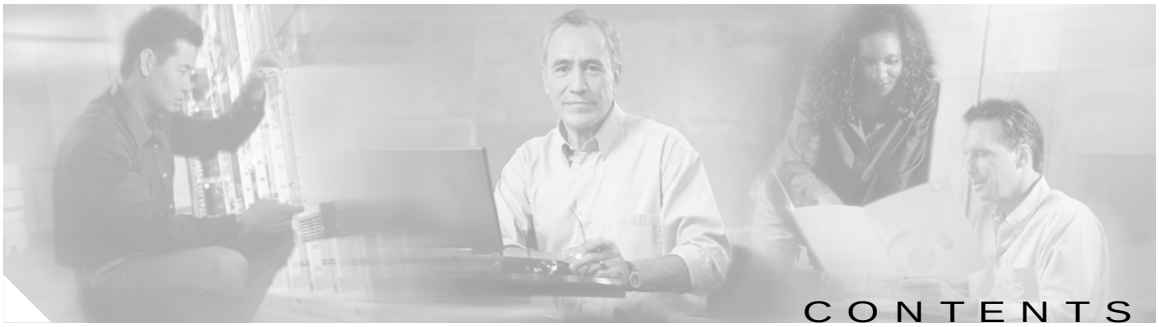
Cisco IOS Novell IPX Command Reference

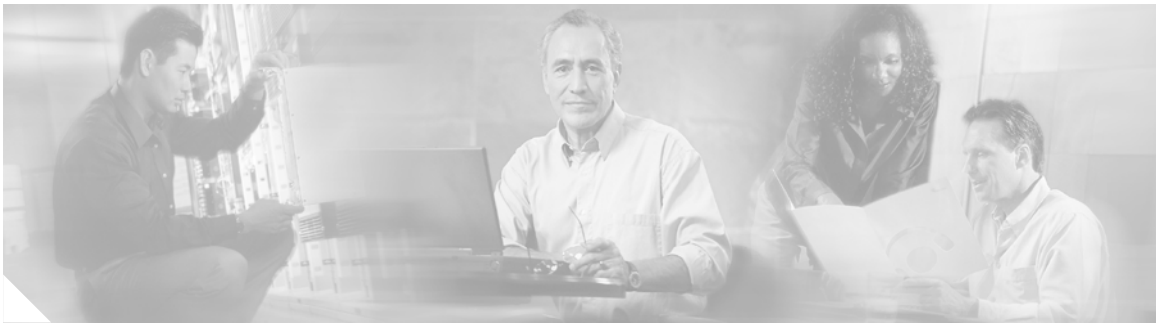
Release 12.4

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: 78-17474-01

Cisco IOS Novell IPX Command Reference





About Cisco IOS Software Documentation for Release 12.4

This chapter describes the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation, technical assistance, and additional publications and information from Cisco Systems. It contains the following sections:

Documentation Objectives

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

Audience

The Cisco IOS software documentation set is intended primarily 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 software commands necessary to perform particular tasks. The Cisco IOS software documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS software release.

Documentation Organization for Cisco IOS Release 12.4

The Cisco IOS Release 12.4 documentation set consists of the configuration guide and command reference pairs listed in Table 1 and the supporting documents listed in Table 2. The configuration guides and command references are organized by technology. For the configuration guides:

- Some technology documentation, such as that for DHCP, contains features introduced in Releases 12.2T and 12.3T and, in some cases, Release 12.2S. To assist you in finding a particular feature, a roadmap document is provided.
- Other technology documentation, such as that for OSPF, consists of a chapter and accompanying Release 12.2T and 12.3T feature documents.

Note In some cases, information contained in Release 12.2T and 12.3T feature documents augments or supersedes content in the accompanying documentation. Therefore it is important to review all feature documents for a particular technology.

Table 1 lists the Cisco IOS Release 12.4 configuration guides and command references.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Description
IP	
Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 *Cisco IOS IP Addressing Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP addressing and services, including Network Address Translation (NAT), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Application Services Configuration Guide, Release 12.4 *Cisco IOS Application Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP application services, including IP access lists, Web Cache Communication Protocol (WCCP), Gateway Load Balancing Protocol (GLBP), Server Load Balancing (SLB), Hot Standby Router Protocol (HSRP), and Virtual Router Redundancy Protocol (VRRP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Mobility Configuration Guide, Release 12.4 *Cisco IOS IP Mobility Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Mobile IP and Cisco Mobile Networks. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Multicast Configuration Guide, Release 12.4 *Cisco IOS IP Multicast Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP multicast, including Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Source Discovery Protocol (MSDP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4 *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP routing protocols, including Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF). The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS IP Switching Configuration Guide, Release 12.4 *Cisco IOS IP Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP switching features, including Cisco Express Forwarding (CEF), fast switching, and Multicast Distributed Switching (MDS). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IPv6 Configuration Guide, Release 12.4 *Cisco IOS IPv6 Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP version 6 (IPv6), including IPv6 broadband access, IPv6 data-link layer, IPv6 multicast routing, IPv6 quality of service (QoS), IPv6 routing, IPv6 services and management, and IPv6 tunnel services. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Optimized Edge Routing Configuration Guide, Release 12.4 *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Optimized Edge Routing (OER) features, including OER prefix learning, OER prefix monitoring, OER operational modes, and OER policy configuration. The command reference provides detailed information about the commands used in the configuration guide.
Security and VPN	
Cisco IOS Security Configuration Guide, Release 12.4 *Cisco IOS Security Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring various aspects of security, including terminal access security, network access security, accounting, traffic filters, router access, and network data encryption with router authentication. The command reference provides detailed information about the commands used in the configuration guide.
QoS	
Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4 *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring quality of service (QoS) features, including traffic classification and marking, traffic policing and shaping, congestion management, congestion avoidance, and signaling. The command reference provides detailed information about the commands used in the configuration guide.
LAN Switching	
Cisco IOS LAN Switching Configuration Guide, Release 12.4 *Cisco IOS LAN Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to local-area network (LAN) switching features, including configuring routing between virtual LANs (VLANs) using Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, and IEEE 802.1Q encapsulation. The command reference provides detailed information about the commands used in the configuration guide.
Multiprotocol Label Switching (MPLS)	
Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4 *Cisco IOS Multiprotocol Label Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Multiprotocol Label Switching (MPLS), including MPLS Label Distribution Protocol, MPLS traffic engineering, and MPLS Virtual Private Networks (VPNs). The command reference provides detailed information about the commands used in the configuration guide.
Network Management	
Cisco IOS IP SLAs Configuration Guide, Release 12.4 *Cisco IOS IP SLAs Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the Cisco IOS IP Service Level Assurances (IP SLAs) feature. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS NetFlow Configuration Guide, Release 12.4 *Cisco IOS NetFlow Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to NetFlow features, including configuring NetFlow to analyze network traffic data, configuring NetFlow aggregation caches and export features, and configuring Simple Network Management Protocol (SNMP) and NetFlow MIB features. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Network Management Configuration Guide, Release 12.4 *Cisco IOS Network Management Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to network management features, including performing basic system management, performing troubleshooting and fault management, configuring Cisco Discovery Protocol (CDP), configuring Cisco Networking Services (CNS), configuring DistributedDirector, and configuring Simple Network Management Protocol (SNMP). The command reference provides detailed information about the commands used in the configuration guide.
Voice	
Cisco IOS Voice Configuration Library, Release 12.4 *Cisco IOS Voice Command Reference*, Release 12.4	The configuration library is a task-oriented collection of configuration guides, application guides, a troubleshooting guide, feature documents, a library preface, a voice glossary, and more. It also covers Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. In addition, the library includes documentation for IP telephony applications. The command reference provides detailed information about the commands used in the configuration library.
Wireless / Mobility	
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring a Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunication System (UMTS) network. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Mobile Wireless Home Agent Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Home Agent Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Mobile Wireless Home Agent, which is an anchor point for mobile terminals for which Mobile IP or Proxy Mobile IP services are provided. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Packet Data Serving Node (PDSN), a wireless gateway between the mobile infrastructure and standard IP networks that enables packet data services in a Code Division Multiple Access (CDMA) environment. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring Cisco IOS Radio Access Network products. The command reference provides detailed information about the commands used in the configuration guide.
Long Reach Ethernet (LRE) and Digital Subscriber Line (xDSL)	
Cisco IOS Broadband and DSL Configuration Guide, Release 12.4 *Cisco IOS Broadband and DSL Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring broadband access aggregation and digital subscriber line features. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Service Selection Gateway Configuration Guide, Release 12.4 *Cisco IOS Service Selection Gateway Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Service Selection Gateway (SSG) features, including subscriber authentication, service access, and accounting. The command reference provides detailed information about the commands used in the configuration guide.
Dial—Access	
Cisco IOS Dial Technologies Configuration Guide, Release 12.4 *Cisco IOS Dial Technologies Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring lines, modems, and ISDN services. This guide also contains information about configuring dialup solutions, including solutions for remote sites dialing in to a central office, Internet service providers (ISPs), ISP customers at home offices, enterprise WAN system administrators implementing dial-on-demand routing, and other corporate environments. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS VPDN Configuration Guide, Release 12.4 *Cisco IOS VPDN Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Virtual Private Dialup Networks (VPDNs), including information about Layer 2 tunneling protocols, client-initiated VPDN tunneling, NAS-initiated VPDN tunneling, and multihop VPDN. The command reference provides detailed information about the commands used in the configuration guide.
Asynchronous Transfer Mode (ATM)	
Cisco IOS Asynchronous Transfer Mode Configuration Guide, Release 12.4 *Cisco IOS Asynchronous Transfer Mode Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Asynchronous Transfer Mode (ATM), including WAN ATM, LAN ATM, and multiprotocol over ATM (MPOA). The command reference provides detailed information about the commands used in the configuration guide.
WAN	
Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 *Cisco IOS Wide-Area Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring wide-area network (WAN) features, including: Layer 2 Tunneling Protocol Version 3 (L2TPv3); Frame Relay; Link Access Procedure, Balanced (LAPB); and X.25. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
System Management	
Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to using Cisco IOS software to configure and maintain Cisco routers and access servers, including information about using the Cisco IOS command-line interface (CLI), loading and maintaining system images, using the Cisco IOS file system, using the Cisco IOS Web browser user interface (UI), and configuring basic file transfer services. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Interface and Hardware Component Configuration Guide, Release 12.4 *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring and managing interfaces and hardware components, including dial shelves, LAN interfaces, logical interfaces, serial interfaces, and virtual interfaces. The command reference provides detailed information about the commands used in the configuration guide.
IBM Technologies	
Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 *Cisco IOS Bridging Command Reference*, Release 12.4 *Cisco IOS IBM Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring: • Bridging features, including: transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and Token Ring Route Switch Module (TRRSM). • IBM network features, including: data-link switching plus (DLSw+), serial tunnel (STUN), and block serial tunnel (BSTUN); Logical Link Control, type 2 (LLC2), and Synchronous Data Link Control (SDLC); IBM Network Media Translation, including SDLC Logical Link Control (SDLLC) and Qualified Logical Link Control (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. The two command references provide detailed information about the commands used in the configuration guide.
Additional and Legacy Protocols	
Cisco IOS AppleTalk Configuration Guide, Release 12.4 *Cisco IOS AppleTalk Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the AppleTalk protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS DECnet Configuration Guide, Release 12.4 *Cisco IOS DECnet Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the DECnet protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS ISO CLNS Configuration Guide, Release 12.4 *Cisco IOS ISO CLNS Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring International Organization for Standardization (ISO) Connectionless Network Service (CLNS). The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS Novell IPX Configuration Guide, Release 12.4 *Cisco IOS Novell IPX Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the Novell Internetwork Packet Exchange (IPX) protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Terminal Services Configuration Guide, Release 12.4 *Cisco IOS Terminal Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring terminal services, including DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). The command reference provides detailed information about the commands used in the configuration guide.

Table 2 lists the documents and resources that support the Cisco IOS Release 12.4 software configuration guides and command references.

Table 2 Cisco IOS Release 12.4 Supporting Documents and Resources

Document Title	Description
Cisco IOS Master Commands List, Release 12.4	An alphabetical listing of all the commands documented in the Cisco IOS Release 12.4 command references.
Cisco IOS New, Modified, Replaced, and Removed Commands, Release 12.4	A listing of all the new, modified, replaced and removed commands since Cisco IOS Release 12.3, grouped by Release 12.3T maintenance release and ordered alphabetically within each group.
Cisco IOS New and Modified Commands, Release 12.3	A listing of all the new, modified, and replaced commands since Cisco IOS Release 12.2, grouped by Release 12.2T maintenance release and ordered alphabetically within each group.
Cisco IOS System Messages, Volume 1 of 2 *Cisco IOS System Messages, Volume 2 of 2*	Listings and descriptions of Cisco IOS system messages. Not all system messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
Cisco IOS Debug Command Reference, Release 12.4	An alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, and usage guidelines.
Release Notes, Release 12.4	A description of general release information, including information about supported platforms, feature sets, platform-specific notes, and Cisco IOS software defects.
Dictionary of Internetworking Terms and Acronyms	Compilation and definitions of the terms and acronyms used in the internetworking industry.

