.
- Established — A BGP connection has been successfully established, and can now start to exchange UPDATE messages.

BGP-ID — Specifies the neighbor’s BGP Identification number.

AS — Specifies the neighbor’s AS number.

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

internet-address

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

Example: **neighbor 192.0.251.167**

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

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

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

Open Msg Errs:    Sent       Received                    Sent
Received
Unsupp versions:  0          0          Unsupp auth code: 0         0
Bad peer AS ident:0          0          Auth failure:    0          0
Bad BGP ident:    0          0          Bad hold time:   0          0

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

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

Paths

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

Syntax: paths

Example: **paths**

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

PathId Path identifier

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

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

AAG Indicates if the path has been atomic-aggregated that is the router that is advertising the given path has selected less specific route over the more specific one when presented with overlapping routes.

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

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

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

AS Path Enumeration of autonomous systems along the path.

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

set: Set of autonomous systems in the path.

Ping

For a complete explanation of the **ping** command, see the IP Ping command in the "Monitoring IP" chapter in *Protocol Configuration and Monitoring Reference Volume 1 for Nways Multiprotocol Access Services Version 1 Release 1*.

Sizes

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

Syntax: sizes

Example: **`sizes`**

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

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

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

Update sequence#
Indicates the current update sequence number.

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

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

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

Traceroute

For a complete explanation of the **traceroute** command, see its description in the "Monitoring IP" chapter of Protocol Configuration and Monitoring Reference Volume 1 for Nways Multiprotocol Access Services Version 1 Release 1.

Exit

Use the **exit** command to return to the previous prompt level.

Syntax: exit

Example: **`exit`**

Appendix A. 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 A-1 lists the packet sizes with defaults.

Table A-1. Network-Specific Packet Size Limits

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
Serial Line	2046*	2	0

* Default

Note: You can configure the maximum packet sizes for Token-Ring 4Mb and Token-Ring 16Mb using the token-ring configuration (`TKR Config>`) process.

