Cisco IOS DECnet Configuration Guide

Cisco IOS Release 15.0S

About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is i ntended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the **^** symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
		A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x	y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x	y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y	z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
Courier font	Courier font is used for information that is displayed on a PC or terminal screen.
Bold Courier font	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:

Caution   Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note   Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Timesaver   Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- Cisco IOS Documentation Set, page iv
- Cisco IOS Documentation on Cisco.com, page iv
- Configuration Guides, Command References, and Supplementary Resources, page v

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.

- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.

  - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.

  - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.

- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.

- Command reference book for **debug** commands. Command pages are listed in alphabetical order.

- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/all_release/all_mcl.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xi.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

Table 1   Cisco IOS and Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS AppleTalk Configuration Guide	AppleTalk protocol.
Cisco IOS XE AppleTalk Configuration Guide	
Cisco IOS AppleTalk Command Reference	
Cisco IOS Asynchronous Transfer Mode Configuration Guide	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
Cisco IOS Asynchronous Transfer Mode Command Reference	

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Bridging and IBM Networking Configuration Guide *Cisco IOS Bridging Command Reference* *Cisco IOS IBM Networking Command Reference*	• Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). • Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
Cisco IOS Broadband and DSL Configuration Guide *Cisco IOS XE Broadband and DSL Configuration Guide* *Cisco IOS Broadband and DSL Command Reference*	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
Cisco IOS Carrier Ethernet Configuration Guide *Cisco IOS Carrier Ethernet Command Reference*	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
Cisco IOS Configuration Fundamentals Configuration Guide *Cisco IOS XE Configuration Fundamentals Configuration Guide* *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
Cisco IOS DECnet Configuration Guide *Cisco IOS XE DECnet Configuration Guide* *Cisco IOS DECnet Command Reference*	DECnet protocol.
Cisco IOS Dial Technologies Configuration Guide *Cisco IOS XE Dial Technologies Configuration Guide* *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
Cisco IOS Flexible NetFlow Configuration Guide *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.

Table 1   *Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)*

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS H.323 Configuration Guide	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
Cisco IOS High Availability Configuration Guide *Cisco IOS XE High Availability Configuration Guide* *Cisco IOS High Availability Command Reference*	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
Cisco IOS Integrated Session Border Controller Command Reference	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
Cisco IOS Intelligent Service Gateway Configuration Guide *Cisco IOS Intelligent Service Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
Cisco IOS Interface and Hardware Component Configuration Guide *Cisco IOS XE Interface and Hardware Component Configuration Guide* *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
Cisco IOS IP Addressing Services Configuration Guide *Cisco IOS XE Addressing Services Configuration Guide* *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
Cisco IOS IP Application Services Configuration Guide *Cisco IOS XE IP Application Services Configuration Guide* *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
Cisco IOS IP Mobility Configuration Guide *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
Cisco IOS IP Multicast Configuration Guide *Cisco IOS XE IP Multicast Configuration Guide* *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

Table 1   Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS IP Routing Protocols Configuration Guide *Cisco IOS XE IP Routing Protocols Configuration Guide* *Cisco IOS IP Routing Protocols Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
Cisco IOS IP SLAs Configuration Guide *Cisco IOS XE IP SLAs Configuration Guide* *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
Cisco IOS IP Switching Configuration Guide *Cisco IOS XE IP Switching Configuration Guide* *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
Cisco IOS IPv6 Configuration Guide *Cisco IOS XE IPv6 Configuration Guide* *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
Cisco IOS ISO CLNS Configuration Guide *Cisco IOS XE ISO CLNS Configuration Guide* *Cisco IOS ISO CLNS Command Reference*	ISO connectionless network service (CLNS).
Cisco IOS LAN Switching Configuration Guide *Cisco IOS XE LAN Switching Configuration Guide* *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
Cisco IOS Mobile Wireless Home Agent Configuration Guide *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.

Table 1   Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Multiprotocol Label Switching Configuration Guide *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
Cisco IOS Multi-Topology Routing Configuration Guide *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
Cisco IOS NetFlow Configuration Guide *Cisco IOS XE NetFlow Configuration Guide* *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, export features.
Cisco IOS Network Management Configuration Guide *Cisco IOS XE Network Management Configuration Guide* *Cisco IOS Network Management Command Reference*	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
Cisco IOS Novell IPX Configuration Guide *Cisco IOS XE Novell IPX Configuration Guide* *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.
Cisco IOS Optimized Edge Routing Configuration Guide *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
Cisco IOS Quality of Service Solutions Configuration Guide *Cisco IOS XE Quality of Service Solutions Configuration Guide* *Cisco IOS Quality of Service Solutions Command Reference*	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
Cisco IOS Security Configuration Guide *Cisco IOS XE Security Configuration Guide* *Cisco IOS Security Command Reference*	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Service Selection Gateway Configuration Guide *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.
Cisco IOS Software Activation Configuration Guide *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
Cisco IOS Software Modularity Installation and Configuration Guide *Cisco IOS Software Modularity Command Reference*	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
Cisco IOS Terminal Services Configuration Guide *Cisco IOS Terminal Services Command Reference* *Cisco IOS XE Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
Cisco IOS Virtual Switch Command Reference	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). **Note** For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
Cisco IOS Voice Configuration Library *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
Cisco IOS VPDN Configuration Guide *Cisco IOS XE VPDN Configuration Guide* *Cisco IOS VPDN Command Reference*	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
Cisco IOS Wide-Area Networking Configuration Guide *Cisco IOS XE Wide-Area Networking Configuration Guide* *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
Cisco IOS Wireless LAN Configuration Guide *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2   Cisco IOS Supplementary Documents and Resources

Document Title	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS Software System Messages	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2008 Cisco Systems, Inc. All rights reserved.

Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last updated: August 6, 2008

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS and Cisco IOS XE Software Documentation" document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.

- Change the behavior of the port; for example, by adding a password or changing the timeout value.

✎

Note   The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 1 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1   CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1   CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on the Cisco ASR1000 series router)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias             set and display aliases command
boot              boot up an external process
confreg           configuration register utility
cont              continue executing a downloaded image
context           display the context of a loaded image
cookie            display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

Note   A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes how to use the Help feature.

Table 2   CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the help feature in any command mode.
?	Lists all commands available for a particular command mode.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'.  If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable      Create a temporary access-List entry
  access-profile     Apply user-profile to interface
  access-template    Create a temporary access-List entry
  alps               ALPS exec commands
  archive            manage archive files
<snip>
```

***partial command*?**