Table 2 Cisco IOS Release 12.4 Supporting Documents and Resources (continued)

Document Title	Description
RFCs	RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/
MIBs	MIBs are used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means 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 an SNMP community string to *public*, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

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

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords, and are used in contexts in which the italic document convention is not available, such as ASCII text.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:

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.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

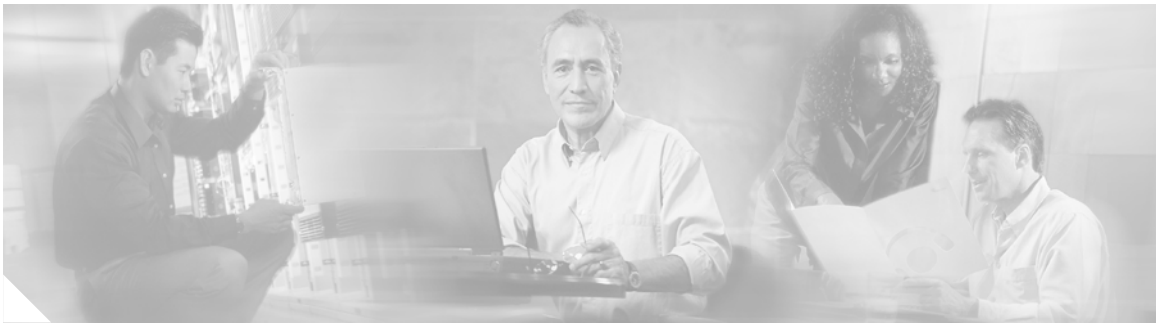
  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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



Using Cisco IOS Software for Release 12.4

This chapter provides helpful tips for understanding and configuring Cisco IOS software using the command-line interface (CLI). It contains the following sections:

For an overview of Cisco IOS software configuration, see the *Cisco IOS Configuration Fundamentals Configuration Guide.*

For information on the conventions used in the Cisco IOS software documentation set, see the "About Cisco IOS Software Documentation for Release 12.4" chapter.

Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS 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.

Table 1 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Table 1 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.
ROM monitor	From privileged EXEC mode, use the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

For more information on command modes, see the "Using the Cisco IOS Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Provides a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for "carriage return." On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 2 shows examples of how you can use the question mark (**?**) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface on a Cisco 7206 router that is running Cisco IOS Release 12.0(3).

Table 2 How to Find Command Options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to `Router#`.

`Router# configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router(config)#`.

`Router(config)# interface serial ?`
`  <0-6>  Serial interface number`
`Router(config)# interface serial 4 ?`
`  /`
`Router(config)# interface serial 4/ ?`
`  <0-3>  Serial interface number`
`Router(config)# interface serial 4/0 ?`
<cr>
`Router(config)# interface serial 4/0`
`Router(config-if)#`
	Enter interface configuration mode by specifying the serial interface that you want to configure using the **interface serial** global configuration command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.
	When the <cr> symbol is displayed, you can press **Enter** to complete the command.
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  load-interval  Specify interval for load calculation for an interface`
`  locaddr-priority  Assign a priority group`
`  logging  Configure logging for interface`
`  loopback  Configure internal loopback on an interface`
`  mac-address  Manually set interface MAC address`
`  mls  mls router sub/interface commands`
`  mpoa  MPOA interface configuration commands`
`  mtu  Set the interface Maximum Transmission Unit (MTU)`
`  netbios  Use a defined NETBIOS access list or enable name-caching`
`  no  Negate a command or set its defaults`
`  nrzi-encoding  Enable use of NRZI encoding`
`  ntp  Configure NTP`
`  .`
`  .`
`  .`
`Router(config-if)#`
	Enter **?** to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.

`Router(config-if)# ip ?`
`Interface IP configuration subcommands:`
`  access-group  Specify access control for packets`
`  accounting  Enable IP accounting on this interface`
`  address  Set the IP address of an interface`
`  authentication  authentication subcommands`
`  bandwidth-percent  Set EIGRP bandwidth limit`
`  broadcast-address  Set the broadcast address of an interface`
`  cgmp  Enable/disable CGMP`
`  directed-broadcast  Enable forwarding of directed broadcasts`
`  dvmrp  DVMRP interface commands`
`  hello-interval  Configures IP-EIGRP hello interval`
`  helper-address  Specify a destination address for UDP broadcasts`
`  hold-time  Configures IP-EIGRP hold time`
`  .`
`  .`
`  .`
`Router(config-if)# ip`
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ip address ?`
`  A.B.C.D  IP address`
`  negotiated  IP Address negotiated over PPP`
`Router(config-if)# ip address`
	Enter the command that you want to configure for the interface. This example uses the **ip address** command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword.
	A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

`Router(config-if)# ip address 172.16.0.1 ?`
`  A.B.C.D  IP subnet mask`
`Router(config-if)# ip address 172.16.0.1`
	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.
	A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?`
`  secondary  Make this IP address a secondary address`
`  <cr>`
`Router(config-if)# ip address 172.16.0.1 255.255.255.0`
	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.
	Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**.
	A <cr> is displayed; you can press **Enter** to complete the command, or you can enter another keyword.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0` `Router(config-if)#`	In this example, Enter is pressed to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands can also have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and

have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Saving Configuration Changes

Use the **copy system:running-config nvram:startup-config** command or the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

command | {**begin** | **include** | **exclude**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
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
```

For more information on the search and filter functionality, see the "Using the Cisco IOS Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

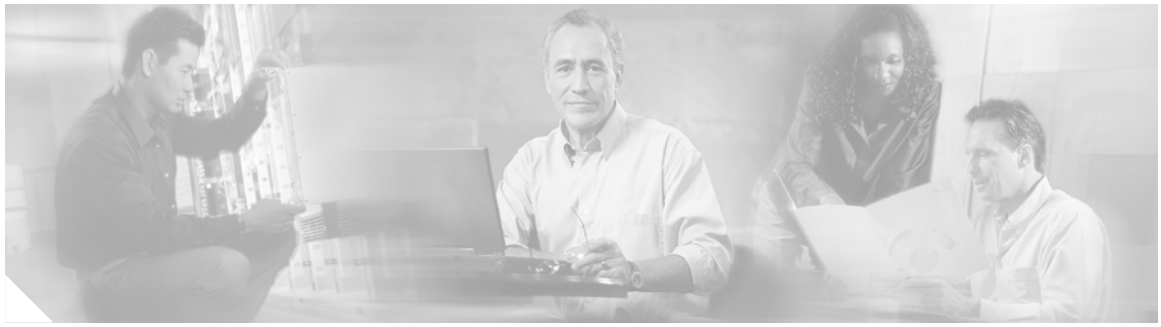
Finding Additional Feature Support Information

If you want to use a specific Cisco IOS software feature, you will need to determine in which Cisco IOS software images that feature is supported. Feature support in Cisco IOS software images is dependant on three main factors: the software version (called the “Release”), the hardware model (the “Platform” or “Series”), and the “Feature Set” (collection of specific features designed for a certain network environment). Although the Cisco IOS software documentation set documents feature support information for Release 12.4 as a whole, it does not generally provide specific hardware and feature set information.

To determine the correct combination of Release (software version), Platform (hardware version), and Feature Set needed to run a particular feature (or any combination of features), use Feature Navigator.

Feature Navigator is a web-based tool available on Cisco.com at http://www.cisco.com/go/fn. Feature Navigator is available only for registered users of Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

Software features may also have additional limitations or restrictions. For example, a minimum amount of system memory may be required. Or there may be known issues for features on certain platforms that have not yet been resolved (called “Caveats”). For the latest information about these limitations, see the release notes for the appropriate Cisco IOS software release. Release notes provide detailed installation instructions, new feature descriptions, system requirements, limitations and restrictions, caveats, and troubleshooting information for a particular software release.



Introduction

Novell Internet Packet Exchange (IPX) is derived from the Xerox Network Systems (XNS) Internet Datagram Protocol (IDP). One major difference between the IPX and XNS protocols is that they do not always use the same Ethernet encapsulation format. A second difference is that IPX uses Novell's proprietary Service Advertising Protocol (SAP) to advertise special network services.

Our implementation of Novell's IPX protocol has been certified as providing full IPX router functionality.

Use the commands in this book to configure and monitor Novell IPX networks. For IPX configuration information and examples, see the *Cisco IOS Novell IPX Configuration Guide*.

Note For all commands that previously used the keyword **novell**, this keyword has been changed to **ipx**. You can still use the keyword **novell** in all commands.

The Next Hop Resolution Protocol (NHRP) for IPX will no longer be available after Cisco IOS Release 12.2(13)T. NHRP for IPX documentation in the *Cisco IOS AppleTalk and Novell IPX Command Reference*, Release 12.2 can be accessed at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fatipx_r/ipx/index.htm

The following commands have been removed from documentation in Cisco IOS Software Release 12.2(13)T and will not appear in future releases of the Cisco IOS software documentation set:

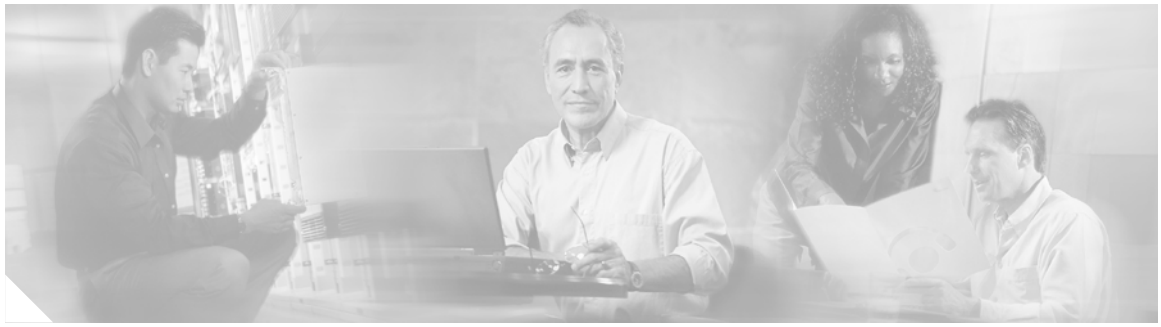
- clear ipx nhrp
- ipx nhrp authentication
- ipx nhrp holdtime
- ipx nhrp interest
- ipx nhrp map
- ipx nhrp max-send
- ipx nhrp network-id
- ipx nhrp nhs
- ipx nhrp record
- ipx nhrp responder
- ipx nhrp use
- show ipx nhrp
- show ipx nhrp traffic

The NetWare Link Services Protocol (NLSP) will no longer be available after Cisco IOS Release 12.2(13)T. NLSP documentation in the *Cisco IOS AppleTalk and Novell IPX Command Reference*, Release 12.2 can be accessed at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fatipx_r/ipx/index.htm

The following commands have been removed from documentation in Cisco IOS Release 12.2(13)T and will not appear in future releases of the Cisco IOS software documentation set:

- access-list (NLSP)
- area-address
- clear ipx nlsp neighbors
- clear ipx route
- clear ipx traffic
- deny (NLSP)
- distribute-list in
- distribute-list out
- distribute-sap-list in
- distribute-sap-list out
- ipx access-list
- ipx advertise-default-route-only
- ipx flooding-unthrottled
- ipx internal-network
- ipx nlsp csnp-interval
- ipx nlsp enable
- ipx nlsp hello-interval
- ipx nlsp hello-multiplier
- ipx nlsp lsp-interval
- ipx nlsp metric
- ipx nlsp multicast
- ipx nlsp priority
- ipx nlsp retransmit-interval
- ipx nlsp rip
- ipx nlsp sap
- ipx ping-default
- ipx potential-pseudonode
- ipx route
- ipx router
- log-adjacency-changes
- multicast (NLSP)
- permit (NLSP)
- redistribute

- route-aggregation (NLSP)
- show ipx nlsp database
- show ipx nlsp neighbors
- show ipx nlsp spf-log
- show ipx route
- show ipx traffic



Cisco IOS Novell IPX Commands

access-list (IPX extended)

To define an extended Novell IPX access list, use the extended version of the **access-list** command in global configuration mode. To remove an extended access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination.network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

no access-list *access-list-number* {**deny** | **permit**} *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination.network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description

access-list-number	Number of the access list. This is a number from 900 to 999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. Table 3 in the "Usage Guidelines" section lists some IPX protocol names and numbers.
source-network	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
.source-node	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
source-network-mask.	(Optional) Mask to be applied to the *source-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *source-node-mask* argument.
source-socket	(Optional) Socket name or number (hexadecimal) from which the packet is being sent. Table 4 in the "Usage Guidelines" section lists some IPX socket names and numbers.

destination.network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.destination-node	(Optional) Node on destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network-mask.	(Optional) Mask to be applied to the *destination-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *destination-node-mask* argument.
destination-socket	(Optional) Socket name or number (hexadecimal) to which the packet is being sent. Table 4 in the "Usage Guidelines" section lists some IPX socket names and numbers.
log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **log** keyword was added.
12.0(1)T	The following keyword and argument were added: • **time-range** • *time-range-name*

Usage Guidelines

Extended IPX access lists filter on protocol type. All other parameters are optional.

If a network mask is used, all other fields are required.

Use the **dipx access-group** command to assign an access list to an interface. You can apply only one extended or one standard access list to an interface. The access list filters all outgoing packets on the interface.

Note For some versions of NetWare, the protocol type field is not a reliable indicator of the type of packet encapsulated by the IPX header. In these cases, use the source and destination socket fields to make this determination. For additional information, contact Novell.

Table 3 lists some IPX protocol names and numbers. Table 4 lists some IPX socket names and numbers. For additional information about IPX protocol numbers and socket numbers, contact Novell.

Table 3 Some IPX Protocol Names and Numbers

IPX Protocol Number (Decimal)	IPX Protocol Name	Protocol (Packet Type)
-1	any	Wildcard; matches any packet type in 900 lists.
0		Undefined; refer to the socket number to determine the packet type.
1	rip	Routing Information Protocol (RIP).
4	sap	Service Advertising Protocol (SAP).
5	spx	Sequenced Packet Exchange (SPX).
17	ncp	NetWare Core Protocol (NCP).
20	netbios	IPX NetBIOS.

Table 4 Some IPX Socket Names and Numbers

IPX Socket Number (Hexadecimal)	IPX Socket Name	Socket
0	all	Wildcard used to match all sockets.
2	cping	Cisco IPX ping packet.
451	ncp	NetWare Core Protocol (NCP) process.
452	sap	Service Advertising Protocol (SAP) process.
453	rip	Routing Information Protocol (RIP) process.
455	netbios	Novell NetBIOS process.
456	diagnostic	Novell diagnostic packet.
457		Novell serialization socket.
4000-7FFF		Dynamic sockets; used by workstations for interaction with file servers and other network servers.
8000-FFFF		Sockets as assigned by Novell, Inc.

Table 4 Some IPX Socket Names and Numbers (continued)

IPX Socket Number (Hexadecimal)	IPX Socket Name	Socket
85BE	eigrp	IPX Enhanced Interior Gateway Routing Protocol (Enhanced IGRP).
9086	nping	Novell standard ping packet.

To delete an extended access list, specify the minimum number of keywords and arguments needed to delete the proper access list. For example, to delete the entire access list, use the following command:

no access-list *access-list-number*

To delete the access list for a specific protocol, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *protocol*

Examples

The following example denies access to all RIP packets from the RIP process socket on source network 1 that are destined for the RIP process socket on network 2. It permits all other traffic. This example uses protocol and socket names rather than hexadecimal numbers.