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 acknowledgement

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

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

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

DDLC dual data-link controller

DDN Defense Data Network

DDP Datagram Delivery Protocol

DDT Dynamic Debugging Tool

DHCP Dynamic Host Configuration Protocol

dir directly connected

DL data link

DLC data link control

DLCI data link connection identifier

DLS data link switching

DLSw data link switching

DMA direct memory access

DNA Digital Network Architecture

DNCP DECnet Protocol Control Protocol

DNIC Data Network Identifier Code

DoD Department of Defense

DOS Disk Operating System

DR designated router

DRAM Dynamic Random Access Memory

DSAP destination service access point

DSE data switching equipment

DSE data switching exchange

DSR data set ready

DSU data service unit

DTE data terminal equipment

DTR data terminal ready

Dtype destination type

DVMRP Distance Vector Multicast Routing Protocol

E1 2.048 Mbps transmission rate

EDEL end delimiter

EDI error detected indicator

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

ELAP EtherTalk Link Access Protocol

ELS Event Logging System

EST Eastern Standard Time

Eth Ethernet

fa-ga functional address-group address

FCS frame check sequence

FECN forward explicit congestion notification

FIFO first in, first out

FLT filter library

FR Frame Relay

FRL Frame Relay

FTP File Transfer Protocol

GMT Greenwich Mean Time

GOSIP Government Open Systems Interconnection Profile

GTE General Telephone Company

GWCON Gateway Console

HDLC high-level data link control

HEX hexadecimal

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

LCP Link Control Protocol

LED light-emitting diode

LF largest frame; line feed

LLC logical link control

LLC2 logical link control 2

LMI local management interface

LRM LAN reporting mechanism

LS link state

LSA link state advertisement

LSB least significant bit

LSreq link state request

LSrxl link state retransmission list

LU logical unit

MAC medium access control

Mb megabit

MB megabyte

Mbps megabits per second

MBps megabytes per second

MC multicast

MCF MAC filtering

MIB Management Information Base

MIB II Management Information Base II

MILNET military network

MOS Micro Operating System

MOSDDT Micro Operating System Dynamic Debugging Tool

MOSPF Open Shortest Path First with multicast extensions

MSB most significant bit

MSDU MAC service data unit

MTU maximum transmission unit

nak not acknowledged

NBP Name Binding Protocol

NBR neighbor

NCP Network Control Protocol

NCP Network Core Protocol

NetBIOS Network Basic Input/Output System

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 non-volatile configuration

OPCON Operator Console

OSI open systems interconnection

OSICP OSI Control Protocol

OSPF Open Shortest Path First

OUI organization unique identifier

PC personal computer

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

SAF source address filtering

SAP service access point

SAP Service Advertising Protocol

sdel start delimiter

SDLC SDLC relay, synchronous data link control

seqno sequence number

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

VINES VIrtual NEtworking System

VIR variable information rate

VL virtual link

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

AAL. ATM Adaptation Layer, the layer that adapts user data to/from the ATM network by adding/removing headers and segmenting/reassembling the data into/from cells.

AAL-5. ATM Adaptation Layer 5, one of several standard AALs. AAL-5 was designed for data communications, and is used by LAN Emulation and Classical IP.

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also *abstract syntax notation 1 (ASN.1)* and *basic encoding rules (BER)*.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in the following standards:

- ITU-T Recommendation X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1994

See also *basic encoding rules (BER)*.

ACCESS. In the Simple Network Management Protocol (SNMP), the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active monitor. In a token-ring network, a function performed at any one time by one ring station that initiates the transmission of tokens and provides token error recovery facilities. Any active adapter on the ring has the ability to provide the active monitor function if the current active monitor fails.

address. In data communication, the unique code assigned to each device, workstation, or user connected to a network.

address mapping table (AMT). A table, maintained within the AppleTalk router, that provides a current mapping of node addresses to hardware addresses.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with *subnet mask* and *subnetwork mask*.

address resolution. (1) A method for mapping network-layer addresses to media-specific addresses. (2) See also *Address Resolution Protocol (ARP)* and *AppleTalk Address Resolution Protocol (AARP)*.

Address Resolution Protocol (ARP). (1) In the Internet suite of protocols, the protocol that dynamically maps an IP address to an address used by a supporting metropolitan or local area network such as Ethernet or token-ring. (2) See also *Reverse Address Resolution Protocol (RARP)*.

addressing. In data communication, the way in which a station selects the station to which it is to send data.

adjacent nodes. Two nodes connected together by at least one path that connects no other node. (T)

Administrative Domain. A collection of hosts and routers, and the interconnecting networks, managed by a single administrative authority.

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) end node. A node that provides a broad range of end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to a subarea network as a peripheral node or to other end nodes.

Advanced Peer-to-Peer Networking (APPN) network. A collection of interconnected network nodes and their client end nodes.

Advanced Peer-to-Peer Networking (APPN) network node. A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

Advanced Peer-to-Peer Networking (APPN) node. An APPN network node or an APPN end node.

alert. A message sent to a management services focal point in a network to identify a problem or an impending problem.

all-stations address. In communications, synonym for *broadcast address*.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

analog. (1) Pertaining to data consisting of continuously variable physical quantities. (A) (2) Contrast with *digital*.

AppleTalk. A network protocol developed by Apple Computer, Inc. This protocol is used to interconnect network devices, which can be a mixture of Apple and non-Apple products.

AppleTalk Address Resolution Protocol (AARP). In AppleTalk networks, a protocol that (a) translates AppleTalk node addresses into hardware addresses and (b) reconciles addressing discrepancies in networks that support more than one set of protocols.

AppleTalk Transaction Protocol (ATP). In AppleTalk networks, a protocol that provides client/server request and response functions for hosts accessing the Zone Information Protocol (ZIP) for zone information.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network*.

APPN network node. See *Advanced Peer-to-Peer Networking (APPN) network node*.

arbitrary MAC addressing (AMA). In DECnet architecture, an addressing scheme used by DECnet

Phase IV-Prime that supports universally administered addresses and locally administered addresses.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

asynchronous (ASYNC). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

ATM. Asynchonous Transfer Mode, a connection-oriented, high-speed networking technology based on cell switching.

ATMARP. ARP in Classical IP.

attachment unit interface (AUI). In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (I) (A)

authentication failure. In the Simple Network Management Protocol (SNMP), a trap that may be generated by an authentication entity when a requesting client is not a member of the SNMP community.

autonomous system. In TCP/IP, a group of networks and routers under one administrative authority. These networks and routers cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. In TCP/IP, a number assigned to an autonomous system by the same central authority that also assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

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)

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) A functional unit, controlled by the processor, that handles the transfer of data between processor storage and local peripheral equipment.

channel service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal's performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loopback testing, which includes the transmission of test signals between the CSU and the network carrier's office channel unit. See also *data service unit (DSU)*.