```
Router(config)# zo?
zone  zone-pair
```

***partial command*<Tab>**

```
Router(config)# we<Tab> webvpn
```

***command* ?**

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

***command keyword* ?**

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

Table 3   CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name
Router(config)# ethernet cfm domain dname ?
  level
Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
  <cr>
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, "two words" is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

> ✎
>
> **Note** The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

  The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4   Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

⚠
Caution   Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression "protocol."

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

Table 5   Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at "^" marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- *Cisco IOS Release 12.2SR System Message Guide*

- *Cisco IOS System Messages, Volume 1 of 2* (Cisco IOS Release 12.4)

- *Cisco IOS System Messages, Volume 2 of 2* (Cisco IOS Release 12.4)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

  or

  "Using Cisco IOS XE Software" chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html

- Cisco Product Support Resources

  http://www.cisco.com/web/psa/products/index.html

- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html

- *White Paper: Cisco IOS Reference Guide*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml

- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)

  http://www.cisco.com/kobayashi/sw-center/

- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl\

DECnet Overview

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Cisco IOS software supports a variety of network protocols. The *Cisco IOS DECnet Configuration Guide* discusses the following network protocol:

- DECnet

The *Cisco IOS IP Configuration Guide* discusses the following network protocols:

- IP
- IP Routing

This overview chapter provides a high-level description of DECnet. For configuration information, see the appropriate section in this publication.

DECnet

Digital Equipment Corporation designed the DECnet stack of protocols in the 1970s as part of its Digital Network Architecture (DNA). DNA supports DECnet routing over Ethernet, Token Ring, FDDI, HDLC, PPP, Frame Relay, Switched Multimegabit Data Service (SMDS), X.25, and IEEE 802.2.

DECnet supports both connectionless and connection-oriented network layers implemented by Open System Interconnection (OSI) protocols. The most recent product release of DECnet is called Phase V, which is equivalent to International Organization for Standardization (ISO) Connectionless Network Service (CLNS). Phase V is compatible with the previous release, Phase IV. Phase IV was similar to OSI routing, but Phase V implements full OSI routing, including support for End System-to-Intermediate System (ES-IS) and Intermediate System-to-Intermediate System (IS-IS) connections. An end system (ES) is a nonrouting network node; an intermediate system (IS) refers to a router. ES-IS support allows ESs and ISs to discover each other. IS-IS provides routing between ISs only.

DECnet Phase IV Prime supports inherent MAC addresses, which allows DECnet nodes to coexist with systems running other protocols that have MAC address restrictions.

DECnet support on Cisco routers includes local-area and wide-area DECnet Phase IV routing over Ethernet, Token Ring, FDDI, and serial lines (X.25, Frame Relay, SMDS). The following are the specifics of the Cisco support:

- Cisco routers interoperate with Digital routers, and Digital hosts do not differentiate between a Cisco router and a Digital router.

- Cisco IOS software uses HDLC framing rather than Digital Data Communications Message Protocol (DDCMP) framing for point-to-point lines.

- If you construct a network using both Cisco and Digital equipment, you must ensure that each point-to-point line has the same type of equipment on both ends.

- Cisco and DECnet Phase IV routers have incompatible X.25 support.

- As with point-to-point lines, you must use equipment from a single vendor on the X.25 portion of your network.

- You can configure your Cisco router running software Release 9.1 or later to interoperate with Digital equipment, or you can configure your Cisco router to operate with other Cisco routers that use prior versions Cisco IOS software.

- Cisco IOS software gives you additional security options through access lists.

- Cisco IOS software supports the address translation gateway (ATG), which allows the router to participate in multiple, independent DECnet networks. In case of duplicate addressing, ATG establishes a user-specified address translation table for selected nodes between networks.

- Digital uses some nonroutable protocols that are not part of the DECnet stack. For example, neither Cisco nor Digital routers can route the Maintenance Operation Protocol (MOP) and local-area transport (LAT); instead, these protocols must be bridged.

- The parameters in the Cisco implementation of DECnet are a subset of the parameters you can modify in the Digital Network Control Program (NCP). Cisco uses the same names, the same range of allowable values, and the same defaults wherever possible. You must use the configuration commands to set DECnet parameters. The Cisco DECnet implementation does not set parameters by communicating with NCP.

- Cisco supports DECnet Phase IV-to-Phase V conversion:

  - Cost information is represented in native mode for the Phase IV or Phase V protocols.

  - Digital has defined algorithms for mapping a subset of the Phase V address space onto the Phase IV address space, and for converting Phase IV and Phase V packets back and forth to support Phase IV hosts in Phase V networks, and vice versa.

- The Cisco implementation and Digital implementation differ in the following ways:

  - You can add Phase V support without modifying your existing Phase IV support.

  - The Cisco implementation delays converting packets from Phase IV to Phase V; while the Digital implementation converts as soon as possible.

Configuring DECnet

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes how to configure the Cisco implementation of the DECnet routing protocol. For a complete description of the DECnet commands in this chapter, refer to the "DECnet Commands" chapter of the *Cisco IOS DECnet Command Reference* publication. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the *Using Cisco IOS Software* document.

Note Not all Cisco access servers support the DECnet protocol. For more information, refer to the release notes for the current Cisco IOS release.

DECnet Configuration Task List

To configure DECnet routing, perform the tasks in the following sections:

- Enabling DECnet Routing (Required)
- Enabling Concurrent Routing and Bridging (Optional)
- Configuring DECnet on Token Rings (Optional)
- Configuring Address Translation (Optional)
- Specifying Name-to-DECnet Address Mapping (Optional)
- Enabling Phase IV-to-Phase V Conversion (Optional)

- Propagating Phase IV Areas Through an OSI Backbone (Optional)
- Establishing the Routing Table Size (Optional)
- Configuring Level 1 Routers (Optional)
- Configuring Level 2 Routers (Optional)
- Specifying Designated Routers (Optional)
- Configuring Static Routing (Optional)
- Controlling Access to DECnet Networks (Optional)
- Configuring DECnet Accounting (Optional)
- Enhancing DECnet Performance (Optional)
- Configuring DECnet over DDR (Optional)
- Configuring DECnet over PPP (Optional)
- Configuring DECnet over WANs (Optional)
- Routing DECnet over ISL in Virtual LANs (Optional)
- Monitoring and Maintaining the DECnet Network (Optional)

See the "DECnet Configuration Examples" section at the end of this chapter for configuration examples.

Enabling DECnet Routing

To enable DECnet routing, perform the tasks in the following sections:

- Either Enabling DECnet Phase IV Routing or Enabling DECnet Phase IV Prime Routing (Required)
- Assigning a DECnet Cost to Each Interface (Required)
- Specifying the DECnet Node Type (Required)

Enabling DECnet Phase IV Routing

To enable DECnet Phase IV routing, use the following command in global configuration mode:

Command	Purpose
Router(config)# **decnet** [*network-number*] **routing** *decnet-address*	Enables the DECnet Phase IV routing protocol on a global basis.

A DECnet host exists as a *node* in an *area.* An area spans many routers, and a single interface can have many areas attached to it. Therefore, if a router exists on many cables, it uses the same area and node for itself on all of them. Note how this protocol differs from other routing protocols, where each interface is given a different internetwork address. Figure 1 shows the DECnet approach.