```
access-list  900  deny  -1 1 rip 2 rip
access-list  900  permit  -1
```

The following example permits type 2 packets from any socket from host 10.0000.0C01.5234 to access any sockets on any node on networks 1000 through 100F. It denies all other traffic (with an implicit deny all):

Note This type is chosen only as an example. The actual type to use depends on the specific application.

```
access-list 910 permit 2 10.0000.0C01.5234 0000.0000.0000 0
  1000.0000.0000.0000 F.FFFF.FFFF.FFFF 0
```

The following example provides a time range to the access list:

```
time-range no-spx
 periodic weekdays 8:00 to 18:00
!
ipx access-list extended test
 permit spx any all any all time-range no spx
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
cdeny (extended)	Sets conditions for a named IPX extended access list.
dipx access-group	Applies generic input and output filters to an interface.
iipx accounting	Defines an IPX access list by name.
ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
ipx output-network-filter	Controls which servers are included in the GNS responses sent by the Cisco IOS software.
ipx router-filter	Filters the routers from which packets are accepted.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list (IPX standard)

To define a standard IPX access list, use the standard version of the **access-list** command in global configuration mode. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *source-network*[.*source-node*[*source-node-mask*]] [*destination-network*[.*destination-node* [*destination-node-mask*]]]

no access-list *access-list-number* {**deny** | **permit**} *source-network*[.*source-node*[*source-node-mask*]] [*destination-network*[.*destination-node* [*destination-node-mask*]]]

Syntax Description

access-list-number	Number of the access list. This is a number from 800 to 899.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source-network	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*source-node*	(Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to *source-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*destination-node*	(Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to *destination-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Standard IPX access lists filter on the source network. All other parameters are optional.

Use the **ipx access-group** command to assign an access list to an interface. The access list filters all outgoing packets on the interface.

To delete a standard access list, specify the minimum number of keywords and arguments needed to delete the proper access list. For example, to delete the entire access list, use the following command:

no access-list *access-list-number*

To delete the access list for a specific network, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *source-network*

Examples

The following example denies access to traffic from all IPX networks (-1) to destination network 2:

```
access-list 800 deny -1 2
```

The following example denies access to all traffic from IPX address 1.0000.0c00.1111:

```
access-list 800 deny 1.0000.0c00.1111
```

The following example denies access from all nodes on network 1 that have a source address beginning with 0000.0c:

```
access-list 800 deny 1.0000.0c00.0000 0000.00ff.ffff
```

The following example denies access from source address 1111.1111.1111 on network 1 to destination address 2222.2222.2222 on network 2:

```
access-list 800 deny 1.1111.1111.1111 0000.0000.0000 2.2222.2222.2222 0000.0000.0000
```

or

```
access-list 800 deny 1.1111.1111.1111 2.2222.2222.2222
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
deny (standard)	Sets conditions for a named IPX access list.
dipx access-group	Applies generic input and output filters to an interface.
iipx accounting	Defines an IPX access list by name.
ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
ipx output-network-filter	Controls the list of networks included in routing updates sent out an interface.
ipx router-filter	Filters the routers from which packets are accepted.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list (SAP filtering)

To define an access list for filtering Service Advertising Protocol (SAP) requests, use the SAP filtering form of the **access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *network*[.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

no access-list *access-list-number* {**deny** | **permit**} *network*[.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

Syntax Description

access-list-number	Number of the SAP access list. This is a number from 1000 to 1099.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
network	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of –1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.node	(Optional) Node specified on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
network-mask.node-mask	(Optional) Mask to be applied to *network* and *node*. Place ones in the bit positions to be masked.
service-type	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services. Table 5 in the "Usage Guidelines" section lists examples of service types.
server-name	(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (" ") to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When configuring SAP filters for NetWare 3.11 and later servers, use the server's internal network and node number (the node number is always 0000.0000.0001) as its address in the **access-list** command. Do not use the *network.node* address of the particular interface board.

Table 5 lists some sample IPX SAP types. For more information about SAP types, contact Novell. Note that in the filter (specified by the *service-type* argument), we define a value of 0 to filter all SAP services. If, however, you receive a SAP packet with a SAP type of 0, this indicates an unknown service.

Table 5 Sample IPX SAP Services

Service Type (Hexadecimal)	Description
1	User
2	User group
3	Print server queue
4	File server
5	Job server
7	Print server
9	Archive server
A	Queue for job servers
21	Network Application Support Systems Network Architecture (NAS SNA) gateway
2D	Time Synchronization value-added process (VAP)
2E	Dynamic SAP
47	Advertising print server
4B	Btrieve VAP 5.0
4C	SQL VAP
7A	TES—NetWare for Virtual Memory System (VMS)
98	NetWare access server
9A	Named Pipes server
9E	Portable NetWare—UNIX
107	RCONSOLE
111	Test server
166	NetWare management (Novell's Network Management Station [NMS])
26A	NetWare management (NMS console)

To delete a SAP access list, specify the minimum number of keywords and arguments needed to delete the proper access list. For example, to delete the entire access list, use the following command:

no access-list *access-list-number*

To delete the access list for a specific network, use the following command:

no access-list *access-list-number* {**deny** | **permit**} *network*

Examples

The following access list blocks all access to a file server (service Type 4) on the directly attached network by resources on other Novell networks, but allows access to all other available services on the interface:

```
access-list 1001 deny -1 4
access-list 1001 permit -1
```

Related Commands

Command	Description
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
iipx accounting	Defines an IPX access list by name.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx output-gns-filter	Controls which servers are included in the GNS responses sent by the Cisco IOS software.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx router-sap-filter	Filters SAP messages received from a particular router.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
priority-list protocol	Establishes queueing priorities based on the protocol type.

clear ipx accounting

To delete all entries in the accounting database when IPX accounting is enabled, use the **clear ipx accounting** command in EXEC mode.

clear ipx accounting [**checkpoint**]

Syntax Description

checkpoint	(Optional) Clears the checkpoint database.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Specifying the **clear ipx accounting** command with no keywords copies the active database to the checkpoint database and clears all entries in the active database. When cleared, active database entries and static entries, such as those set by the **ipx accounting-list** command, are reset to zero. Dynamically found entries are deleted.

Any traffic that traverses the router after you issue the **clear ipx accounting** command is saved in the active database. Accounting information in the checkpoint database at that time reflects traffic prior to the most recent **clear ipx accounting** command.

You can also delete all entries in the active and checkpoint database by issuing the **clear ipx accounting** command twice in succession.

Examples

The following example first displays the contents of the active database before the contents are cleared. Then, the **clear ipx accounting** command clears all entries in the active database. As a result, the **show ipx accounting** command shows that there is no accounting information in the active database. Lastly, the **show ipx accounting checkpoint** command shows that the contents of the active database were copied to the checkpoint database when the **clear ipx accounting** command was issued.

```
Router# show ipx accounting

Source                  Destination               Packets           Bytes
0000C003.0000.0c05.6030 0000C003.0260.8c9b.4e33         72            2880
0000C001.0260.8c8d.da75 0000C003.0260.8c9b.4e33         14             624
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.da75         62            3110
0000C001.0260.8c8d.e7c6 0000C003.0260.8c9b.4e33         20            1470
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.e7c6         20            1470

Accounting data age is      6

Router# clear ipx accounting
Router# show ipx accounting

Source                  Destination               Packets           Bytes

Accounting data age is      0
```

```
Router# show ipx accounting checkpoint

Source                  Destination               Packets           Bytes
0000C003.0000.0c05.6030 0000C003.0260.8c9b.4e33         72            2880
0000C001.0260.8c8d.da75 0000C003.0260.8c9b.4e33         14             624
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.da75         62            3110
0000C001.0260.8c8d.e7c6 0000C003.0260.8c9b.4e33         20            1470
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.e7c6         20            1470

Accounting data age is      6
```

Related Commands

Command	Description
iipx accounting	Enables IPX accounting.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.
show ipx accounting	Displays the active or checkpoint accounting database.

clear ipx cache

To delete entries from the IPX fast-switching cache, use the **clear ipx cache** command in EXEC mode.

clear ipx cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **clear ipx cache** command clears entries used for fast switching and autonomous switching.

Examples

The following example deletes all entries from the IPX fast-switching cache:

```
clear ipx cache
```

Related Commands

Command	Description
ipx route-cache	Enables IPX fast switching.
show ipx cache	Displays the contents of the IPX fast-switching cache.

clear ipx sap

To clear IPX SAP entries from the IPX routing table, use the **clear ipx sap** command in EXEC mode.

clear ipx sap {***** | *sap-type* | *sap-name*}

Syntax Description

*****	Clears all IPX SAP service entries by marking them invalid.
sap-type	Specifies the type of services that you want to clear by marking as invalid. This is an four-digit hexadecimal number that uniquely identifies a service type. It can be a number in the range 1 to FFFF. You do not need to specify leading zeros in the service number. For example, for the service number 00AA, you can enter AA.
sap-name	Specifies a certain name of service so that you can clear IPX SAP service entries that begin with the specified name. The name can be any contiguous string of printable ASCII characters. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters. For example, to clear all services that begin with the name "accounting," enter the command clear ipx sap accounting* to clear all services that begin with the name "accounting". Use double quotation marks (“ ”) to enclose strings containing embedded spaces.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You can use the **clear ipx sap** command to research problems with the service table.

Examples

The following example clears all service entries from the IPX routing table:

```
clear ipx sap *
```

cdeny (extended)

To set conditions for a named IPX extended access list, use the **deny** command in access-list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

deny *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

no deny *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description

protocol	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. You can also use the word **any** to match all protocol types.
source-network	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword **any** to match all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
.source-node	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
source-network-mask.	(Optional) Mask to be applied to the *source-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *source-node-mask* argument.
source-socket	(Optional) Socket name or number (hexadecimal) from which the packet is being sent. You can also use the keyword **all** to match all sockets.

destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword **any** to match all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.destination-node	(Optional) Node on the destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network-mask.	(Optional) Mask to be applied to the *destination-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *destination-node-mask* argument.
destination-socket	(Optional) Socket name or number (hexadecimal) to which the packet is being sent.
log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(1)T	The following keyword and argument were added: • **time-range** • *time-range-name*

Usage Guidelines

Use this command following the **iipx accounting** command to specify conditions under which a packet cannot pass the named access list.

For additional information on IPX protocol names and numbers, and IPX socket names and numbers, see the **access-list** (IPX extended) command.

Examples

The following example creates an extended access list named *sal* that denies all SPX packets:

```
ipx access-list extended sal
 deny spx any all any all log
 permit any
```

The following example provides a time range to deny access :

```
time-range no-spx
 periodic weekdays 8:00 to 18:00
!
ipx access-list extended test
 permit spx any all any all time-range no spx
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
dipx access-group	Applies generic input and output filters to an interface.
iipx accounting	Defines an IPX access list by name.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
show ipx access-list	Displays the contents of all current IPX access lists.

deny (SAP filtering)

To set conditions for a named IPX SAP filtering access list, use the **deny** command in access-list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

deny *network*[.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

no deny *network*[.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

Syntax Description

network	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of –1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.node	(Optional) Node on *network*. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
network-mask.node-mask	(Optional) Mask to be applied to *network* and *node*. Place ones in the bit positions to be masked.
service-type	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.
server-name	(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use this command following the **iipx accounting** command to specify conditions under which a packet cannot pass the named access list.

For additional information on IPX SAP service types, see the **access-list** (SAP filtering) command.

Examples

The following example creates a SAP access list named *MyServer* that denies MyServer to be sent in SAP advertisements:

```
ipx access-list sap MyServer
```

```
deny 1234 4 MyServer
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
dipx access-group	Applies generic input and output filters to an interface.
iipx accounting	Defines an IPX access list by name.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
show ipx access-list	Displays the contents of all current IPX access lists.

deny (standard)

To set conditions for a named IPX access list, use the **deny** command in access-list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

deny *source-network*[.*source-node* [*source-node-mask*]] [*destination-network*[.*destination-node* [*destination-node-mask*]]]

no deny *source-network*[.*source-node* [*source-node-mask*]] [*destination-network*[.*destination-node* [*destination-node-mask*]]]

Syntax Description

source-network	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*source-node*	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*destination-node*	(Optional) Node on the destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use this command following the **iipx accounting** command to specify conditions under which a packet cannot pass the named access list.

For additional information on creating IPX access lists, see the **access-list** (IPX standard) command.

Examples

The following example creates a standard access list named *fred*. It denies communication with only IPX network number 5678.

```
ipx access-list standard fred
 deny 5678 any
 permit any
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
dipx access-group	Applies generic input and output filters to an interface.
iipx accounting	Defines an IPX access list by name.
prc-interval	Sets conditions for a named IPX access list.
show ipx access-list	Displays the contents of all current IPX access lists.

dipx access-group

To apply generic input and output filters to an interface, use the **ipx access-group** command in interface configuration mode. To remove filters, use the **no** form of this command.

ipx access-group {*access-list-number* | *name*} [**in** | **out**]

no ipx access-group {*access-list-number* | *name*} [**in** | **out**]

Syntax Description

access-list-number	Number of the access list. For standard access lists, *access-list-number* is a number from 800 to 899. For extended access lists, the value for the *access-list-number* argument is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
in	(Optional) Filters inbound packets. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list.
out	(Optional) Filters outbound packets. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. This is the default when you do not specify an input (**in**) or output (**out**) keyword in the command line.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Generic filters control which data packets an interface receives or sends out based on the packet source and destination addresses, IPX protocol type, and source and destination socket numbers. You use the standard **access-list** and extended **access-list** commands to specify the filtering conditions.

You can apply only one input filter and one output filter per interface or subinterface.

When you do not specify an input (**in**) or output (**out**) filter in the command line, the default is an output filter.

You cannot configure an output filter on an interface where autonomous switching is already configured. Similarly, you cannot configure autonomous switching on an interface where an output filter is already present. You cannot configure an input filter on an interface if autonomous switching is already configured on *any* interface. Likewise, you cannot configure input filters if autonomous switching is already enabled on *any* interface.

Examples

The following example applies access list 801 to Ethernet interface 1. Because the command line does not specify an input filter or output filter with the keywords **in** or **out**, the software assumes that it is an output filter.

```
interface ethernet 1
 ipx access-group 801
```

The following example applies access list 901 to Ethernet interface 0. The access list is an input filter access list as specified by the keyword **in**.

```
interface ethernet 0
 ipx access-group 901 in
```

To remove the input access list filter in the previous example, you must specify the **in** keyword when you use the **no** form of the command. The following example correctly removes the access list:

```
interface ethernet 0
 no ipx access-group 901 in
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
cdeny (extended)	Sets conditions for a named IPX extended access list.
deny (standard)	Sets conditions for a named IPX access list.
iipx accounting	Defines an IPX access list by name.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
prc-interval	Sets conditions for a named IPX access list.
priority-list protocol	Establishes queueing priorities based on the protocol type.

iipx accounting

To enable IPX accounting, use the **ipx accounting** command in interface configuration mode. To disable IPX accounting, use the **no** form of this command.

ipx accounting

no ipx accounting

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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 allows you to monitor both current traffic and traffic that has previously traversed the router.

IPX accounting statistics will be accurate even if IPX access lists are being used or if IPX fast switching is enabled. Enabling IPX accounting significantly decreases performance of a fast switched interface.

IPX accounting does not keep statistics if autonomous switching is enabled. In fact, IPX accounting is disabled if autonomous or SSE switching is enabled.

Examples

The following example enables IPX accounting on Ethernet interface 0:

```
interface ethernet 0
 ipx accounting
```

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.
show ipx accounting	Displays the active or checkpoint accounting database.

iipx ipxwan

To enable the IPX wide-area network (IPXWAN) protocol on a serial interface, use the **ipx ipxwan** command in interface configuration mode. To disable the IPXWAN protocol, use the **no** form of this command.

ipx ipxwan [*local-node* {*network-number* | **unnumbered**} *local-server-name retry-interval retry-limit*]

no ipx ipxwan

Syntax Description

local-node	(Optional) Primary network number of the router. This is an IPX network number that is unique across the entire internetwork. On NetWare 3.*x* servers, the primary network number is called the internal network number. The device with the higher number is determined to be the link master. A value of 0 causes the Cisco IOS software to use the configured internal network number.
network-number	(Optional) IPX network number to be used for the link if this router is the one determined to be the link master. The number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 0 to FFFFFFFD. A value 0 is equivalent to specifying the keyword **unnumbered**. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
unnumbered	(Optional) Specifies that no IPX network number is defined for the link. This is equivalent to specifying a value of 0 for the *network-number* argument.
local-server-name	(Optional) Name of the local router. It can be up to 47 characters long, and can contain uppercase letters, digits, underscores (_), hyphens (-), and at signs (@). On NetWare 3.*x* servers, this is the router name. For our routers, this is the name of the router as configured via the **hostname** command; that is, the name that precedes the standard prompt, which is an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode.
retry-interval	(Optional) Retry interval, in seconds. This interval defines how often the software will retry the IPXWAN start-up negotiation if a start-up failure occurs. Retries will occur until the retry limit defined by the *retry-limit* argument is reached. It can be a value from 1 to 600. The default is 20 seconds.
retry-limit	(Optional) Maximum number of times the software retries the IPXWAN start-up negotiation before taking the action defined by the **ipx ipxwan error** command. It can be a value from 1 through 100. The default is 3.

Defaults

IPXWAN is disabled.

If you enable IPXWAN, the default is **unnumbered**.

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keyword and argument were added: • **unnumbered** • *retry-interval*

Usage Guidelines If you omit all optional arguments and keywords, the **ipx ipxwan** command defaults to **ipx ipxwan 0 unnumbered** *router-name* (which is equivalent to **ipx ipxwan 0** *local-server-name*), where *router-name* is the name of the router as configured with the **hostname** global configuration command. For this configuration, the **show ipx interface** command displays `ipx ipxwan 0 0 local-server-name`.

If you enter a value of 0 for the *network-number* argument, the output of the **show running-config** EXEC command does not show the 0 but rather reports this value as "unnumbered."

The name of each device on each side of the link must be different.

IPXWAN is a start-up end-to-end options negotiations protocol. When a link comes up, the first IPX packets sent across are IPXWAN packets negotiating the options for the link. When the IPXWAN options have been successfully determined, normal IPX traffic starts. The three options negotiated are the link IPX network number, internal network number, and link delay (ticks) characteristics. The side of the link with the higher local-node number (internal network number) gives the IPX network number and delay to use for the link to the other side. Once IPXWAN finishes, no IPXWAN packets are sent unless link characteristics change or the connection fails. For example, if the IPX delay is changed from the default setting, an IPXWAN restart will be forced.

To enable the IPXWAN protocol on a serial interface, you must not have configured an IPX network number (using the **ipx network** interface configuration command) on that interface.

To control the delay on a link, use the **ipx delay** interface configuration command. If you issue this command when the serial link is already up, the state of the link will be reset and renegotiated.

Examples The following example enables IPXWAN on serial interface 0:

```
interface serial 0
 encapsulation ppp
 ipx ipxwan
```

The following example enables IPXWAN on serial interface 1 on device CHICAGO-AS. When the link comes up, CHICAGO-AS will be the master because it has a larger internal network number. It will give the IPX number 100 to NYC-AS to use as the network number for the link. The link delay, in ticks, will be determined by the exchange of packets between the two access servers.

On the local access server (CHICAGO-AS):

```
interface serial 1
 no ipx network
 encapsulation ppp
 ipx ipxwan 6666 100 CHICAGO-AS
```

On the remote router (NYC-AS):

```
interface serial 0
 no ipx network
 encapsulation ppp
 ipx ipxwan 1000 101 NYC-AS
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.
hostname	Specifies or modify the host name for the network server.
ipx delay	Sets the tick count.
iipx ipxwan	Sets an internal network number for use by IPXWAN.
ipx ipxwan error	Defines how to handle IPXWAN when IPX fails to negotiate properly at link startup.
ipx ipxwan static	Negotiates static routes on a link configured for IPXWAN.
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

iipx route-cache

To enable IPX fast switching, use the **ipx route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

ipx route-cache

no ipx route-cache

Syntax Description

This command has no arguments or keywords.

Defaults

Fast switching is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Fast switching allows higher throughput by switching packets using a cache created by previous transit packets. Fast switching is enabled by default on all interfaces that support fast switching, including Token Ring, Frame Relay, PPP, Switched Multimegabit Data Service (SMDS), and ATM.

On ciscoBus-2 interface cards, fast switching is done between all encapsulation types. On other interface cards, fast switching is done in all cases *except* the following: transfer of packets with sap encapsulation from an Ethernet, a Token Ring, or an FDDI network to a standard serial line.

You might want to disable fast switching in two situations. One is if you want to save memory on the interface cards: fast-switching caches require more memory than those used for standard switching. The second situation is to avoid congestion on interface cards when a high-bandwidth interface is writing large amounts of information to a low-bandwidth interface.

Note CiscoBus (Cbus) switching of IPX packets is not supported on the MultiChannel Interface Processor (MIP) interface.

Examples

The following example enables fast switching on an interface:

```
interface ethernet 0
 ipx route-cache
```

The following example disables fast switching on an interface:

```
interface ethernet 0
 no ipx route-cache
```

Related Commands

Command	Description
clear ipx cache	Deletes entries from the IPX fast-switching cache.
ipx watchdog	Causes the Cisco IOS software to respond to the watchdog packets of a server on behalf of a remote client.
show ipx cache	Displays the contents of the IPX fast-switching cache.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx accounting-list

To filter networks for which IPX accounting information is kept, use the **ipx accounting-list** command in global configuration mode. To remove the filter, use the **no** form of this command.

ipx accounting-list *number mask*

no ipx accounting-list *number mask*

Syntax Description

number	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.
mask	Network mask.