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with *line switching*.

class A network. In Internet communications, a network in which the high-order (most significant) bit of the IP address is set to 0 and the host ID occupies the three low-order octets.

class B network. In Internet communications, a network in which the two high-order (most significant and next-to-most significant) bits of the IP address are set to 1 and 0, respectively, and the host ID occupies the two low-order octets.

class of service (COS). A set of characteristics (such as route security, transmission priority, and bandwidth) used to construct a route between session partners. The class of service is derived from a mode name specified by the initiator of a session.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

clocking. (1) In binary synchronous communication, the use of clock pulses to control synchronization of data and control characters. (2) A method of controlling the number of data bits sent on a telecommunication line in a given time.

collision. An unwanted condition that results from concurrent transmissions on a channel. (T)

collision detection. In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

Committed information rate. The maximum amount of data in bits that the network agrees to deliver.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

compression. (1) The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. (2) Any encoding to reduce the number of bits used to represent a given message or record.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

configuration file. A file that specifies the characteristics of a system device or network.

configuration parameter. A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

configuration report server (CRS). In the IBM Token-Ring Network Bridge Program, the server that accepts commands from the LAN Network Manager (LNM) to get station information, set station parameters, and remove stations on its ring. This server also collects and forwards configuration reports generated by stations on its ring. The configuration reports include the new active monitor reports and the nearest active upstream neighbor (NAUN) reports.

congestion. See *network congestion*.

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

control point management services (CPMS). A component of a control point, consisting of management services function sets, that provides facilities to assist in performing problem management, performance and accounting management, change management, and configuration management. Capabilities provided by the CPMS include sending requests to physical unit management services (PUMS) to test system resources, collecting statistical information (for example, error and performance data) from PUMS about the system resources, and analyzing and presenting test results and statistical information collected about the system resources. Analysis and presentation responsibilities for problem determination and performance monitoring can be distributed among multiple CPMSs.

control point management services unit (CP-MSU). The message unit that contains management services data and flows between management services function sets. This message unit is in general data stream (GDS) format. See also *management services unit (MSU)* and *network management vector transport (NMVT)*.

D

D-bit. Delivery-confirmation bit. In X.25 communications, the bit in a data packet or call-request packet that is set to 1 if end-to-end acknowledgment (delivery confirmation) is required from the recipient.

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

data carrier detect (DCD). Synonym for *received line signal detector (RLSD)*.

data circuit. (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (I) (2) In SNA, synonym for *link connection*. (3) See also *physical circuit* and *virtual circuit*.

Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.
2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal

conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	in-channel signaling
1–15	reserved
16–991	assigned using frame-relay connection procedures
992–1007	layer 2 management of frame-relay bearer service
1008–1022	reserved
1023	in-channel layer management

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link layer. In the Open Systems Interconnection reference model, the layer that provides services to transfer data between entities in the network layer over a communication link. The data link layer detects and possibly corrects errors that may occur in the physical layer. (T)

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. See also *packet level* and *physical level*. (2) In X.25 communications, synonym for *frame level*.

data link switching (DLSw). A method of transporting network protocols that use IEEE 802.2 logical link control (LLC) type 2. SNA and NetBIOS are examples of protocols that use LLC type 2. See also *encapsulation* and *spoofing*.

data packet. In X.25 communications, a packet used for the transmission of user data on a virtual circuit at the DTE/DCE interface.

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

data set ready (DSR). Synonym for *DCE ready*.

data switching exchange (DSE). The equipment installed at a single location to provide switching functions, such as circuit switching, message switching, and packet switching. (I)

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (I)

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.
2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (I) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram consists of an IP header followed by the transport layer data. (3) See also *packet* and *segment*.

Datagram Delivery Protocol (DDP). In AppleTalk networks, a protocol that provides network connectivity

by means of connectionless socket-to-socket delivery service on the internet layer.

DCE ready. In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that the local data circuit-terminating equipment (DCE) is connected to the communication channel and is ready to send data. Synonymous with *data set ready (DSR)*.