Enabling DECnet changes the MAC addresses of the router interfaces. Changing the MAC addresses is not a problem on routers equipped with nonvolatile memory. On systems that attempt to get their IP network addresses from network servers instead of from nonvolatile memory, there might be a problem with the hardware addresses changing and confusing other IP-speaking hosts. If you are attempting to use DECnet on such a configuration, be sure to set all global DECnet parameters before enabling DECnet routing on the interfaces.

With DECnet Phase IV Prime, the change of MAC addresses is not an issue because you can change the MAC address of the interface.

✎
Note If you plan to use DECnet and Internet Packet Exchange (IPX) routing concurrently on the same interface, you should enable DECnet routing first, then enable IPX routing without specifying the optional MAC address. If you enable IPX, then DECnet, IPX routing will be disrupted.

Once you have enabled DECnet routing, you can obtain MAC addresses by using the **show interfaces** EXEC command. To disable DECnet routing, use the **no decnet routing** command.

Figure 1   DECnet Nodes and Area
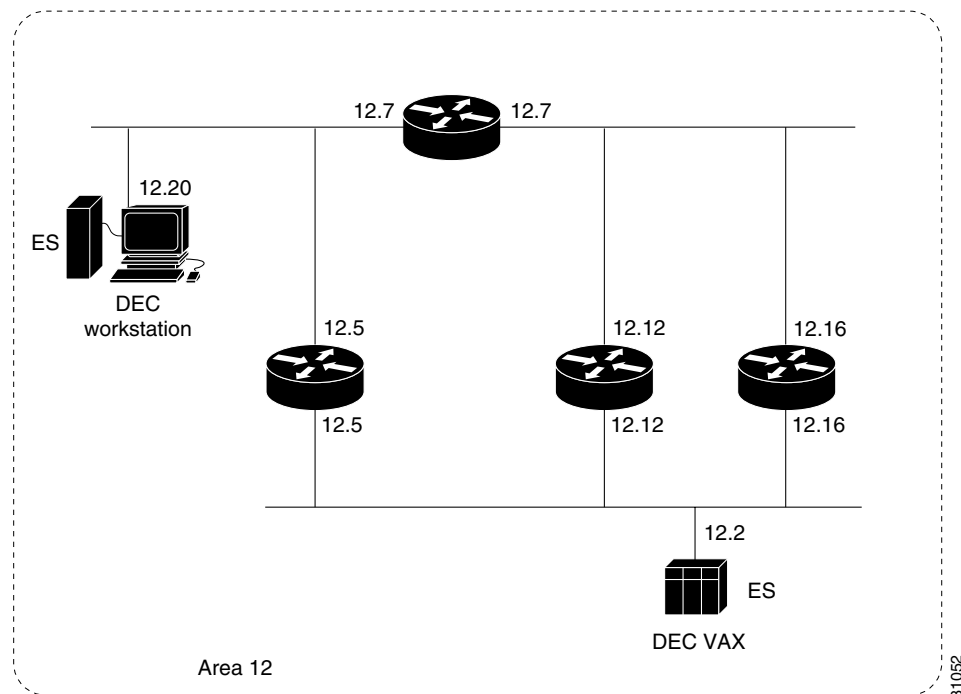
Enabling DECnet Phase IV Prime Routing

DECnet Phase IV requires that a MAC station address be constructed using DECnet addressing conventions, with a standard high-order byte string (AA-00-04-00) concatenated with the byte-swapped DECnet node address. Using DECnet addressing conventions can cause problems in configurations in which DECnet nodes must coexist with systems running protocols that have other MAC address restrictions.

DECnet Phase IV Prime allows an arbitrary MAC address on the LAN. An address can be assigned globally (that is, assigned by the IEEE), or it can be assigned locally by a system administrator.

To enable or disable DECnet Phase IV Prime, use one of the following commands in global configuration mode:

Command	Purpose
Router(config)# **decnet** [*network-number*] **routing iv-prime** *decnet-address*	Specifies Phase IV Prime routing.
Router(config)# **no decnet routing**	Stops DECnet Phase IV or Phase IV Prime routing.

Optionally, to map a DECnet multicast address to a Token Ring functional address other than the default functional address, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **decnet multicast-map** *multicast-address-type functional-address*	Specifies the type of multicast address and the functional address to which the multicast ID will map.

For examples of how to enable DECnet Phase IV Prime Routing, see the "DECnet Phase IV Prime Examples" section at the end of this chapter.

Assigning a DECnet Cost to Each Interface

After you have enabled DECnet routing, you must assign a cost to each interface over which you want DECnet to run. Assigning a cost to an interface enables DECnet on the interface and, using a standard formula, assigns a different MAC address than that "burned in" by the manufacturer. This section describes how to assign a cost to each interface.

DECnet routing decisions are based on cost, an arbitrary measure used to compare paths on the internetwork. Costs are based on such measures as hop count or media bandwidth. The lower the cost, the better the path. You must assign a cost to each interface.

To assign a cost to each interface for DECnet Phase IV Prime, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **decnet cost** *cost-value*	Assigns a cost to an interface.

Most DECnet installations have individualized routing strategies for using costs. Therefore, check the routing strategy used at your installation to ensure that the costs you specify are consistent with those set for other hosts on the network.

Figure 2 shows four routers (three Ethernets) and the various routes linking them. Each link has a different cost associated with it. The least-expensive route from Router 7 to Router 20 is via Router 12.

Figure 2   ***DECnet Cost Values***
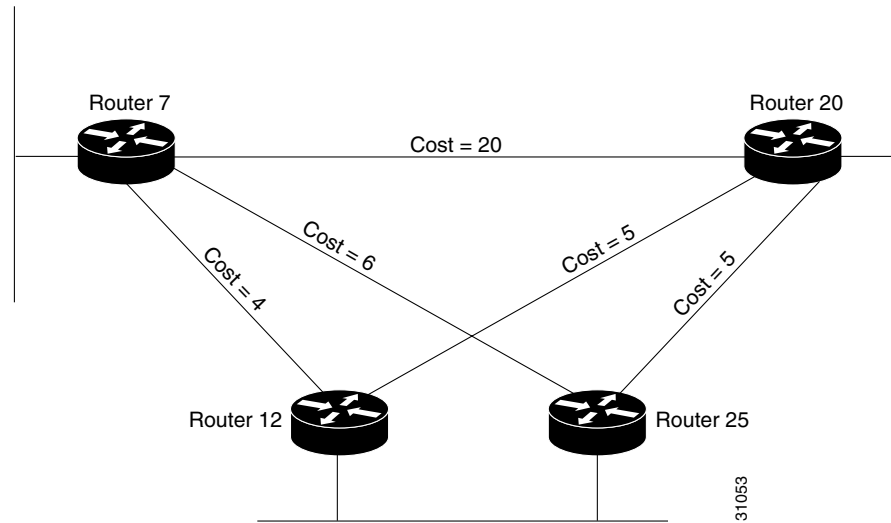
Specifying the DECnet Node Type

DECnet routing nodes are referred to as either Level 1 or Level 2 routers. You must specify the node type of the router. A Level 1 router exchanges packets with other end nodes and routers in the same area and ignores Level 2 packets; this type of routing is called *intra-area routing*. Level 2 routers participate in the DECnet routing protocol with other routers and route packets to and from routers in other areas; this type of routing is called *interarea routing*. Level 2 routers also act as Level 1 routers in their own area.

The keyword **area** indicates a Level 2, interarea, router. The keyword **routing-iv** indicates a Level 1, intra-area router. Level 1, intra-area routing is the default. In Level 1 mode, Cisco IOS software sends packets destined for other areas to a designated interarea router, which forwards them outside the area.

To specify the node types, use one of the following commands in global configuration mode:

Command	Purpose
`Router(config)# ` **`decnet`** `[network-number]` **`node-type area`**	Specifies an interarea node type of the router.
`Router(config)# ` **`decnet`** `[network-number]` **`node-type routing-iv`**	Specifies an intra-area node type of the router.

For an example of how to configure DECnet, see the "DECnet Example" section at the end of this chapter.

Enabling Concurrent Routing and Bridging

You can route DECnet on some interfaces and transparently bridge it on other interfaces simultaneously. To do this, you must enable concurrent routing and bridging. To configure an interface for concurrent routing and bridging, you use the **bridge crb** command.

To enable concurrent routing and bridging, use the following command in global configuration mode:

Command	Purpose
`Router(config)# `**`bridge crb`**	Enables concurrent routing and bridging.

Configuring DECnet on Token Rings

If any Cisco routers are running Release 9.0 or earlier, you can use the Token Ring as a backbone or transit network for DECnet routing but you cannot communicate with non-Cisco DECnet nodes on the Token Ring.

If all Cisco routers are running Release 9.1 or later, you can set DECnet encapsulation to allow Cisco interoperation with non-Cisco equipment.

If you have both Release 9.0 and 9.1 routers in the same network, and you want them to interoperate, you must set the encapsulation type to **pre-dec** on the Release 9.1 routers.

To run DECnet on Token Ring interfaces, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# `**`interface tokenring`** `number`	Enables DECnet on the Token Ring interface, and then enters interface configuration mode.
Step 2	`Router(config-if)# `**`decnet encapsulation`** `{`**`pre-dec`** `| `**`dec`**`}`	Configures the DECnet encapsulation mode for the specified interface.

Use the keyword **dec** with routers running Release 9.1 or later. Use the keyword **pre-dec** with routers running Release 9.0 or earlier, or in a network where routers running 9.0 and 9.1 must interoperate.

Configuring Address Translation

If you set up multiple networks, we recommend that you configure address translation in order to avoid problems with duplicate addressing between networks. If you have multiple DECnet networks, you must establish an address translation table for selected nodes between networks. Establishing an address translation table eliminates any potential problems of duplicate addressing occurring between networks. The address translation gateway (ATG) allows you to define multiple DECnet networks and map between them.

Mapping Between Networks

Configuring ATG allows Cisco IOS software to route traffic for multiple independent DECnet networks, and to establish a user-specified address translation for selected nodes between networks. Address translation allows connectivity between DECnet networks that might not otherwise be possible because of address conflicts (duplicate addresses) between them. Configuring ATG can be done over all media types.

When you use ATG, all the DECnet configuration commands implicitly apply to network number 0 unless you specify otherwise.

To translate a virtual DECnet address to a real network address, use the following command in global configuration mode:

Command	Purpose
`Router(config)# decnet first-network map virtual-address second-network real-address`	Establishes a translation entry to translate a virtual DECnet address to a real DECnet address for the router.

To display the address mapping information used by the DECnet ATG, use the **show decnet map** EXEC command.

For a simple example of how to configure address translation, see the "Address Translation Example" section at the end of this chapter.

Making a "Poor Man's Routing" Connection

As an additional feature and security precaution, DECnet "Poor Man's Routing" can be used between nodes outside of the translation map, provided those nodes have access to nodes that are in the map. For example, as illustrated in Figure 3 in the "Address Translation Example" section at the end of this chapter, a user on node B could issue the following VMS operating system command:

```
$ dir A::D::E::
```

When a Poor Man's Routing connection is made between two networks, only the two adjacent nodes between the networks will have any direct knowledge about the other network. Application-level network access can then be specified to route through the connection.

> **Note** Cisco does not support Poor Man's Routing directly; the intermediate nodes must be VMS systems with Poor Man's Routing enabled in the file-access language.

Specifying Name-to-DECnet Address Mapping

You can define a name-to-DECnet address mapping, which can be used instead of typing the set of numbers associated with a DECnet address.

To define a name-to-DECnet address mapping, use the following command in global configuration mode:

Command	Purpose
`Router(config)# decnet host name decnet-address`	Defines a name-to-DECnet address mapping.

The assigned DECnet name is displayed, where applicable, in the output of the **decnet route** and **show hosts** EXEC commands.

Enabling Phase IV-to-Phase V Conversion

Routers that have conversion enabled advertise reachability to both Phase IV and Phase V hosts in both Phase IV and Phase V routing updates. If you have Phase IV hosts in Phase V networks and vice versa, you must enable Phase IV-to-Phase V conversion (and vice versa) in order for all nodes to communicate with each other. To enable DECnet conversion, you must have both DECnet and ISO CLNS configured on your router; then use the following command in global configuration mode:

Command	Purpose
Router(config)# **decnet conversion** *nsap-prefix*	Enables DECnet Phase IV-to-Phase V (and vice versa) conversion on the router.

Verify that the area you specify in the **decnet conversion** global configuration command is the same as the area you specified in the ISO CLNS address. You must also enable CLNS on all interfaces, even if the router has only Phase IV hosts on some of the interfaces. Enabling CLNS on all interfaces allows information about those routers to be included in link-state packets and, consequently, enables other routers to be informed about the routers connected by that interface.

For an example of how to enable a Phase IV area through an OSI backbone, see the "Phase IV-to-Phase V Conversion Example" section at the end of this chapter.

Propagating Phase IV VAX Clusters to Phase V Areas

A Phase IV VAX cluster comprises one or more VAX machines, each with its own individual node address, and a supplemental node address for the cluster. One VAX machine, known as the gratuitous router, will act as the router for the cluster and advertise the cluster alias as an ISO CLNS end system that is attached to the gratuitous router.

The gratuitous router forms an adjacency with the nearest Phase IV router through the process of exchanging L1 router hellos with this router, similar to the process that Phase IV end systems follow to form an adjacency with Phase IV routers through the exchange of endnode hellos.

The Phase IV router will target the cluster alias specifically looking for the L1 routing updates from the gratuitous router, extracting the cluster alias from the update, and injecting the cluster alias into the Phase V cloud as an ISO CLNS end system. The router will also advertise all routes as being reachable through itself at a cost of 704 and a hop count value of 29, so that the gratuitous router will always attempt to route through the Phase IV router unless it already has a better route. Thus, the Phase IV VAX cluster is made reachable to remote end systems.

✏️ **Note** For conversion between Phase IV and Phase V to function, the Phase V area must be numbered so that it matches the converted Phase IV area.

The gratuitous router must form an adjacency with the router that is performing the Phase IV-to Phase-V conversion, therefore, the VAX cluster must be located on the same physical LAN as the Phase IV and Phase V routers.

The hold time for the cluster alias adjacency has a default of 300 seconds and must exceed the VAX broadcast routing timer. To configure the DECnet cluster alias adjacency, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **decnet cluster-holdtime**	Sets a hold time for a cluster alias adjacency.

To propagate Phase IV VAX clusters to Phase V areas, perform the tasks in these sections:

- Enabling Phase IV-to-Phase V Conversion
- Configuring CLNS IS-IS
- Configuring DECnet Cluster Alias Updates and Setting the DECnet Cluster Hold Time

Enabling Phase IV-to-Phase V Conversion

To enable Phase IV-to-Phase V conversion, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **decnet conversion nsap-prefix**	Enables DECnet Phase IV-to-Phase V (and vice versa) conversion on the router.

Configuring CLNS IS-IS

To enable Connetionless Network Service (CLNS) Intermediate System-to-Intermediate System (IS-IS), use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **clns routing**	Enables routing of CLNS packets.
Step 2	Router(config)# **router isis** [tag]	Enables IS-IS and enters router configuration mode.

Configuring DECnet Cluster Alias Updates and Setting the DECnet Cluster Hold Time

To configure DECnet cluster alias updates and set the DECnet cluster hold time, use the following commands beginning in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# **decnet cluster-alias update**	Allows DECnet cluster aliases updates to be propagated.
Step 2	Router(config-if)# **decnet cost** *cost-value*	Assigns a cost to an interface.
Step 3	Router(config-if)# **decnet cluster holdtime** *seconds*	Sets a hold time for a cluster alias adjacency.

For an example of how to propagate Phase IV VAX clusters to Phase V areas, see the "Phase IV VAX Cluster Alias to Phase V Areas Example" section at the end of this chapter.

Propagating Phase IV Areas Through an OSI Backbone

One limitation of the Phase IV-to-Phase V conversion has been the inability to propagate Phase IV area routes through Open System Interconnection (OSI) clouds. Using the "advertise" feature, you can explicitly configure any DECnet Phase IV areas that you want to propagate outward. You configure the border routers at the Phase IV/Phase V junction.

When distant routers send a packet destined across the cloud to a border router, the router converts the route and sends it as an OSI packet. In order for the converting router to have the corresponding OSI entry in which to convert the Phase IV packet, the other border router at the Phase IV/V junction must inject *static discard* routes. In this way, the first router converts the packet from Phase IV to Phase V, sending it through the cloud. At the other end, the router advertising the static discard route converts the packet back to Phase IV and discards the Phase V packet. In effect, a false entry is created in the Phase IV area table to propagate this information to other routers. This entry will not overwrite a native Phase IV entry if one already exists in the table.

To enable Phase IV areas to propagate through an OSI backbone on the router, use the following command in global configuration mode:

Command	Purpose
Router(config)# **decnet advertise** *decnet-area hops cost*	Enables DECnet Phase IV areas to propagate through an OSI backbone on the router.

To enable the border router *at the far end* to convert the Phase V packet back to Phase IV, it must advertise a static discard route. To configure the far border router, use the following command in global configuration mode:

Command	Purpose
Router(config)# **clns route** *nsap-prefix* **discard**	Advertises a static discard route on the far-end border router.

For an example of how to enable a Phase IV area through an OSI backbone, see the "Phase IV Areas Through an OSI Backbone Example" section at the end of this chapter.

Establishing the Routing Table Size

You can configure the maximum number of addresses and areas allowed in the Cisco IOS software routing table. It is best to keep the number of routing updates small. All areas or nodes that cannot be reached must be advertised as unreachable. When configuring the routing table size, indicate the maximum node and area numbers that can exist in the network. In general, all routers on the network should use the same values for maximum addresses and nodes.

To establish the routing table size, use either or both of the following commands in global configuration mode as needed:

Command	Purpose
`Router(config)#` **`decnet`** [`network-number`] **`max-address`** `value`	Sets the maximum node address that can exist in the network.
`Router(config)#` **`decnet`** [`network-number`] **`max-area`** `area-number`	Sets the largest number of areas that Cisco IOS software can handle in its routing table.

Configuring Level 1 Routers

Perform any of the tasks in the following section for the routers you have configured as Level 1 (intra-area) routers. In Level 1 mode, the router sends packets destined for other areas to a designated interarea router, which forwards them outside the area.

Setting Areas as Unreachable

You can set the maximum cost that Cisco IOS software considers usable for intra-area routing. The software ignores routes within its local area that have a cost greater than the value you specify.

Setting Maximum Number of Hops

You can also set the maximum number of hops (or traversal of different paths) that Cisco IOS software considers usable for intra-area routing. The software ignores routes within its local area that have a value greater than you specify.

To set certain intra-areas as unreachable based on cost value or hop count, use either or both of the following commands in global configuration mode as needed:

Command	Purpose
`Router(config)#` **`decnet`** [`network-number`] **`max-cost`** `cost`	Sets the maximum cost value for intra-area routing.
`Router(config)#` **`decnet`** [`network-number`] **`max-hops`** `hop-count`	Sets the maximum hop count value for intra-area routing.

Configuring Level 2 Routers

Perform any of the tasks in the following section for the routers you have configured as Level 2 (interarea) routers. In Level 2 mode, Cisco IOS software sends packets destined for other areas via the least-cost path to another interarea router.

Setting Areas as Unreachable

You can set the maximum cost for a usable route to a distant area. Cisco IOS software treats as unreachable any route with a cost greater than the value you specify.