DECnet. A network architecture that defines the operation of a family of software modules, databases, and hardware components typically used to tie Digital Equipment Corporation systems together for resource sharing, distributed computation, or remote system configuration. DECnet network implementations follow the Digital Network Architecture (DNA) model.

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

designated router. A router that informs end nodes of the existence and identity of other routers. The selection of the designated router is based upon the router with the highest priority. When several routers share the highest priority, the router with the highest station address is selected.

destination node. The node to which a request or data is sent.

destination port. The 8-port asynchronous adapter that serves as a connection point with a serial service.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. Contrast with *source service access point (SSAP)*.

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

digital. (1) Pertaining to data that consist of digits. (T) (2) Pertaining to data in the form of digits. (A) (3) Contrast with *analog*.

Digital Network Architecture (DNA). The model for all DECnet hardware and software implementations.

direct memory access (DMA). The system facility that allows a device on the Micro Channel bus to get direct access to the system or bus memory without the intervention of the system processor.

directory. A table of identifiers and references to the corresponding items of data. (I) (A)

directory service (DS). An application service element that translates the symbolic names used by application processes into the complete network addresses used in an OSI environment. (T)

directory services (DS). A control point component of an APPN node that maintains knowledge of the location of network resources.

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies. (3) See *Administrative Domain* and *domain name*.

domain name. In the Internet suite of protocols, a name of a host system. A domain name consists of a sequence of subnames separated by a delimiter character. For example, if the fully qualified domain name (FQDN) of a host system is `ralvm7.vnet.ibm.com`, each of the following is a domain name:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

domain name server. In the Internet suite of protocols, a server program that supplies name-to-address translation by mapping domain names to IP addresses. Synonymous with *name server*.

Domain Name System (DNS). In the Internet suite of protocols, the distributed database system used to map domain names to IP addresses.

dotted decimal notation. The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent IP addresses.

dump. (1) Data that has been dumped. (T) (2) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

dynamic reconfiguration (DR). The process of changing the network configuration (peripheral PUs and LUs) without regenerating complete configuration tables or deactivating the affected major node.

Dynamic Routing. Routing using learned routes rather than routes statically configured at initialization.

E

echo. In data communication, a reflected signal on a communications channel. For example, on a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

EIA 232. In data communication, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

encapsulation. (1) In communications, a technique used by layered protocols by which a layer adds control information to the protocol data unit (PDU) from the layer it supports. In this respect, the layer encapsulates the data from the supported layer. In the Internet suite of protocols, for example, a packet would contain control information from the physical layer, followed by control information from the network layer, followed by the application protocol data. (2) See also *data link switching*.

encode. To convert data by the use of a code in such a manner that reconversion to the original form is possible. (T)

end node (EN). (1) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node*. (2) In communications, a node that is frequently attached to a single data link and cannot perform intermediate routing functions.

entry point (EP). In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

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

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

flow control. (1) In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the rate of flow of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units. (2) See also *pacing*.

fragment. See *fragmentation*.

fragmentation. (1) The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted. (2) See also *segmenting*.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures.

frame level. Synonymous with *data link level*. See *link level*.

frame relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols. (3) In TCP/IP, synonym for *router*.

general data stream (GDS). The data stream used for conversations in LU 6.2 sessions.

general data stream (GDS) variable. A type of RU substructure that is preceded by an identifier and a length field and includes either application data, user control data, or SNA-defined control data.

H

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

heap memory. The amount of RAM used to dynamically allocate data structures.

Hello. A protocol used by a group of cooperating, trusting routers to allow them to discover minimal delay routes.

hello message. (1) A message sent periodically to establish and test reachability between routers or between routers and hosts. (2) In the Internet suite of protocols, a message defined by the Hello protocol as an Interior Gateway Protocol (IGP).

heuristic. Pertaining to exploratory methods of problem solving in which solutions are discovered by evaluation of the progress made toward the final result.

high-level data link control (HDLC). In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

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.

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 services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data.

Note: ISDNs are used in public and private network architectures.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interior gateway. In Internet communications, a gateway that communicates only with its own autonomous system. Contrast with *exterior gateway*.

Interior Gateway Protocol (IGP). In the Internet suite of protocols, a protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

intermediate node. A node that is at the end of more than one branch. (T)

intermediate session routing (ISR). A type of routing function within an APPN network node that provides session-level flow control and outage reporting for all sessions that pass through the node but whose end points are elsewhere.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

International Telecommunication Union (ITU). The specialized telecommunication agency of the United Nations, established to provide standardized communication procedures and practices, including frequency allocation and radio regulations worldwide.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Architecture Board (IAB). The technical body that oversees the development of the Internet suite of protocols that are known as TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Control Protocol (ICP). The VIrtual NEtworking System (VINES) protocol that provides exception notifications, metric notifications, and PING support. See also *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

Internetwork Packet Exchange (IPX). (1) The network protocol used to connect Novell's servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology. (2) See also *Xerox Network Systems (XNS)*.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units. (T)

intra-area routing. In Internet communications, the routing of data within an area.

Inverse Address Resolution Protocol (InARP). In the Internet suite of protocols, the protocol used for locating a protocol address through the known hardware

address. In a frame-relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comments (RFC) 791. It is usually represented in dotted decimal notation.

IP datagram. In the Internet suite of protocols, the fundamental unit of information transmitted through an internet. It contains source and destination addresses, user data, and control information such as the length of the datagram, the header checksum, and flags indicating whether the datagram can be or has been fragmented.

IP router. A device in an IP internet that is responsible for making decisions about the paths over which network traffic will flow. Routing protocols are used to gain information about the network and to determine the best route over which the datagram should be forwarded toward the final destination. The datagrams are routed based on IP destination addresses.

IPXWAN. A Novell protocol that is used to exchange router-to-router information before exchanging standard Internetwork Packet Exchange (IPX) routing information and traffic over wide area networks (WANs).

L

LAN bridge server (LBS). In the IBM Token-Ring Network Bridge Program, the server that keeps statistical information about frames forwarded between two or more rings (through a bridge). The LBS sends these statistics to the appropriate LAN managers through the LAN reporting mechanism (LRM).

LAN Emulation (LE). An ATM Forum standard that supports legacy LAN applications over ATM networks.

LAN Emulation Client (LEC). A LAN Emulation component that represents users of the Emulated LAN.

LAN Emulation Configuration Server (LECS). A LAN Emulation Service component that centralizes and disseminates configuration data.

LAN Emulation Server (LES). A LAN Emulation Service component that resolves LAN Destinations to ATM Addresses.

LAN Network Manager (LNM). An IBM licensed program that enables a user to manage and monitor LAN resources from a central workstation.

LAN segment. (1) Any portion of a LAN (for example, a bus or ring) that can operate independently, but that is connected to other parts of the network by means of bridges. (2) A ring or bus network without bridges.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture. (T) (2) In the Open Systems Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols, that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions in other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

LE. LAN Emulation. An ATM Forum standard that supports legacy LAN applications over ATM networks.

LEC. LAN Emulation Client. A LAN Emulation component that represents users of the Emulated LAN.

LECS. LAN Emulation Configuration Server. A LAN Emulation Service component that centralizes and disseminates configuration data.

LES. LAN Emulation Server. A LAN Emulation Service component that resolves LAN Destinations to ATM Addresses.

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 object. Synonym for *MIB variable*.

MIB variable. In the Simple Network Management Protocol (SNMP), a specific instance of data defined in a MIB module. Synonymous with *MIB object*.

MIB view. In the Simple Network Management Protocol (SNMP), the collection of managed objects, known to the agent, that is visible to a particular community.

MILNET. The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

modulo. (1) Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. (2) See also *modulus*.

modulus. A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 (9 - 4 = 5; 4 - 9 = -5; and 5 divides both 5 and -5 without leaving a remainder).

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

multicast. (1) Transmission of the same data to a selected group of destinations. (T) (2) A special form of broadcast in which copies of a packet are delivered to only a subset of all possible destinations.

multiple-domain support (MDS). A technique for transporting management services data between management services function sets over LU-LU and CP-CP sessions. See also *multiple-domain support message unit (MDS-MU)*.

multiple-domain support message unit (MDS-MU). The message unit that contains management services data and flows between management services function sets over the LU-LU and CP-CP sessions used by multiple-domain support. This message unit, as well as the actual management services data that it contains, is in general data stream (GDS) format. See also *control point management services unit (CP-MSU)*, *management services unit (MSU)*, and *network management vector transport (NMVT)*.