Setting Maximum Number of Hops

You can also set the maximum number of hops for a usable route to a distant area. Cisco IOS software treats as unreachable any route with a hop count greater than the value you specify.

To set certain interareas as unreachable based on cost value or hop count, use either or both of the following commands in global configuration mode as needed:

Command	Purpose
Router(config)# **decnet** [*network-number*] **area-max-cost** *value*	Sets the maximum cost specification value for interarea routing.
Router(config)# **decnet** [*network-number*] **area-max-hops** *value*	Sets the maximum hop count value for interarea routing.

Specifying Designated Routers

You can determine the router with which all end nodes on an Ethernet communicate if they do not know where else to send a packet. This router is called the *designated* router and is the router with the highest priority. When two or more routers on a single Ethernet in a single area share the same highest priority, the router with the highest node number is selected. You can reset the priority to help ensure that it is elected the designated router in its area. The priority is specified on a per-interface basis.

To specify designated routers, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **decnet router-priority** *value*	Assigns or changes a priority number to a router on a per-interface basis to receive packets for which no destination is specified.

Configuring Static Routing

Static routing is used when it is not possible or desirable to use dynamic routing. The following are some instances of when you would use static routing:

- The routers do not support the same dynamic routing protocol.
- Your network includes WAN links that involve paying for connect time or for per-packet charges.
- You want routers to advertise connectivity to external networks, but you are not running an interdomain routing protocol.
- You must interoperate with equipment from another vendor that does not support any of the dynamic routing protocols that we support.
- The router operates over X.25, Frame Relay, or Switched Multimegabit Data Service (SMDS) networks.

Note   An interface that is configured for static routing cannot reroute around failed links.

To configure static routing, perform any of the tasks in the following sections:

- Configuring a Static Route (Optional)

- Configuring a Static Route for an Interface (Optional)
- Configuring a Default Static Route (Optional)
- Configuring a Default Static Route for an Interface (Optional)
- Configuring DECnet Static Route Propagation (Optional)

Configuring a Static Route

You can configure a specific static route and apply it globally even when you use dynamic routing.

To apply a specific static route globally, use the following command in global configuration mode:

Command	Purpose
Router(config)# **decnet route** *decnet-address next-hop-address* [*hops* [*cost*]]	Configures a specific static route.

Configuring a Static Route for an Interface

You can select a specific interface for a specific static route when you do not know the address of your neighbor.

To apply a specific static route to a specific interface, use the following command in global configuration mode:

Command	Purpose
Router(config)# **decnet route** *decnet-address next-hop-type number* [*snpa-address*] [*hops* [*cost*]]	Configures a specific static route for a specific interface.

Configuring a Default Static Route

You can configure a default static route and apply it globally, even when you use dynamic routing.

To apply a default static route globally, use the following command in global configuration mode:

Command	Purpose
Router(config)# **decnet route default** *next-hop-address* [*hops* [*cost*]]	Configures a default route.

Configuring a Default Static Route for an Interface

You can configure a specific interface for a default static route when you do not know the address of your neighbor.

To apply a default static route to a specific interface, use the following command in global configuration mode:

Command	Purpose
Router(config)# **decnet route default** *next-hop-type number* [*snpa-address*] [*hops* [*cost*]]	Configures a specific default route for a specific interface.

Configuring DECnet Static Route Propagation

When you use static routes or default static routes, you can specify whether the static routes are propagated. By default, DECnet static routes will not be propagated to other routers.

To enable or disable static route propagation, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **decnet propagate static**	Enables static route propagation.
Router(config)# **no decnet propagate static**	Disables static route propagation.

Controlling Access to DECnet Networks

Cisco provides several layers of access control for network security. You can perform any or all of the tasks in the following sections:

- Creating an Access List Based on Source Addresses (Optional)
- Creating an Access List Based on Source and Destination Addresses (Optional)
- Adding Filters to Access Lists (Optional)
- Configuring Access Groups (Optional)
- Configuring Routing Filters (Optional)

Creating an Access List Based on Source Addresses

You can configure lists globally to control access by source addresses. The standard form of the DECnet access list has a source DECnet address followed by a source-mask address, with bits set wherever the corresponding bits in the address should be ignored. DECnet addresses are written in the form *area.node*. For example, 50.4 is area 50, node 4. All addresses and masks are in decimal notation.

To create a standard DECnet access list, use the following command in global configuration mode:

Command	Purpose
Router(config)# **access-list** *access-list-number* {**permit** | **deny**} *source source-mask*	Creates an access list to restrict access to a single address.

To disable the list, use the **no access-list** command.

Creating an Access List Based on Source and Destination Addresses

The extended form of the DECnet access list has a source DECnet address and mask pair, followed by a destination DECnet address and mask pair.

To configure an extended DECnet access list, use the following command in global configuration mode:

Command	Purpose
Router(config)# **access-list** *access-list-number* {**permit** │ **deny**} *source source-mask* [*destination destination-mask*]	Creates an extended access list for several addresses.

To disable the extended access list, use the **no access-list** command.

Adding Filters to Access Lists

DECnet access lists can be used to filter *connect initiate* packets. With these packets, you can filter by DECnet object type, such as MAIL.

To add filters to access lists, use the following command in global configuration mode:

Command	Purpose
Router(config)# **access-list** *access-list-number* {**permit** │ **deny**} *source source-mask* [*destination destination-mask* {**eq** │ **neq**} [[*source-object*] [*destination-object*] [*identification*]] **any**]	Adds filtering (by DECnet object type) to an access list.

Configuring Access Groups

You can restrict access to specific interfaces by applying an access list to them. Interfaces that are associated with the same access list are considered to be an access group.

To configure access groups, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **decnet access-group** *access-list-number*	Assigns an access list to a specified interface.

Configuring Routing Filters

You can control access to hello messages or routing information being received or sent on an interface. Addresses that are not in the access list are shown in the update message as unreachable.

To configure routing filters, use either or both of the following commands in interface configuration mode as needed:

Command	Purpose
`Router(config-if)# `**`decnet in-routing-filter`**` access-list-number`	Controls access to hello messages or routing information received on a specified interface.
`Router(config-if)# `**`decnet out-routing-filter`**` access-list-number`	Controls access to routing information being sent on a specified interface.

Configuring DECnet Accounting

DECnet accounting enables you to collect information about DECnet packets and the number of bytes that are switched through the Cisco IOS software. You collect accounting information based on the source and destination DECnet addresses. DECnet accounting tracks only DECnet traffic that is routed out an interface on which DECnet accounting is configured; it does not track traffic generated by or terminating at the router itself.

DECnet access lists and fast switching support DECnet accounting statistics. Autonomous and silicon switching engine (SSE) switching do not support DECnet accounting statistics.

The Cisco IOS software maintains two accounting databases: an active database and a checkpoint database. The active database contains accounting data tracked until the database is cleared. When the active database is cleared, its contents are copied to the checkpoint database. Using these two databases together enables you to monitor both current traffic and traffic that has previously traversed the router.

To configure DECnet accounting, perform the tasks described in the following sections:

- Enabling DECnet Routing on the Router
- Enabling DECnet Accounting
- Customizing DECnet Accounting

Enabling DECnet Routing on the Router

To enable DECnet routing, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# `**`decnet`**` [network-number] `**`routing`**` [`**`iv-prime`**`] decnet-address`	Enables DECnet routing.
Step 2	`Router(config)# `**`decnet`**` [network-number] `**`node-type`**` [`**`area`**`	`**`routing-iv`**`]`	Specifies the node type (interarea or intra-area).

Enabling DECnet Accounting

To enable DECnet accounting on a specific interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface` *`type slot`***`/`***`port`*	Specifies the serial interface.
Step 2	`Router(config-if)# decnet cost` *`cost-value`*	Specifies the cost value for the interface.
Step 3	`Router(config-if)# decnet accounting`	Enables DECnet accounting.

> ✎
> **Note**   If DECnet accounting is enabled on an interface but no accounting list is specified, DECnet accounting will track all traffic through the interface, up to the accounting threshold limit.