N

Name Binding Protocol (NBP). In AppleTalk networks, a protocol that provides name translation function from the AppleTalk entity (resource) name (character string) into an AppleTalk IP address (16-bit number) on the transport layer.

name resolution. In Internet communications, the process of mapping a machine name to the corresponding Internet Protocol (IP) address. See also *Domain Name System (DNS)*.

name server. In the Internet suite of protocols, synonym for *domain name server*.

nearest active upstream neighbor (NAUN). In the IBM Token-Ring Network, the station sending data directly to a given station on the ring.

neighbor. A router on a common subnetwork that has been designated by a network administrator to receive routing information.

NetBIOS. Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) A group of nodes and the links interconnecting them.

network accessible unit (NAU). A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the destination of information transmitted by the path control network. Synonymous with *network addressable unit*.

network address. According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU). Synonym for *network accessible unit*.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion. An undesirable overload condition caused by traffic in excess of what a network can handle.

network identifier. (1) In TCP/IP, that part of the IP address that defines a network. The length of the network ID depends on the type of network class (A, B, or C). (2) A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

Network Information Center (NIC). In Internet communications, local, regional, and national groups throughout the world who provide assistance, documentation, training, and other services to users.

network layer. In Open Systems Interconnection (OSI) architecture, the layer that is responsible for routing, switching, and link-layer access across the OSI environment.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management station. In the Simple Network Management Protocol (SNMP), a station that executes management application programs that monitor and control network elements.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network node (NN). See *Advanced Peer-to-Peer Networking (APPN) network node*.

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*.

nonseed router. In AppleTalk networks, a router that acquires network number range and zone list information from a seed router attached to the same network.

O

Open Shortest Path First (OSPF). In the Internet suite of protocols, a function that provides intradomain information transfer. An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

Open Systems Interconnection (OSI). (1) The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) (2) The use of standardized procedures to enable the interconnection of data processing systems.

Note: OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

Open Systems Interconnection (OSI) architecture. Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

Open Systems Interconnection (OSI) reference model. A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

origin. An external logical unit (LU) or application program from which a message or other data originates. See also *destination*.

orphan circuit. A non-configured circuit whose availability is learned dynamically.

P

pacing. (1) A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. (2) See also *flow control*, *receive pacing*, *send pacing*, *session-level pacing*, and *virtual route (VR) pacing*.

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet mode operation. Synonym for *packet switching*.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with *packet mode operation*. See also *circuit switching*.

parallel bridges. A pair of bridges connected to the same LAN segment, creating redundant paths to the segment.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also *explicit route (ER)*, *route extension*, and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units

(PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path cost. In link-state routing protocols, the sum of the link costs along the path between two nodes or networks.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment.

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with *global character* and *wildcard character*.

permanent virtual circuit (PVC). In X.25 and frame-relay communications, a virtual circuit that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with *switched virtual circuit (SVC)*.

physical circuit. A circuit established without multiplexing. See also *data circuit*. Contrast with *virtual circuit*.

physical layer. In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain, and release physical connections over the transmission medium. (T)

physical unit (PU). (1) The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. (2) See also *peripheral PU* and *subarea PU*.

ping command. The command that sends an Internet Control Message Protocol (ICMP) echo-request packet to a gateway, router, or host with the expectation of receiving a reply.

Point-to-Point Protocol (PPP). A protocol that provides a method for encapsulating and transmitting packets over serial point-to-point links.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (6) Synonymous with *socket*.

port number. In Internet communications, the identification of an application entity to the transport service.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with *line control discipline* and *line discipline*. See *bracket protocol* and *link protocol*.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

R

Rapid Transport Protocol (RTP) connection. In high-performance routing (HPR), the connection established between the endpoints of the route to transport session traffic.

reachability. The ability of a node or a resource to communicate with another node or resource.

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

reassembly. In communications, the process of putting segmented packets back together after they have been received.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See *RNR packet*.

received line signal detector (RLSD). In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE). Synonymous with *carrier detect* and *data carrier detect (DCD)*.

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Synonym for *link-attached*. (3) Contrast with *local*.

remote bridging. The function of a bridge that allows two bridges to connect multiple LANs using a telecommunication link. Contrast with *local bridging*.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any host in the network. The local host receives the results of the command execution.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

reset request packet. In X.25 communications, a packet transmitted by the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE) to request that a virtual call or a permanent virtual circuit be reset. The reason for the request can also be specified in the packet.

ring. See *ring network*.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

ring segment. A section of a ring that can be isolated (by unplugging connectors) from the rest of the ring. See *LAN segment*.

rlogin (remote login). A service, offered by Berkeley UNIX-based systems, that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes information about the user's environment (for example, terminal type) to the remote machine.

RNR packet. A packet used by a data terminal equipment (DTE) or by a data circuit-terminating equipment (DCE) to indicate a temporary inability to accept additional packets for a virtual call or permanent virtual circuit.

root bridge. The bridge that is the root of a spanning tree formed between other active bridges in the bridging network. The root bridge originates and transmits bridge protocol data units (BPDUs) to other active bridges to maintain the spanning tree topology. It is the bridge with the highest priority in the network.

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunication link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

Route Selection control vector (RSCV). A control vector that describes a route within an APPN network. The RSCV consists of an ordered sequence of control vectors that identify the TGs and nodes that make up the path from an origin node to a destination node.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. (3) In OSI terminology, a function that determines a path by which an entity can be reached. (4) In TCP/IP, synonymous with *gateway*. (5) Contrast with *bridge*.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing domain. In Internet communications, a group of intermediate systems that use a routing protocol so that the representation of the overall network is the same within each intermediate system. Routing domains are connected to each other by exterior links.

Routing Information Protocol (RIP). In the Internet suite of protocols, an interior gateway protocol used to exchange intradomain routing information and to determine optimum routes between internet hosts. RIP determines optimum routes on the basis of route metrics, not link transmission speed.

routing loop. A situation that occurs when routers circulate information among themselves until convergence occurs or until the networks involved are considered unreachable.

routing protocol. A technique used by a router to find other routers and to remain up to date about the best way to get to reachable networks.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). In AppleTalk networks, a protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

RouTing update Protocol (RTP). The VIrtual NEtworking System (VINES) protocol that maintains the routing database and allows the exchange of routing information between VINES nodes. See also *Internet Control Protocol (ICP)*.

rsh. A variant of the rlogin command that invokes a command interpreter on a remote UNIX machine and passes the command-line arguments to the command interpreter, skipping the login step completely.

S

seed router. In AppleTalk networks, a router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed router must be initially set up using the configurator tool. Contrast with *nonseed router*.

segment. (1) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

segmenting. In OSI, a function performed by a layer to map one protocol data unit (PDU) from the layer it supports into multiple PDUs.

sequence number. In communications, a number assigned to a particular frame or packet to control the transmission flow and receipt of data.

server. A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

Service Advertising Protocol (SAP). In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and 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. An endpoint for communication between processes or application programs.

source route bridging. In LANs, a bridging method that uses the routing information field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The routing information field is inserted into the MAC header by the source node. The information in the routing information field is derived from explorer packets generated by the source host.

source routing. In LANs, a method by which the sending station determines the route the frame will follow and includes the routing information with the frame. Bridges then read the routing information to determine whether they should forward the frame.

source service access point (SSAP). In SNA and TCP/IP, a logical address that allows a system to send data to a remote device from the appropriate communications support. Contrast with *destination service access point (DSAP)*.

spanning tree. In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topology to ensure that there is only one route between any two LANs in the bridged network. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

sphere of control (SOC). The set of control point domains served by a single management services focal point.

sphere of control (SOC) node. A node directly in the sphere of control of a focal point. A SOC node has exchanged management services capabilities with its focal point. An APPN end node can be a SOC node if it supports the function to exchange management services capabilities.

split horizon. A technique for minimizing the time to achieve network convergence. A router records the interface over which it received a particular route and does not propagate its information about the route back over the same interface.

spoofing. For data links, a technique in which a protocol initiated from an end station is acknowledged and processed by an intermediate node on behalf of the final destination. In IBM 6611 data link switching, for example, SNA frames are encapsulated into TCP/IP packets for transport across a non-SNA wide area network, unpacked by another IBM 6611, and passed to the final destination. A benefit of spoofing is the prevention of end-to-end session timeouts.

standard MIB. In the Simple Network Management Protocol (SNMP), a MIB module that is located under the management branch of the Structure of Management Information (SMI) and that is considered a standard by the Internet Engineering Task Force (IETF).

static route. The route between hosts, networks, or both that is manually entered into a routing table.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

StreetTalk. In the VIrtual NEtworking System (VINES), a unique network-wide naming and addressing system that allows users to locate and access any resource on the network without knowing the network topology. See also *Internet Control Protocol (ICP)* and *RouTing update Protocol (RTP)*.