For an example of how to enable DEC net accounting on a specific interface, see the "DECnet Accounting Configuration Example" section at the end of this chapter.

Customizing DECnet Accounting

To customize DECnet accounting, use one or more of the following commands in global configuration mode:

Command	Purpose
`Router(config)# decnet accounting threshold` *`threshold`*	Specifies the maximum number of accounting entries.
`Router(config)# decnet accounting transits` *`count`*	Specifies the maximum number of transit entries.
`Router(config)# decnet accounting list` *`src-dec-address dest-dec-address`*	Specifies the source and destination pair addresses for which DECnet accounting information is kept. Use one command for each source and destination pair.

Enhancing DECnet Performance

To optimize internetwork performance, perform any or all of the tasks in the following sections:

- Setting Maximum Equal-Cost Paths (Optional)
- Establishing Selection for Paths of Equal Cost (Optional)
- Setting Maximum Visits (Optional)
- Adjusting the Hello Timer (Optional)
- Disabling Fast Switching (Optional)
- Setting the Congestion Threshold (Optional)
- Adjusting the Broadcast Routing Timer (Optional)

Setting Maximum Equal-Cost Paths

You can set the maximum number of equal-cost paths to a destination on a global basis. Limiting the number of equal-cost paths can save memory on routers with limited memory or with very large configurations. Additionally, in networks with a large number of multiple paths and end systems with limited ability to cache out-of-sequence packets, performance might suffer when traffic is split between many paths.

To set maximum equal-cost paths, use the following command in global configuration mode:

Command	Purpose
Router(config)# **decnet** [*network-number*] **max-paths** *value*	Sets the maximum number of equal-cost paths to a destination. Paths are set in the routing table.

To display the first hop route to a specified address and to show all equal-cost paths to a single destination, use the **show decnet route** EXEC command.

Establishing Selection for Paths of Equal Cost

You can establish one of two methods for selecting among paths of equal cost on the router: on a round-robin basis, which is the default, or by configuring Cisco IOS software so that traffic for any higher-layer session is always routed over the same path.

In the round-robin or *normal* mode, the first packet is sent to the first node, the second packet to the second node, and so on. If the final node is reached before all packets are sent, the next packet in line is sent to the first node, then to the second node, and so forth.

The *interim* mode supports older implementations of DECnet (VMS versions 4.5 and earlier) that do not support out-of-order packet caching. Other sessions might take another path, thus using equal-cost paths that a router might have for a particular destination.

To select normal or interim mode on the router, use one of the following commands in global configuration mode:

Command	Purpose
Router(config)# **decnet path-split-mode normal**	Specifies that traffic is routed over equal-cost paths on a round-robin basis.
Router(config)# **decnet path-split-mode interim**	Specifies that traffic is always routed over the same path.

Setting Maximum Visits

You can determine the number of times that a packet can pass through a router. Cisco IOS software ignores packets that have a value greater than the amount of visits you specify. Digital recommends that the value be at least twice the number of maximum hops, to allow packets to reach their destinations when routes are changing.

To set the number of times a packet can pass through a router, use the following command in global configuration mode:

Command	Purpose
`Router(config)# `**`decnet`**` [`*`network-number`*`]` **`max-visits`** *`value`*	Sets the number of times a packet can pass through a router.

Adjusting the Hello Timer

Hosts use the hello messages to identify the hosts with which they can communicate directly. The Cisco IOS software sends hello messages every 15 seconds by default. On extremely slow serial lines, you might want to increase this value on a per-interface basis to reduce overhead.

To adjust the interval for sending hello messages, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# `**`decnet hello-timer`**` `*`seconds`*	Adjusts the interval (in seconds) for sending hello messages on interfaces with DECnet enabled.

Disabling Fast Switching

By default, our DECnet routing software implements fast switching of DECnet packets. You might want to disable fast switching to save memory space on interface cards and to help avoid congestion when high-bandwidth interfaces are writing large amounts of information to low-bandwidth interfaces. Disabling fast switching is especially important when rates slower than T1 are used.

To disable fast switching of DECnet packets, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# `**`no decnet route-cache`**	Disables fast switching of DECnet packets on a per-interface basis.

Setting the Congestion Threshold

If a router configured for DECnet experiences congestion, it sets the *congestion-experienced* bit. You can define the congestion threshold on a per-interface basis. By setting this threshold, you will cause the system to set the congestion-experienced bit if the output queue has more than the specified number of packets in it.

To set the congestion threshold, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# `**`decnet congestion-threshold`**` `*`number`*	Sets the congestion threshold.

Adjusting the Broadcast Routing Timer

Other routers use broadcast updates to construct local routing tables. Increasing the time between routing updates on a per-interface basis reduces the amount of unnecessary network traffic. Digital calls this parameter the *broadcast routing timer* because Digital uses a different timer for serial lines. Our DECnet implementation does not make this distinction.

To adjust the broadcast routing timer, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **decnet routing-timer** *seconds*	Adjusts how often Cisco IOS software sends routing updates that list all the hosts that the router can reach on a per-interface basis.

Configuring DECnet over DDR

Dial-on-demand routing (DDR) is now supported for DECnet. For more information, refer to the "Dial-on-Demand Routing" section in the *Cisco IOS Dial Technologies Configuration Guide*.

Configuring DECnet over PPP

DECnet packets can now be fast switched over PPP. For more information, refer to the *Cisco IOS Dial Technologies Configuration Guide.*

Configuring DECnet over WANs

You can configure DECnet over X.25, SMDS, and Frame Relay networks by configuring the appropriate address mappings as described in the "Configuring X.25 and LAPB," "Configuring SMDS," and "Configuring Frame Relay" chapters in the *Cisco IOS Wide-Area Networking Configuration Guide*.

Enabling Split Horizon

Split horizon is enabled by default. When split horizon is enabled, routing updates sent out on an interface do not include any information that was originally learned from that interface, and broadcasts are not re-sent on the receiving interface. Disabling split horizon causes Cisco IOS software to include all information in routing updates and to resend broadcast packets on the network from which they were received.

To disable split horizon, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **no decnet split-horizon**	Disables split horizon when sending routing updates.

Routing DECnet over ISL in Virtual LANs

DECnet can be routed over virtual LAN (VLAN) subinterfaces using the Inter-Switch Link (ISL) encapsulation protocol. Full-feature Cisco IOS software is supported on a per-VLAN basis, allowing standard DECnet capabilities to be configured on VLANs. Refer to the *Cisco IOS Switching Services Configuration Guide* for information on configuring DECnet routing over ISL in VLANs.

Monitoring and Maintaining the DECnet Network

To clear counters, test network node reachability, and display information about DECnet networks, use the following commands in user EXEC or privileged EXEC mode:

Command	Purpose
Router> **clear decnet counters**	Clears the DECnet counters.
Router> **ping decnet** {*host* | *address*}	Tests network node reachability.
Router# **show decnet**	Displays the global DECnet parameters.
Router> **show decnet interface** [*type number*]	Displays the global DECnet status and configuration for all interfaces, or the status and configuration for a specified interface, including address, paths, cost, access lists, and more.
Router> **show decnet map**	Lists address mapping information used by the DECnet ATG.
Router# **show decnet neighbors**	Displays all Phase IV and Phase IV Prime neighbors and the MAC address associated with each neighbor.
Router> **show decnet route** [*decnet-address*]	Displays DECnet routing table.
Router# **show decnet static**	Displays static DECnet routing table.
Router> **show decnet traffic**	Lists DECnet traffic statistics, including datagrams sent, received, and forwarded.

Configuring MOP

To enable Maintenance Operation Protocol (MOP) on an interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **mop enabled**	Enables MOP.

To enable an interface to send out periodic MOP system identification messages on an interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **mop sysid**	Enables MOP message support.

DECnet Configuration Examples

The following sections show examples of some common DECnet configuration activities:

- DECnet Phase IV Prime Examples
- DECnet Example
- Address Translation Example
- Phase IV-to-Phase V Conversion Example
- Phase IV VAX Cluster Alias to Phase V Areas Example
- Phase IV Areas Through an OSI Backbone Example
- DECnet Accounting Configuration Example

DECnet Phase IV Prime Examples

This section includes examples of configuring DECnet Phase IV Prime support for inherent MAC addresses. The comments in these examples point out some possible configuration errors, in addition to explaining correct command lines.

The following example shows how to configure an Ethernet interface 0 for DECnet Phase IV Prime:

```
decnet routing iv-prime 1.1
interface ethernet 0
 decnet cost 10
! Router is bilingual on Ethernet interface 0.
```

The following example shows how to configure a Token Ring interface 1 with a MAC address that is not supported by DECnet Phase IV:

```
decnet routing 2.1
interface tokenring 1
 decnet cost 5
 mac-address 0000.0c00.62e6
! Interface Token Ring 1 has MAC address as set.
! This is an error because the Token Ring interface has a MAC address that is
! not Phase IV-compatible, and the router is not running Phase IV Prime.
```

The following example shows how to configure the router to support DECnet Phase IV Prime later in the configuration:

```
interface tokenring 1
 decnet cost 5
 mac-address 0000.0c00.62e6
! Invalid configuration, because router is only Phase IV.
 decnet routing iv-prime 5.5
! Become a Phase IV Prime router.

interface tokenring 1
 mac-address 0000.0c00.62e6
! Valid configuration because the router is now running Phase IV Prime.
```

The following example shows valid and invalid ways of using the **decnet multicast-map** command:

```
decnet routing iv-prime 3.4

interface tokenring 1
 decnet multicast-map phiv-prime-all-bridges c000.2000.0000
! Invalid value (phiv-prime-all-bridges) for multicast ID string.
```

```
interface tokenring 1
 decnet multicast-map iv-prime-all-routers d000.2000.0000
! Invalid value (d000.2000.0000) for functional address.

interface tokenring 1
 decnet multicast-map iv-prime-all-routers c000.2000.0000
! This will work. The command redefines the multicast to functional address
! mapping for the "all Phase IV Prime routers" multicast.
```

DECnet Example

The following example shows the commands required for enabling DECnet. DECnet routing is established on a router at address 4.27. The node is configured as a Level 2, or interarea router. A cost of four is set for the Ethernet interface 0. A cost of ten is set for the serial 1 interface.

```
decnet routing 4.27
decnet node area
interface ethernet 0
 decnet cost 4
interface serial 1
 decnet cost 10
```

Address Translation Example

In Figure 3, the router is connected to two DECnet networks using Ethernet. The following example shows how to configure an ATG between Network 0 and Network 1.

Figure 3   ATG Configuration Example
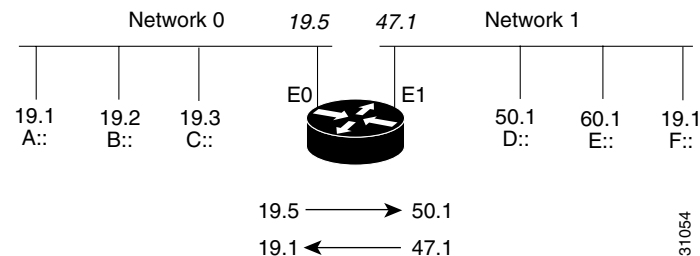
In Network 0, the router is configured at address 19.4 and is a Level 1 router. In Network 1, the router is configured at address 50.5 and is an area router. At this point, no routing information is exchanged between the two networks. Each network in the router has a separate routing table.

```
decnet 0 routing 19.4
decnet 0 node routing-iv
interface ethernet 0
 decnet 0 cost 1
!
decnet 1 routing 50.5
decnet 1 node area
interface ethernet 1
 decnet 1 cost 1
```

The following example shows how to establish a translation map:

```
decnet 0 map 19.5 1 50.1
decnet 1 map 47.1 0 19.1
```

Packets in Network 0 sent to virtual address 19.5 will be routed to Network 1, and the destination address will be translated to 50.1. Packets sent to virtual address 47.1 in Network 1 will be routed to Network 0 as 19.1.

Table 1 defines the parameters for the translation map.

Table 1   **Packet Exchange Between Nodes A and D**

Source	Destination
A packet addressed as: 19.1	is received on Ethernet 0 as: 19.5
Translates to: 47.1	and is sent out Ethernet 1 as: 50.1
A reply packet: 50.1	is received on Ethernet 0 as: 47.1
Translates to: 19.5	and is sent on Ethernet 0 as: 19.1

Network 0 uses a block of addresses from its area to map the remote nodes. In Network 0, the router will advertise nodes 19.5 and 19.6. These nodes must not already exist in Network 0.

Network 1 uses another area for the address translation. Because Cisco IOS software will be advertising the availability of area 47, that area should not already exist in Network 1 because DECnet area fragmentation could occur.

Only nodes that exist in the maps on both networks will be able to communicate directly. Network 0 node 19.1 will be able to communicate with Network 1 node 50.1 (as 19.5), but will not be able to communicate directly with Network 1 node 60.1.

When naming nodes, use the appropriate address in each network. See the configurations that follow for examples.

Network 0 VMS NCP Command File Sample

```
$MCR NCP
define node 19.1 name A
define node 19.2 name B
define node 19.3 name C
define node 19.4 name GS
define node 19.5 name D
define node 19.6 name F
```

Network 1 VMS NCP Command File Sample

```
$MCR NCP
define node 50.1 name D
define node 50.5 name GS
define node 60.1 name E
define node 19.1 name F
define node 47.1 name A
define node 47.2 name C
```

Phase IV-to-Phase V Conversion Example

Figure 4 shows that for the DECnet Phase IV-to-Phase V conversion to work properly, Connectionless Network Service (CLNS) Intermediate System-to-Intermediate System (IS-IS) must be configured on certain interfaces.

Note that although Router A has only Phase IV hosts connected by its Ethernet 0 interface, the interface must be configured for CLNS IS-IS for Router A to convert the Phase IV adjacency information into Phase V. If the Ethernet interface 0 on Router A is not configured for CLNS IS-IS, Router B will never receive information about Router D and end node 1.

Figure 4   *Sample Phase IV-to-Phase V Network Conversion*
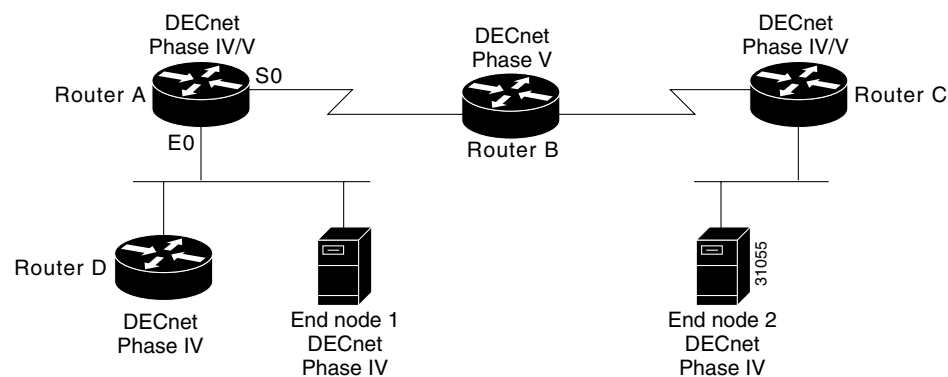
Configuration for Router A

```
decnet routing 1.1
decnet conversion 49
clns routing
router isis
 net 49.0001.aa00.0400.0104.00
interface ethernet 0
 clns router isis
 decnet cost 4
interface serial 0
 clns router isis
```

Sample Configuration for Router D

```
decnet routing 1.10
interface ethernet 0
 decnet cost 4
```

Phase IV VAX Cluster Alias to Phase V Areas Example

The following example shows the commands required for allowing Phase IV VAX cluster alias to be reachable by Phase V areas. Note that cluster alias updates will only be propagated when Phase IV-to-Phase V conversion has been enabled, the router has been configured for CLNS IS-IS, and the **decnet cluster-alias update** command has been entered in order to allow updates. For the Ethernet interface 1/0 interface, a DECnet cost of four and a DECnet cluster holdtime of 200 seconds has been entered:

```
decnet routing 1.1
decnet conversion 49
```

```
clns routing
router isis
 net 49.0001.aa00.0400.0104.00
interface ethernet 1/0
 clns router isis
 decnet cost 4
 decnet cluster 200
 decnet cluster-alias update
```

Phase IV Areas Through an OSI Backbone Example

The following example shows how to configure border routers to propagate Phase IV areas through an OSI backbone using the advertise feature. In this example, Router X in area 8 wants to communicate with Router Y in area 9.

Figure 5 illustrates the network, and the configurations that follow illustrate the commands required for enabling the advertise feature.

Figure 5　　　Sample Phase IV/Phase V Backbone Network
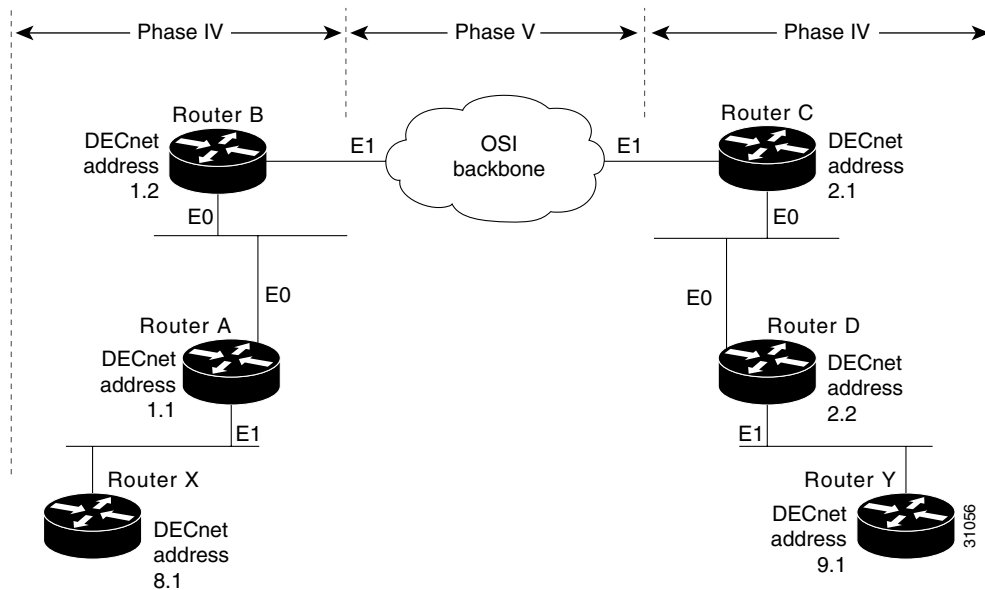
Configuration for Router B

```
decnet conversion 49
! Propagate Area 9 reachability information
decnet advertise 9 4 2
! Create dummy OSI route to force conversion to Phase IV
clns route 49.0008 discard
```

Configuration for Router C

```
decnet conversion 49
! Propagate Area 8 reachability information
decnet advertise 8 6 3
! Create dummy OSI route to force conversion to Phase IV
clns route 49.0009 discard
```

The routing table for Router A will then contain the following, as displayed with the **show decnet route** EXEC command:

```
  Area       Cost   Hops   Next Hop to Node      Expires   Prio

*1            0      0        (Local) -> 1.1
*8            4      1      Ethernet1 -> 8.1         35      64    A
*9            5      2      Ethernet0 -> 1.2
  Node       Cost   Hops   Next Hop to Node      Expires   Prio

*(Area)       0      0        (Local) -> 1.1
*1.1          0      0        (Local) -> 1.1
*1.2          4      1      Ethernet4 -> 1.2         38      64    VA
```

The routing table for Router B will then contain the following:

```
  Area       Cost   Hops   Next Hop to Node      Expires   Prio

*1            0      0        (Local) -> 1.2
*8            8      2      Ethernet0 -> 1.1
*9            4      2          (OSI) -> 1.2
  Node       Cost   Hops   Next Hop to Node      Expires   Prio

*(Area)       0      0        (Local) -> 1.2
*1.1          4      1      Ethernet0 -> 1.1         37      64    VA
*1.2          0      0        (Local) -> 1.2
```

The routing table for Router C will then contain the following:

```
  Area       Cost   Hops   Next Hop to Node      Expires   Prio

*2            0      0        (Local) -> 2.1
*8            6      3          (OSI) -> 2.1
*9            8      2      Ethernet0 -> 2.2
  Node       Cost   Hops   Next Hop to Node      Expires   Prio

*(Area)       0      0        (Local) -> 2.1
*2.1          0      0        (Local) -> 2.1
*2.2          4      1      Ethernet0 -> 2.2         33      64    VA
```

DECnet Accounting Configuration Example

Figure 6 illustrates DECnet accounting configured on the outbound serial interfaces for Router A and Router C. Note that because Router A and Router C exist in two different DECnet areas, they must be configured as interarea, or Level 2, routers.

Figure 6   *DECnet Accounting Configuration*
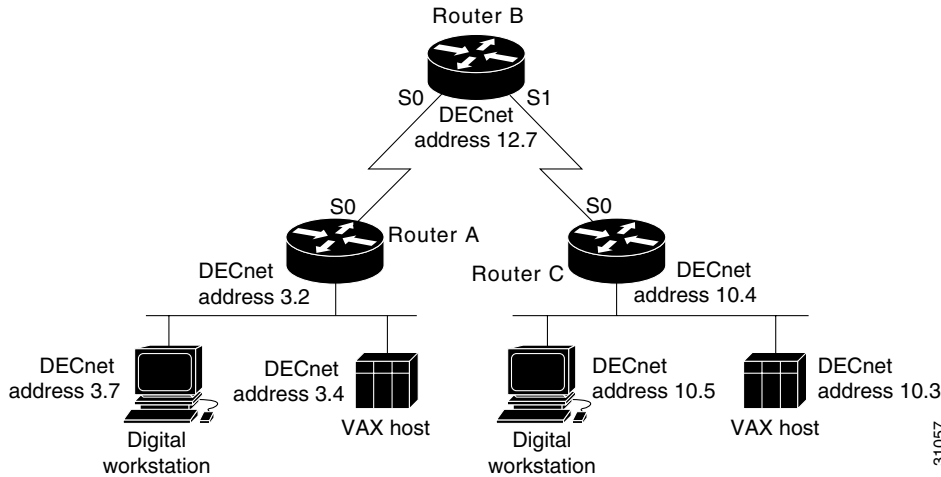
On Router A, DECnet accounting is enabled on an interface that is routing DECnet traffic. With no other commands used for the interface configuration, DECnet accounting on Router A tracks all DECnet traffic outbound on that interface up to the default accounting threshold of 512 source and destination pair addresses.

Configuration for Router A

```
decnet routing 3.2
decnet node-type area
interface serial 0
 decnet cost 20
 decnet accounting
interface ethernet 0
 decnet cost 4
```

Router B is configured to track traffic between all pairs specified in the **decnet accounting list** command. Router B also tracks traffic for pairs not specified in the **decnet accounting list** command up to the value specified for the **decnet accounting transit** command. If traffic between a source and destination endpoint pair not listed traverses the router, that traffic is added to the aggregate value, which appears in the display for the **show decnet accounting** command.

Configuration for Router B

```
decnet routing 12.7
interface serial 0
 decnet cost 20
 decnet accounting
interface serial 1
 decnet cost 20
 decnet accounting
decnet node type area
decnet accounting list 3.4 10.5
decnet accounting list 3.7 10.5
decnet accounting list 3.4 10.3
decnet accounting transits 2
```

Router C is configured to track DECnet traffic according to the values specified with the DECnet commands. The accounting threshold is set to 1000, which means that DECnet accounting will track all traffic passing through the router for up to 1000 source and destination address pairs.

Configuration for Router C

```
decnet routing 10.4
decnet node-type area
interface serial 0
 decnet cost 20
 decnet accounting
 decnet accounting threshold 1000
interface ethernet 0
 decnet cost 4
```