Structure of Management Information (SMI). (1) In the Simple Network Management Protocol (SNMP), the rules used to define the objects that can be accessed by means of a network management protocol. (2) In OSI, the set of standards relating to management information. The set includes the *Management Information Model* and the *Guidelines for the Definition of Managed Objects*.

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for *subnetwork*.

subnet address. In Internet communications, an extension to the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use `$AA` as their service access point (SAP) value.

subnetwork 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)*.

SYNTAX. In the Simple Network Management Protocol (SNMP), a clause in the MIB module that defines the abstract data structure that corresponds to a managed object.

system configuration. A process that specifies the devices and programs that form a particular data processing system.

system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for users of the network. Multiple SSCPs, cooperating as peers with one another, can divide the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a “threshold exceeded” occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

throughput class. In packet switching, the speed at which data terminal equipment (DTE) packets travel through the packet switching network.

time to live (TTL). A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

topology database update (TDU). A message about a new or changed link or node that is broadcast among APPN network nodes to maintain the network topology database, which is fully replicated in each network node. A TDU contains information that identifies the following:

- The sending node
- The node and link characteristics of various resources in the network
- The sequence number of the most recent update for each of the resources described.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

transceiver (transmitter-receiver). In LANs, a physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and that sense collisions.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission group (TG). (1) A connection between adjacent nodes that is identified by a transmission group number. (2) In a subarea network, a single link or a group of links between adjacent nodes. When a transmission group consists of a group of links, the links are viewed as a single logical link, and the transmission group is called a *multilink transmission group (MLTG)*. A *mixed-media multilink transmission group (MMMLTG)* is one that contains links of different medium types (for example, token-ring, switched SDLC, nonswitched SDLC, and frame-relay links). (3) In an APPN network, a single link between adjacent nodes. (4) See also *parallel transmission groups*.

transmission header (TH). Control information, optionally followed by a basic information unit (BIU) or a BIU segment, that is created and used by path control to route message units and to control their flow within the network. See also *path information unit*.

transparent bridging. In LANs, a method for tying individual local area networks together through the medium access control (MAC) level. A transparent bridge stores the tables that contain MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

transport layer. In the Open Systems Interconnection reference model, the layer that provides a reliable end-to-end data transfer service. There may be relay open systems in the path. (T) See also *Open Systems Interconnection reference model*.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

tunneling. To treat a transport network as though it were a single communication link or LAN. See also *encapsulation*.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The European version (E1) transmits 2.048 Mbps.

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.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.

VINES. VIrtual NEtworking System.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit*. Contrast with *physical circuit*. (2) A logical connection established between two DTEs.

virtual link. In Open Shortest Path First (OSPF), a point-to-point interface that connects border routers that are separated by a non-backbone transit area. Because area routers are part of the OSPF backbone, the virtual link connects the backbone. The virtual links ensure that the OSPF backbone does not become discontinuous.

VIrtual 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

Special Characters

A

B

C

D

E

F

H

I

J

P

R

S

T

U

V

W

Tell Us What You Think!

Nways Multiprotocol Access Services
Protocol Configuration and Monitoring Reference Volume 2
Version 1 Release 1

Publication No. SC30-3885-00

We hope you find this publication useful, readable, and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form. If you are in the U.S.A., you can mail this form postage free or fax it to us at 1-800-253-3520. Elsewhere, your local IBM branch office or representative will forward your comments or you may mail them directly to us.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

Specific comments or problems:

Please tell us how we can improve this book:

Thank you for your comments. If you would like a reply, provide the necessary information below.

Name

Address

Company or Organization

Phone No.

Tell Us What You Think!
SC30-3885-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Design & Information Development
Dept. CGF/Bldg. 656
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

SC30-3885-00

Cut or Fold
Along Line

Part Number: 85H7920

Printed in U.S.A.