Defaults

No filters are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The source and destination addresses of each IPX packet traversing the router are compared with the network numbers in the filter. If there is a match, accounting information about the IPX packet is entered into the active accounting database. If there is no match, the IPX packet is considered to be a transit packet and may be counted, depending on the setting of the **ipx accounting-transits** global configuration command.

Examples

The following example adds all networks with IPX network numbers beginning with 1 to the list of networks for which accounting information is kept:

```
ipx accounting-list 1 0000.0000.0000
```

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
iipx accounting	Enables IPX accounting.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.
show ipx accounting	Displays the active or checkpoint accounting database.

ipx accounting-threshold

To set the maximum number of accounting database entries, use the **ipx accounting-threshold** command in global configuration mode. To restore the default, use the **no** form of this command.

ipx accounting-threshold *threshold*

no ipx accounting-threshold *threshold*

Syntax Description

threshold	Maximum number of entries (source and destination address pairs) that the Cisco IOS software can accumulate.

Defaults

512 entries

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The accounting threshold defines the maximum number of entries (source and destination address pairs) that the software accumulates. The threshold is designed to prevent IPX accounting from consuming all available free memory. This level of memory consumption could occur in a router that is switching traffic for many hosts. To determine whether overflows have occurred, use the **show ipx accounting** EXEC command.

Examples

The following example sets the IPX accounting database threshold to 500 entries:

```
ipx accounting-threshold 500
```

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
iipx accounting	Enables IPX accounting.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.
show ipx accounting	Displays the active or checkpoint accounting database.

ipx accounting-transits

To set the maximum number of transit entries that will be stored in the IPX accounting database, use the **ipx accounting-transits** command in global configuration mode. To disable this function, use the **no** form of this command.

ipx accounting-transits *count*

no ipx accounting-transits

Syntax Description

count	Number of transit entries that will be stored in the IPX accounting database.

Defaults

0 entries

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Transit entries are those that do not match any of the networks specified by **ipx accounting-list** global configuration commands. If you have not defined networks with **ipx accounting-list** commands, IPX accounting tracks all traffic through the interface (all transit entries) up to the accounting threshold limit.

Examples

The following example specifies a maximum of 100 transit records to be stored in the IPX accounting database:

```
ipx accounting-transits 100
```

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
show ipx accounting	Displays the active or checkpoint accounting database.

ipx advertise-default-route-only (RIP)

To advertise only the default RIP route via the specified network, use the **ipx advertise-default-route-only** command in interface configuration mode. To advertise all known RIP routes out the interface, use the **no** form of this command.

ipx advertise-default-route-only *network*

no ipx advertise-default-route-only *network*

Syntax Description

network	Number of the network through which to advertise the default route.

Defaults

All known routes are advertised out the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If you specify the **ipx advertise-default-route-only** command, only a known default RIP route is advertised out the interface; no other networks will be advertised. If you have a large number of routes in the routing table, for example, on the order of 1000 routes, none of them will be advertised out the interface. However, if the default route is known, it will be advertised. Nodes on the interface can still reach any of the 1000 networks via the default route.

Specifying the **ipx advertise-default-route-only** command results in a significant reduction in CPU processing overhead when there are many routes and many interfaces. It also reduces the load on downstream routers.

This command applies only to RIP. Enhanced IGRP is not affected when you enable this command. It continues to advertise all routes that it knows about.

Note Not all routers recognize and support the default route. Use this command with caution if you are not sure if all routers in your network support the default route.

Examples

The following example enables the advertising of the default route only:

```
interface ethernet 1
 ipx network 1234
 ipx advertise-default-route-only 1234
```

Related Commands

Command	Description
ipx default-route	Forwards to the default network all packets for which a route to the destination network is unknown.

ipx advertise-to-lost-route

To enable the sending of lost route mechanism packets, use the **ipx advertise-to-lost-route** command in global configuration mode. To disable the flooding of network down notifications that are not part of the Novell lost route algorithm, use the **no** form of this command.

ipx advertise-to-lost-route

no ipx advertise-to-lost-route

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You may reduce congestion on slow WAN links when there are many changes in an unstable network by turning off part of the Novell lost route algorithm. To turn off part of the Novell lost route algorithm, use the **no ipx advertise-to-lost-route** command.

Note The side effect of disabling the Novell lost route algorithm is longer convergence times in networks with multiple paths to networks.

Examples

The following example enables the Novell lost route algorithm:

```
ipx advertise-to-lost-route
```

ipx backup-server-query-interval (EIGRP)

To change the time between successive queries of each Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor's backup server table, use the **ipx backup-server-query-interval** command in global configuration mode. To restore the default time, use the **no** form of this command.

ipx backup-server-query-interval *interval*

no ipx backup-server-query-interval

Syntax Description

interval	Minimum time, in seconds, between successive queries of each Enhanced IGRP neighbor's backup server table. The default is 15 seconds.

Defaults

15 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A lower interval may use more CPU resources, but may cause lost server information to be retrieved from other servers' tables sooner.

Examples

The following example changes the server query time to 5 seconds:

```
ipx backup-server-query-interval 5
```

ipx bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ipx bandwidth-percent eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx bandwidth-percent eigrp *as-number percent*

no ipx bandwidth-percent eigrp *as-number*

Syntax Description

as-number	Autonomous system number.
percent	Percentage of bandwidth that Enhanced IGRP may use.

Defaults

50 percent

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Enhanced IGRP will use up to 50 percent of the bandwidth of a link, as defined by the **bandwidth** interface configuration command. This command may be used if some other fraction of the bandwidth is desired. Note that values greater than 100 percent may be configured; this may be useful if the bandwidth is set artificially low for other reasons.

Examples

The following example allows Enhanced IGRP to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 209:

```
interface serial 0
 bandwidth 56
 ipx bandwidth-percent eigrp 209 75
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipx router	Specifies the routing protocol to use.

ipx broadcast-fastswitching

To enable the router to fast switch IPX directed broadcast packets, use the **ipx broadcast-fastswitching** command in global configuration mode. To disable fast switching of IPX directed broadcast packets, use the **no** form of this command.

ipx broadcast-fastswitching

no ipx broadcast-fastswitching

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

The default behavior is to process switch directed broadcast packets.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

A directed broadcast is one with a network layer destination address of the form net.ffff.ffff.ffff. The **ipx broadcast-fastswitching** command permits the router to fast switch IPX directed broadcast packets. This may be useful in certain broadcast-based applications that rely on helpering.

Note that the router never uses autonomous switching for eligible directed broadcast packets, even if autonomous switching is enabled on the output interface. Also note that routing and service updates are always exempt from this treatment.

Examples

The following example enables the router to fast switch IPX directed broadcast packets:

```
ipx broadcast-fastswitching
```

ipx default-output-rip-delay

To set the default interpacket delay for RIP updates sent on all interfaces, use the **ipx default-output-rip-delay** command in global configuration mode. To return to the initial default delay value, use the **no** form of this command.

ipx default-output-rip-delay *delay*

no ipx default-output-rip-delay

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. The **ipx default-output-rip-delay** command sets a default interpacket delay for all interfaces.

The system uses the delay specified by the **ipx default-output-rip-delay** command for periodic and triggered routing updates when no delay is set for periodic and triggered routing updates on an interface. When you set a delay for triggered routing updates, the system uses the delay specified by the **ipx default-output-rip-delay** command for only the periodic routing updates sent on all interfaces.

To set a delay for triggered routing updates, see the **ipx triggered-rip-delay** or **ipx default-triggered-rip-delay** commands.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Examples

The following example sets a default interpacket delay of 55 ms for RIP updates sent on all interfaces:

```
ipx default-output-rip-delay 55
```

Related Commands

Command	Description
ipx default-triggered-rip-delay	Sets the default interpacket delay for triggered RIP updates sent on all interfaces.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx triggered-rip-delay	Sets the interpacket delay for triggered RIP updates sent on a single interface.

ipx default-output-sap-delay

To set a default interpacket delay for SAP updates sent on all interfaces, use the **ipx default-output-sap-delay** command in global configuration mode. To return to the initial default delay value, use the **no** form of this command.

ipx default-output-sap-delay *delay*

no ipx default-output-sap-delay

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. The **ipx default-output-sap-delay** command sets a default interpacket delay for all interfaces.

The system uses the delay specified by the **ipx default-output-sap-delay** command for periodic and triggered SAP updates when no delay is set for periodic and triggered updates on an interface. When you set a delay for triggered updates, the system uses the delay specified by the **ipx default-output-sap-delay** command only for the periodic SAP updates sent on all interfaces.

To set a delay for triggered updates, see the **ipx triggered-sap-delay** or **ipx default-triggered-sap-delay** commands.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these servers.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 interfaces.

Examples

The following example sets a default interpacket delay of 55 ms for SAP updates sent on all interfaces:

```
ipx default-output-sap-delay 55
```

Related Commands

Command	Description
ipx default-triggered-sap-delay	Sets the default interpacket delay for triggered SAP updates sent on all interfaces.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx triggered-sap-delay	Sets the interpacket delay for triggered SAP updates sent on a single interface.

ipx default-route

To forward to the default network all packets for which a route to the destination network is unknown, use the **ipx default-route** command in global configuration mode. To disable the use of the default network, use the **no** form of this command.

ipx default-route

no ipx default-route

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled. All packets for which a route to the destination is unknown are forwarded to the default network, which is -2 (0xFFFFFFFE).

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

When you use the **no ipx default-route** command, Cisco IOS software no longer uses -2 as the default network. Instead, the software interprets -2 as a regular network and packets for which a route to the destination network is unknown are dropped.

Examples

The following example disables the forwarding of packets towards the default network:

```
no ipx default-route
```

Related Commands

Command	Description
ipx advertise-default-route-only	Advertises only the default RIP route through the specified network.

ipx default-triggered-rip-delay

To set the default interpacket delay for triggered RIP updates sent on all interfaces, use the **ipx default-triggered-rip-delay** command in global configuration mode. To return to the system default delay, use the **no** form of this command.

ipx default-triggered-rip-delay *delay*

no ipx default-triggered-rip-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. A triggered routing update is one that the system sends in response to a "trigger" event, such as a request packet, interface up/down, route up/down, or server up/down.

The **ipx default-triggered-rip-delay** command sets the default interpacket delay for triggered routing updates sent on all interfaces. On a single interface, you can override this global default delay for triggered routing updates using the **ipx triggered-rip-delay** interface command.

The global default delay for triggered routing updates overrides the delay value set by the **ipx output-rip-delay** or **ipx broadcast-fastswitching** command for triggered routing updates.

If the delay value set by the **ipx output-rip-delay** or **ipx broadcast-fastswitching** command is high, then we strongly recommend a low delay value for triggered routing updates so that updates triggered by special events are sent in a more timely manner than periodic routing updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is approximately 100 ms.

When you do not set the interpacket delay for triggered routing updates, the system uses the delay specified by the **ipx output-rip-delay** or **ipx broadcast-fastswitching** command for both periodic and triggered routing updates.

When you use the **no** form of the **ipx default-triggered-rip-delay** command, the system uses the delay set by the **ipx output-rip-delay** or **ipx broadcast-fastswitching** command for triggered RIP updates, if set. Otherwise, the system uses the initial default delay as described in the "Defaults" section.

This command is also useful on limited bandwidth point-to-point links, or X.25 and Frame Relay multipoint interfaces.

Examples

The following example sets an interpacket delay of 55 ms for triggered routing updates sent on all interfaces:

```
ipx default-triggered-rip-delay 55
```

Related Commands

Command	Description
ipx broadcast-fastswitching	Sets the default interpacket delay for RIP updates sent on all interfaces
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx triggered-rip-delay	Sets the interpacket delay for triggered RIP updates sent on a single interface.

ipx default-triggered-rip-holddown

To set the global default for the **ipx triggered-rip-holddown** interface configuration command, use the **ipx default-triggered-rip-holddown** command in global configuration mode. To re-establish the default value of 55 milliseconds, use the **no** form of this command.

ipx default-triggered-rip-holddown *milliseconds*

no ipx default-triggered-rip-holddown *milliseconds*

Syntax Description

milliseconds	Specifies how many milliseconds (ms) a router will wait before sending the triggered route change information.

Defaults

55 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Setting the global default for the **ipx triggered-rip-holddown** interface configuration command saves you from needing to configure the command on every interface.

Examples

The following example shows the hold-down time changed to 100 milliseconds:

```
ipx default-triggered-rip-holddown 100
```

Related Commands

Command	Description
ipx default-triggered-sap-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-sap-holddown** command.
ipx triggered-rip-holddown	Sets an amount of time an IPX RIP process will wait before sending flashes about RIP changes.
ipx triggered-sap-holddown	Sets an amount of time an IPX SAP process will wait before sending flashes about SAP changes.

ipx default-triggered-sap-delay

To set the default interpacket delay for triggered SAP updates sent on all interfaces, use the **ipx default-triggered-sap-delay** command in global configuration mode. To return to the system default delay, use the **no** form of this command.

ipx default-triggered-sap-delay *delay*

no ipx default-triggered-sap-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. A triggered SAP update is one that the system sends in response to a "trigger" event, such as a request packet, interface up/down, route up/down, or server up/down.

The **ipx default-triggered-sap-delay** command sets the default interpacket delay for triggered SAP updates sent on all interfaces. On a single interface, you can override this global default delay for triggered updates using the **ipx triggered-sap-delay** interface command.

The global default delay for triggered updates overrides the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered updates.

If the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command is high, then we strongly recommend a low delay value for triggered updates so that updates triggered by special events are sent in a more timely manner than periodic updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX servers.

The default delay on a NetWare 3.11 server is approximately 100 ms.

When you do not set the interpacket delay for triggered SAP updates, the system uses the delay specified by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for both periodic and triggered SAP updates.

When you use the **no** form of the **ipx default-triggered-sap-delay** command, the system uses the delay set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered SAP updates, if set. Otherwise, the system uses the initial default delay as described in the "Defaults" section.

This command is also useful on limited bandwidth point-to-point links, or X.25 and Frame Relay multipoint interfaces.

Examples

The following example sets an interpacket delay of 55 ms for triggered SAP updates sent on all interfaces:

```
ipx default-triggered-sap-delay 55
```

Related Commands

Command	Description
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx triggered-sap-delay	Sets the interpacket delay for triggered SAP updates sent on a single interface.

ipx default-triggered-sap-holddown

To set the global default for the **ipx triggered-sap-holddown** interface configuration command, use the **ipx default-triggered-sap-holddown** command in global configuration mode. To re-establish the default value of 55 milliseconds, use the **no** form of this command.

ipx default-triggered-sap-holddown *milliseconds*

no ipx default-triggered-sap-holddown *milliseconds*

Syntax Description

milliseconds	Specifies how many milliseconds (ms) a router will wait before sending the triggered route change information.

Defaults

55 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Setting the global default for the **ipx triggered-sap-holddown** interface configuration command saves you from needing to configure a **triggered-sap-holddown** command on every interface.

Examples

The following example shows the hold-down time changed to 100 ms:

```
ipx default-triggered-sap-holddown 100
```

Related Commands

Command	Description
ipx default-triggered-rip-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-rip-holddown** command.
ipx triggered-rip-holddown	Sets an amount of time an IPX RIP process will wait before sending flashes about RIP changes.
ipx triggered-sap-holddown	Sets an amount of time an IPX SAP process will wait before sending flashes about SAP changes.

ipx delay

To set the tick count, use the **ipx delay** command in interface configuration mode. To reset the default increment in the delay field, use the **no** form of this command.

ipx delay *ticks*

no ipx delay

Syntax Description

ticks	Number of IBM clock ticks of delay to use. One clock tick is 1/18 of a second (approximately 55 ms).

Defaults

The IPX default delay is determined from the interface delay configured on the interface with the **delay** command. It is (interface delay + 333) / 334. Therefore, unless you change the delay by a value greater than 334, you will not notice a difference.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx delay** command sets the count used in the IPX RIP delay field, which is also known as the *ticks* field.

IPXWAN links determine their delay dynamically. If you do not specify the **ipx delay** command on an interface and you have not changed the interface delays with the **interface delay** interface configuration command, all LAN interfaces have a delay of 1 and all WAN interfaces have a delay of 6. The preferred method of adjusting delays is to use the **ipx delay** command, not the **interface delay** command. The **show ipx interface** EXEC command display only the delay value configured with the **ipx delay** command.

With IPXWAN, if you change the interface delay with the **interface delay** command, the **ipx delay** command uses that delay when calculating a delay to use. Also, when changing delays with IPXWAN, the changes affect only the link's calculated delay on the side considered to be the master.

Leaving the delay at its default value is sufficient for most interfaces.

Examples

The following example changes the delay for serial interface 0 to 10 ticks:

```
interface serial 0
 ipx delay 10
```

Related Commands

Command	Description
delay	Sets a delay value for an interface.
ipx maximum-paths	Sets the maximum number of equal-cost paths the Cisco IOS software uses when forwarding packets.
ipx output-network-filter	Controls the list of networks included in routing updates sent out an interface.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.

ipx down

To administratively shut down an IPX network, use the **ipx down** command in interface configuration mode. To restart the network, use the **no** form of this command.

ipx down *network*

no ipx down

Syntax Description

network	Number of the network to shut down. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx down** command administratively shuts down the specified network. The network still exists in the configuration, but is not active. When shutting down, the network sends out update packets informing its neighbors that it is shutting down. This allows the neighboring systems to update their routing, SAP, and other tables without having to wait for routes and services learned via this network to time out.

To shut down an interface in a manner that is considerate of one's neighbor, use **ipx down** before using the **shutdown** command.

Examples

The following example administratively shuts down network AA on Ethernet interface 0:

```
interface ethernet 0
 ipx down AA
```

ipx eigrp-sap-split-horizon

To configure Enhanced Interior Gateway Routing Protocol (EIGRP) SAP split horizon, use the **ipx eigrp-sap-split-horizon** command in global configuration mode. To revert to the default, use the **no** form of this command.

ipx eigrp-sap-split-horizon

no ipx eigrp-sap-split-horizon

Syntax Description

This command has no argument or keywords.

Defaults

Enabled on LANs and disabled on WANs.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

When split horizon is enabled, Enhanced IGRP SAP update and packets are not sent back to the same interface where the SAP is received from. This reduces the number of Enhanced IGRP packets on the network.

Split horizon blocks information about SAPs from being advertised by a router about any interface from which that information originated. Typically, this behavior optimizes communication among multiple routers, particularly when links are broken. However, with nonbroadcast networks, such as Frame Relay and SMDS, situations can arise for which this behavior is less than ideal. For these situations, you may wish to disable split horizon.

Note When the **ipx sap-incremental split-horizon** interface configuration command is configured, it takes precedence over the **ipx eigrp-sap-split-horizon** command.

Examples

The following example disables split horizon on the router:

```
no ipx eigrp-sap-split-horizon
```

Related Commands

Command	Description
ipx sap-incremental split-horizon	Configures incremental SAP split horizon.
ipx split-horizon eigrp	Configures split horizon.
show ipx eigrp neighbors	Displays the neighbors discovered by Enhanced IGRP.

ipx encapsulation

To set the Ethernet frame type of the interface to that of the local file server, use the **ipx encapsulation** command in interface configuration mode. To reset the frame type to the default, use the **no** form of this command.

ipx encapsulation *encapsulation-type*

no ipx encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	(Required) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 6.

Table 6 describes the types of encapsulation available for specific interfaces.

Table 6 Encapsulation Types

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Uses Novell's Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For serial interfaces only—Uses High-Level Data Link Control (HDLC) encapsulation.
novell-ether	For Ethernet interfaces only—Uses Novell's Ethernet_802.3 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Uses Novell's FDDI_RAW encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.
sap	For Ethernet interfaces—Uses Novell's Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by NetWare Version 3.12 and 4.0. For Token Ring interfaces—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header. For FDDI interfaces—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.
snap	For Ethernet interfaces—Uses Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Subnetwork Access Protocol (SNAP) LLC header. For Token Ring and FDDI interfaces—This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.

Defaults

novell-ether

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can configure an IPX network on any supported interface as long as all the networks on the same physical interface use a distinct encapsulation type. For example, you can configure up to four IPX networks on a single Ethernet cable because Ethernet supports four encapsulation types.

The interface processes only packets with the correct encapsulation and the correct network number. IPX networks that use other encapsulations can be present on the physical network. The only effect on the router is that it uses some processing time to examine packets to determine whether they have the correct encapsulation.

Note If you have not yet enabled IPX routing on the interface, you can save time by using the **ipx network** command, which allows you to enable IPX routing on the interface and select the encapsulation type in one command.

To determine the frame type of the server, use the **config** command at the prompt of the local server.

Examples

The following example sets the frame type to Novell Ethernet II:

```
interface ethernet 0
 ipx encapsulation arpa
```

Related Commands

Command	Description
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).
ipx routing	Enables IPX routing.

ipx gns-reply-disable

To disable the sending of replies to IPX Get Nearest Server (GNS) queries, use the **ipx gns-reply-disable** command in interface configuration mode. To return to the default, use the **no** form of this command.

ipx gns-reply-disable

no ipx gns-reply-disable

Syntax Description

This command has no arguments or keywords.

Defaults

Replies are sent to IPX GNS queries.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example disables the sending of replies to GNS queries on Ethernet interface 0:

```
interface ethernet 0
 ipx gns-reply-disable
```

Related Commands

Command	Description
ipx gns-response-delay	Changes the delay when responding to GNS requests.

ipx gns-response-delay

To change the delay when responding to Get Nearest Server (GNS) requests, use the **ipx gns-response-delay** command in global or interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx gns-response-delay [*milliseconds*]

no ipx gns-response-delay

Syntax Description

milliseconds	(Optional) Time, in milliseconds (ms), that the Cisco IOS software waits after receiving a GNS request from an IPX client before responding with a server name to that client. The default is zero, which indicates no delay.

Defaults

0 (no delay)

Command Modes

Global configuration (globally changes the delay for the router)
Interface configuration (overrides the globally configured delay for an interface)

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command can be used in two modes: global configuration or interface configuration. In both modes, the command syntax is the same. A delay in responding to GNS requests might be imposed so that, in certain topologies, any local Novell IPX servers respond to the GNS requests before our software does. It is desirable to have these end-host server systems get their reply to the client before the router does because the client typically takes the first response, not the best response. In this case the best response is the one from the local server.

NetWare 2.*x* has a problem with dual-connected servers in parallel with a router. If you are using this version of NetWare, you should set a GNS delay. A value of 500 ms is recommended.

In situations in which servers are always located across routers from their clients, there is no need for a delay to be imposed.

Examples

The following example sets the delay in responding to GNS requests to 500 ms (0.5 seconds):

```
ipx gns-response-delay 500
```

Related Commands

Command	Description
ipx gns-reply-disable	Disables the sending of replies to IPX GNS queries.
ipx rip-response-delay	Changes the delay when responding to RIP requests.

ipx gns-round-robin

To rotate using a round-robin selection method through a set of eligible servers when responding to Get Nearest Server (GNS) requests, use the **ipx gns-round-robin** command in global configuration mode. To use the most recently learned server, use the **no** form of this command.

ipx gns-round-robin

no ipx gns-round-robin

Syntax Description

This command has no arguments or keywords.

Defaults

The most recently learned eligible server is used.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

In the normal server selection process, requests for service are responded to with the most recently learned, closest server. If you enable the round-robin method, the Cisco IOS software maintains a list of the nearest servers eligible to provide specific services. It uses this list when responding to GNS requests. Responses to requests are distributed in a round-robin fashion across all active IPX interfaces on the router.

Eligible servers are those that satisfy the "nearest" requirement for a given request and that are not filtered either by a SAP filter or by a GNS filter.

Examples

The following example responds to GNS requests using a round-robin selection method from a list of eligible nearest servers:

```
ipx gns-round-robin
```

Related Commands

Command	Description
ipx output-gns-filter	Controls which servers are included in the GNS responses sent by the Cisco IOS software.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.

ipx hello-interval eigrp

To configure the interval between Enhanced Interior Gateway Routing Protocol (EIGRP) hello packets, use the **ipx hello-interval eigrp** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx hello-interval eigrp *autonomous-system-number seconds*

no ipx hello-interval eigrp *autonomous-system-number seconds*

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can a number from 1 to 65,535.
seconds	Interval between hello packets, in seconds. The default interval is 5 seconds, which is one-third of the default hold time.

Defaults

For low-speed NBMA networks: 60 seconds
For all other networks: 5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The default of 60 seconds applies only to low-speed, nonbroadcast, multiaccess (NBMA) media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for purposes of Enhanced IGRP, Frame Relay and SMDS networks may or may not be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise they are considered not to be NBMA.

Examples

The following example changes the hello interval to 10 seconds:

```
interface ethernet 0
 ipx network 10
 ipx hello-interval eigrp 4 10
```

Related Commands

Command	Description
ipx hold-down eigrp	Specifies the length of time a lost Enhanced IGRP route is placed in the hold-down state.

ipx helper-address

To forward broadcast packets to a specified server, use the **ipx helper-address** command in interface configuration mode. To disable this function, use the **no** form of this command.

ipx helper-address *network.node*

no ipx helper-address *network.node*

Syntax Description

network	Network on which the target IPX server resides. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of -1 indicates all-nets flooding. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.node	Node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). A node number of FFFF.FFFF.FFFF matches all servers.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Routers normally block all broadcast requests and do not forward them to other network segments. This is done to prevent the degradation of performance over the entire network. The **ipx helper-address** command allows broadcasts to be forwarded to other networks. This is useful when a network segment does not have an end-host capable of servicing a particular type of broadcast request. This command lets you forward the broadcasts to a server, network, or networks that can process them. Incoming unrecognized broadcast packets that match the access list created with the **ipx helper-list** command, if it is present, are forwarded.

You can specify multiple **ipx helper-address** commands on a given interface.

The Cisco IOS software supports all-networks flooded broadcasts (sometimes referred to as *all-nets flooding*). These are broadcast messages that are forwarded to all networks. To configure the all-nets flooding, define the IPX helper address for an interface as follows:

```
ipx helper-address -1.FFFF.FFFF.FFFF
```

On systems configured for IPX routing, this helper address is displayed as follows (via the **show ipx interface** command):

```
FFFFFFFF.FFFF.FFFF.FFFF
```

Although our software takes care to keep broadcast traffic to a minimum, some duplication is unavoidable. When loops exist, all-nets flooding can propagate bursts of excess traffic that will eventually age out when the hop count reaches its limit (16 hops). Use all-nets flooding carefully and only when necessary. Note that you can apply additional restrictions by defining a helper list.

To forward type 20 packets to only those nodes specified by the **ipx helper-address** command, use the **ipx helper-address** command in conjunction with the **ipx type-20-helpered** global configuration command.

To forward type 20 packets to all nodes on the network, use the **ipx type-20-propagation** command. See the **ipx type-20-propagation** command for more information.

Examples

The following example forwards all-nets broadcasts on Ethernet interface 0 (except type 20 propagation packets) are forwarded to IPX server 00b4.23cd.110a on network bb:

```
interface ethernet 0
 ipx helper-address bb.00b4.23cd.110a
```

Related Commands

Command	Description
ipx helper-list	Assigns an access list to an interface to control broadcast traffic (including type 20 propagation packets).
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx helper-list

To assign an access list to an interface to control broadcast traffic (including type 20 propagation packets), use the **ipx helper-list** command in interface configuration mode. To remove the access list from an interface, use the **no** form of this command.

ipx helper-list {*access-list-number* | *name*}

no ipx helper-list {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, the value for the *access-list-number* argument is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No access list is preassigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx helper-list** command specifies an access list to use in forwarding broadcast packets. One use of this command is to prevent client nodes from discovering services they should not use.

Because the destination address of a broadcast packet is by definition the broadcast address, this command is useful only for filtering based on the source address of the broadcast packet.

The helper list, if present, is applied to both all-nets broadcast packets and type 20 propagation packets.

The helper list on the input interface is applied to packets before they are output via either the helper address or type 20 propagation packet mechanism.

Examples

The following example assigns access list 900 to Ethernet interface 0 to control broadcast traffic:

```
interface ethernet 0
 ipx helper-list 900
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-list	Defines an IPX access list by name.
ipx helper-address	Forwards broadcast packets to a specified server.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
prc-interval	Sets conditions for a named IPX access list.

ipx hold-down eigrp

To specify the length of time a lost Enhanced Interior Gateway Routing Protocol (EIGRP) route is placed in the hold-down state, use the **ipx hold-down eigrp** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipx hold-down eigrp *autonomous-system-number seconds*

no ipx hold-down eigrp *autonomous-system-number seconds*

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
seconds	Hold-down time, in seconds. The default hold time is 5 seconds.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When an Enhanced IGRP route is lost, it is placed into a hold-down state for a period of time. The purpose of the hold-down state is to ensure the validity of any new routes for the same destination.

The amount of time a lost Enhanced IGRP route is placed in the hold-down state is configurable. Set the amount of time to a value longer than the default of 5 seconds if your network requires a longer time for the unreachable route information to propagate.

Examples

The following example changes the hold-down time for autonomous system from 4 to 45 seconds:

```
interface ethernet 0
 ipx network 10
 ipx hold-down eigrp 4 45
```

ipx hold-time eigrp

To specify the length of time for which a neighbor should consider Enhanced IGRP hello packets valid, use the **ipx hold-time eigrp** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipx hold-time eigrp *autonomous-system-number seconds*

no ipx hold-time eigrp *autonomous-system-number seconds*

Syntax Description

autonomous-system-number	Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
seconds	Hold time, in seconds. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The default hold time is 15 seconds, which is three times the hello interval.

Defaults

For low-speed nonbroadcast, multiaccess (NBMA) networks: 180 seconds
For all other networks: 15 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If the current value for the hold time is less than two times the interval between hello packets, the hold time will be reset to three times the hello interval.

If a router does not receive a hello packet within the specified hold time, routes through the router are considered available.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds applies only to low-speed NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command.

Examples

The following example changes the hold time to 45 seconds:

```
interface ethernet 0
 ipx network 10
 ipx hold-time eigrp 4 45
```

Related Commands

Command	Description
ipx hello-interval eigrp	Configures the interval between Enhanced IGRP hello packets.

ipx input-network-filter (RIP)

To control which networks are added to the Cisco IOS software routing table, use the **ipx input-network-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx input-network-filter {*access-list-number* | *name*}

no ipx input-network-filter {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, the value for the *access-list-number* argument is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx input-network-filter** command controls which networks are added to the routing table based on the networks learned in incoming IPX routing updates (RIP updates) on the interface.

You can issue only one **ipx input-network-filter** command on each interface.

Examples

In the following example, access list 876 controls which networks are added to the routing table when IPX routing updates are received on Ethernet interface 1. Routing updates for network 1b will be accepted. Routing updates for all other networks are implicitly denied and are not added to the routing table.

```
access-list 876 permit 1b
interface ethernet 1
 ipx input-network-filter 876
```

The following example is a variation of the preceding that explicitly denies network 1a and explicitly allows updates for all other networks:

```
access-list 876 deny 1a
access-list 876 permit -1
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-list	Defines an IPX access list by name.
ipx output-network-filter	Controls the list of networks included in routing updates sent out an interface.
ipx router-filter	Filters the routers from which packets are accepted.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
prc-interval	Sets conditions for a named IPX access list.

ipx input-sap-filter

To control which services are added to the Cisco IOS software SAP table, use the **ipx input-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx input-sap-filter {*access-list-number* | *name*}

no ipx input-sap-filter {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the SAP access list. All incoming packets are filtered by the entries in this access list. The argument *access-list-number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx input-sap-filter** command filters all incoming service advertisements received by the router. This is done prior to accepting information about a service.

You can issue only one **ipx input-sap-filter** command on each interface.

When configuring SAP filters for NetWare 3.11 and later servers, use the server's internal network and node number (the node number is always 0000.0000.0001) as its address in the **access-list** (SAP filtering) command. Do not use the *network.node* address of the particular interface board.

Examples

The following example denies service advertisements about the server at address 3c.0800.89a1.1527, but accepts information about all other services on all other networks:

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
!
interface ethernet 0
 ipx input-sap-filter 1000
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx router-sap-filter	Filters SAP messages received from a particular router.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx ipxwan error

To define how to handle IPX wide-area network (IPXWAN) when IPX fails to negotiate properly at link startup, use the **ipx ipxwan error** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipx ipxwan error [**reset** | **resume** | **shutdown**]

no ipx ipxwan error [**reset** | **resume** | **shutdown**]

Syntax Description

reset	(Optional) Resets the link when negotiations fail. This is the default action.
resume	(Optional) When negotiations fail, IPXWAN ignores the failure, takes no special action, and resumes the start-up negotiation attempt.
shutdown	(Optional) Shuts down the link when negotiations fail.

Defaults

The link is reset.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use the **ipx ipxwan error** command to define what action to take if the IPXWAN startup negotiation fails.

Examples

In the following example, the serial link will be shut down if the IPXWAN startup negotiation fails after three attempts spaced 20 seconds apart:

```
interface serial 0
 encapsulation ppp
 ipx ipxwan
 ipx ipxwan error shutdown
```

Related Commands

Command	Description
iipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx ipxwan static	Negotiates static routes on a link configured for IPXWAN.

ipx ipxwan static

To negotiate static routes on a link configured for IPX wide-area network (IPXWAN), use the **ipx ipxwan static** command in interface configuration mode. To disable static route negotiation, use the **no** form of this command.

ipx ipxwan static

no ipx ipxwan static

Syntax Description

This command has no arguments or keywords.

Defaults

Static routing is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

When you specify the **ipx ipxwan static** command, the interface negotiates static routing on the link. If the router at the other side of the link is not configured to negotiate for static routing, the link will not initialize.

Examples

The following example enables static routing with IPXWAN:

```
interface serial 0
 encapsulation ppp
 ipx ipxwan
 ipx ipxwan static
```

Related Commands

Command	Description
iipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx ipxwan error	Defines how to handle IPXWAN when IPX fails to negotiate properly at link startup.

ipx link-delay

To specify the link delay, use the **ipx link-delay** command in interface configuration mode. To return to the default link delay, use the **no** form of this command.

ipx link-delay *microseconds*

no ipx link-delay *microseconds*

Syntax Description

microseconds	Delay, in microseconds.

Defaults

No link delay (delay of 0).

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The link delay you specify replaces the default value or overrides the value measured by IPXWAN when it starts.

Examples

The following example sets the link delay to 20 microseconds:

```
ipx link-delay 20
```

Related Commands

Command	Description
iipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx spx-idle-time	Sets the amount of time to wait before starting the spoofing of SPX keepalive packets following inactive data transfer.

ipx linkup-request (RIP)

To enable the sending of a general RIP and/or SAP query when an interface comes up, use the **ipx linkup-request** command in interface configuration mode. To disable the sending of a general RIP and/or SAP query when an interface comes up, use the **no** form of this command.

ipx linkup-request {**rip** | **sap**}

no ipx linkup-request {**rip** | **sap**}

Syntax Description

rip	Enables the sending of a general RIP query when an interface comes up.
sap	Enables the sending of a general SAP query when an interface comes up.

Defaults

General RIP and SAP queries are sent.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Under normal operation, when using serial or other point-to-point links, the router sends RIP and SAP information twice when an interface comes up. The RIP and SAP information is sent as soon as the link is up and is sent again when the router receives a general RIP query from the other end of the connection. By disabling the **ipx linkup-request** command, the router sends the RIP and SAP information once, instead of twice.

Examples

The following example configures the router to disable the general query for both RIP and SAP on serial interface 0:

```
interface serial 0
 no ipx linkup-request rip
 no ipx linkup-request sap
```

Related Commands

Command	Description
ipx update interval	Adjusts the RIP or SAP update interval.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx maximum-hops (RIP)

To set the maximum hop count allowed for IPX packets, use the **ipx maximum-hops** command in global configuration mode. To return to the default number of hops, use the **no** form of this command.

ipx maximum-hops *hops*

no ipx maximum-hops *hops*

Syntax Description

hops	Maximum number of hops considered to be reachable by non-RIP routing protocols. Also, maximum number of routers that an IPX packet can traverse before being dropped. It can be a value from 16 to 254. The default is 16 hops.

Defaults

16 hops

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Packets whose hop count is equal to or greater than that specified by the **ipx maximum-hops** command are dropped.

In periodic RIP updates, the Cisco IOS software never advertises any network with a hop count greater than 15. However, using protocols other than RIP, the software might learn routes that are farther away than 15 hops. The **ipx maximum-hops** command defines the maximum number of hops that the software will accept as reachable, as well as the maximum number of hops that an IPX packet can traverse before it is dropped by the software. Also, the software will respond to a specific RIP request for a network that is reachable at a distance of greater than 15 hops.

Examples

The following command configures the software to accept routes that are up to 64 hops away:

```
ipx maximum-hops 64
```

ipx maximum-paths

To set the maximum number of equal-cost paths that the Cisco IOS software uses when forwarding packets, use the **ipx maximum-paths** command in global configuration mode. To restore the default value, use the **no** form of this command.

ipx maximum-paths *paths*

no ipx maximum-paths

Syntax Description

paths	Maximum number of equal-cost paths which the Cisco IOS software will use. It can be a number from 1 to 512. The default value is 1.

Defaults

1 path

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx maximum-paths** command increases throughput by allowing the software to choose among several equal-cost, parallel paths. (Note that when paths have differing costs, the software chooses lower-cost routes in preference to higher-cost routes.)

When per-host load sharing is disabled, IPX performs load sharing on a packet-by-packet basis in round-robin fashion, regardless of whether you are using fast switching or process switching. That is, the first packet is sent along the first path, the second packet along the second path, and so on. When the final path is reached, the next packet is sent to the first path, the next to the second path, and so on.

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 systems with limited ability to cache out-of-sequence packets, performance might suffer when traffic is split between many paths.

When you enable per-host load sharing, IPX performs load sharing by transmitting traffic across multiple, equal-cost paths while guaranteeing that packets for a given end host always take the same path. Per-host load sharing decreases the possibility that successive packets to a given end host will arrive out of order.

With per-host load balancing, the number of equal-cost paths set by the **ipx maximum-paths** command must be greater than one; otherwise, per-host load sharing has no effect.

Examples

In the following example, the software uses up to three parallel paths:

```
ipx maximum-paths 3
```

Related Commands

Command	Description
ipx delay	Sets the tick count.
ipx per-host-load-share	Enables per-host load sharing.
show ipx route	Displays the contents of the IPX routing table.

ipx netbios input-access-filter

To control incoming IPX NetBIOS FindName messages, use the **ipx netbios input-access-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx netbios input-access-filter {**host** | **bytes**} *name*

no ipx netbios input-access-filter {**host** | **bytes**} *name*

Syntax Description

host	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.
bytes	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.
name	Name of a NetBIOS access list.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can issue only one **ipx netbios input-access-filter host** and one **ipx netbios input-access-filter bytes** command on each interface.

These filters apply only to IPX NetBIOS FindName packets. They have no effect on LLC2 NetBIOS packets.

Examples

The following example filters packets arriving on Token Ring interface 1 using the NetBIOS access list named engineering:

```
netbios access-list host engineering permit eng*
netbios access-list host engineering deny manu*

interface tokenring 1
 ipx netbios input-access-filter engineering
```

Related Commands

Command	Description
ipx netbios output-access-filter	Controls outgoing NetBIOS FindName messages.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx netbios output-access-filter

To control outgoing NetBIOS FindName messages, use the **ipx netbios output-access-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx netbios output-access-filter {**host** | **bytes**} *name*

no ipx netbios output-access-filter {**host** | **bytes**} *name*

Syntax Description

host	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.
bytes	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.
name	Name of a previously defined NetBIOS access list.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can issue only one **ipx netbios output-access-filter host** and one **ipx netbios output-access-filter bytes** command on each interface.

These filters apply only to IPX NetBIOS FindName packets. They have no effect on LLC2 NetBIOS packets.

Examples

The following example filters packets leaving Token Ring interface 1 using the NetBIOS access list named engineering:

```
netbios access-list bytes engineering permit 20 AA**04

interface token 1
 ipx netbios output-access-filter bytes engineering
```

Related Commands

Command	Description
ipx netbios input-access-filter	Controls incoming IPX NetBIOS FindName messages.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx netbios-socket-input-checks

To enable additional checks that are performed on Network Basic Input/Output System (NetBIOS) packets that do not conform fully to Novell Type20 NetBIOS packets, use the **ipx netbios-socket-input-checks** command in global configuration mode. To disable the additional checking, use the **no** form of this command.

ipx netbios-socket-input-checks

no ipx netbios-socket-input-checks

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you use the **ipx netbios-socket-input-checks** command to enable additional checks on NetBIOS packets that do not fully conform to Novell Type20 NetBIOS packets, the same checks that are performed on Type20 packets to avoid broadcast loops are performed for any packet that does not have the netBIOS socket, even if it is not a Novell Type20 packet.

Note In order to forward non-Type20 broadcasts, you must configure a helper address on two or more interfaces. For more information, see the **ipx helper-address** command earlier in this chapter.

Examples

The following example enables the additional checks on NetBIOS packets:

```
ipx netbios-socket-input-checks
```

Related Commands

Command	Description
ipx helper-address	Forwards broadcast packets to a specified server.
ipx type-20-input-checks	Restricts the acceptance of IPX Type20 propagation packet broadcasts.
ipx type-20-output-checks	Restricts the forwarding of IPX Type20 propagation packet broadcasts.
ipx type-20-propagation	Forwards IPX Type20 propagation packet broadcasts to other network segments.

ipx network

To enable IPX routing on a particular interface and to optionally select the type of encapsulation (framing), use the **ipx network** command in interface configuration mode. To disable IPX routing, use the **no** form of this command.

ipx network *network* [**encapsulation** *encapsulation-type* [**secondary**]]

no ipx network *network* [**encapsulation** *encapsulation-type*]

Syntax Description

network	Network number. This is an 8-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.
encapsulation *encapsulation-type*	(Optional) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 7.
secondary	(Optional) Indicates an additional (secondary) network configured after the first (primary) network.

Table 7 describes the types of encapsulation available for specific interfaces.

Table 7 Encapsulation Types

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Uses Novell's Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For serial interfaces only—Uses High-Level Data Link Control (HDLC) encapsulation.
novell-ether	For Ethernet interfaces only—Uses Novell's Ethernet_802.3 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Uses Novell's FDDI_RAW encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.

Table 7 Encapsulation Types (continued)

Encapsulation Type	Description
sap	For Ethernet interfaces—Uses Novell's Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by NetWare Version 3.12 and 4.0. For Token Ring interfaces—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header. For FDDI interfaces—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.
snap	For Ethernet interfaces—Uses Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Subnetwork Access Protocol (SNAP) LLC header. For Token Ring and FDDI interfaces—This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.

Defaults

IPX routing is disabled.

Encapsulation types:
For Ethernet: **novell-ether**
For Token Ring: **sap**
For FDDI: **snap**
For serial: **hdlc**

If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from **novell-ether** to **sap**.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to support the FDDI interface.

Usage Guidelines

The **ipx network** command allows you to configure a single logical network on a physical network or more than one logical network on the same physical network (network cable segment). Each network on a given interface must have a different encapsulation type.

Note You cannot configure more than 200 IPX interfaces on a router using the **ipx network** command.

The first network you configure on an interface is considered to be the primary network. Any additional networks are considered to be secondary networks; these must include the **secondary** keyword.

Note In future Cisco IOS software releases, primary and secondary networks may not be supported.

You can configure an IPX network on any supported interface as long as all the networks on the same physical interface use a distinct encapsulation type. For example, you can configure up to four IPX networks on a single Ethernet cable because Ethernet supports four encapsulation types.

The interface processes only packets with the correct encapsulation and the correct network number. IPX networks that use encapsulations can be present on the physical network. The only effect on the router is that it uses some processing time to examine packets to determine whether they have the correct encapsulation.

All logical networks on an interface share the same set of configuration parameters. For example, if you change the IPX RIP update time on an interface, you change it for all networks on that interface.

When you define multiple logical networks on the same physical network, IPX treats each encapsulation as if it were a separate physical network. This means, for example, that IPX sends RIP updates and SAP updates for each logical network.

The **ipx network** command is useful when migrating from one type of encapsulation to another. If you are using it for this purpose, you should define the new encapsulation on the primary network.

Note If you have already enabled IPX routing on the specified interface, you can use the **ipx encapsulation** command to change the encapsulation type.

To delete all networks on an interface, use the following command:

no ipx network

Deleting the primary network with the following command also deletes all networks on that interface. The argument *number* is the number of the primary network.

no ipx network *number*

To delete a secondary network on an interface, use one of the following commands. The argument *number* is the number of a secondary network.

no ipx network *number*

no ipx network *number* **encapsulation** *encapsulation-type*

Novell's FDDI_RAW encapsulation is common in bridged or switched environments that connect Ethernet-based Novell end hosts via a FDDI backbone. Packets with FDDI_RAW encapsulation are classified as Novell packets and are not automatically bridged when you enable both bridging and IPX routing. Additionally, you cannot configure FDDI_RAW encapsulation on an interface configured for IPX autonomous or silicon switching engine (SSE) switching. Similarly, you cannot enable IPX autonomous or SSE switching on an interface configured with FDDI_RAW encapsulation.

With FDDI_RAW encapsulation, platforms that do not use CBUS architecture support fast switching. Platforms using CBUS architecture support only process switching of **novell-fddi** packets received on an FDDI interface.

Examples

The following example uses subinterfaces to create four logical networks on Ethernet interface 0. Each subinterface has a different encapsulation. Any interface configuration parameters that you specify on an individual subinterface are applied to that subinterface only.

```
ipx routing
interface ethernet 0
 ipx network 1 encapsulation novell-ether

interface ethernet 0.1
 ipx network 2 encapsulation snap

interface ethernet 0.2
 ipx network 3 encapsulation arpa

interface ethernet 0
 ipx network 4 encapsulation sap
```

The following example uses primary and secondary networks to create the same four logical networks as shown previously in this section. Any interface configuration parameters that you specify on this interface are applied to all the logical networks. For example, if you set the routing update timer to 120 seconds, this value is used on all four networks.

```
ipx routing
ipx network 1 encapsulation novell-ether
ipx network 2 encapsulation snap secondary
ipx network 3 encapsulation arpa secondary
ipx network 4 encapsulation sap secondary
```

The following example enables IPX routing on FDDI interfaces 0.2 and 0.3. On FDDI interface 0.2, the encapsulation type is SNAP. On FDDI interface 0.3, the encapsulation type is Novell's FDDI_RAW.

```
ipx routing

interface fddi 0.2 enc sde 2
 ipx network f02 encapsulation snap

interface fddi 0.3 enc sde 3
 ipx network f03 encapsulation novell-fddi
```

Related Commands

Command	Description
ipx encapsulation	Sets the Ethernet frame type of the interface to that of the local file server.
ipx routing	Enables IPX routing.

ipx output-ggs-filter

To control which servers are included in the Get General Service (GGS) responses sent by Cisco IOS software, use the **ipx output-ggs-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx output-ggs-filter {*access-list-number* | *name*}

no ipx output-ggs-filter {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the Service Advertising Protocol (SAP) access list. All outgoing GGS packets are filtered by the entries in this list. The *access-list number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent their being confused with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

You can issue only one **ipx output-ggs-filter** command on each interface.

Note Because GGS SAP response filters are applied ahead of output SAP filters, a SAP entry permitted to pass through the GGS SAP response filter can still be filtered by the output SAP filter.

Examples

The following example excludes the server at address 3c.0800.89a1.1527 from GGS responses sent on Ethernet interface 0, but allows all other servers:

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
ipx routing

interface ethernet 0
 ipx network 2B
 ipx output-ggs-filter 1000
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx output-gns-filter	Controls which servers are included in the GGS responses sent by the Cisco IOS software.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx router-sap-filter	Filters SAP messages received from a particular router.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx output-gns-filter

To control which servers are included in the Get Nearest Server (GNS) responses sent by Cisco IOS software, use the **ipx output-gns-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx output-gns-filter {*access-list-number* | *name*}

no ipx output-gns-filter {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the SAP access list. All outgoing GNS packets are filtered by the entries in this access list. The argument *access-list-number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can issue only one **ipx output-gns-filter** command on each interface.

Examples

The following example excludes the server at address 3c.0800.89a1.1527 from GNS responses sent on Ethernet interface 0, but allows all other servers:

```
access-list 1000 deny 3c.0800.89a1.1527
access-list 1000 permit -1
ipx routing

interface ethernet 0
 ipx network 2B
 ipx output-gns-filter 1000
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx gns-round-robin	Rotates using a round-robin selection method through a set of eligible servers when responding to GNS requests.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx output-network-filter (RIP)

To control the list of networks included in routing updates sent out an interface, use the **ipx output-network-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx output-network-filter {*access-list-number* | *name*}

no ipx output-network-filter {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx output-network-filter** command controls which networks the Cisco IOS software advertises in its IPX routing updates (RIP updates).

You can issue only one **ipx output-network-filter** command on each interface.

Examples

In the following example, access list 896 controls which networks are specified in routing updates sent out the serial 1 interface. This configuration causes network 2b to be the only network advertised in Novell routing updates sent on the specified serial interface.

```
access-list 896 permit 2b

interface serial 1
 ipx output-network-filter 896
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-list	Defines an IPX access list by name.
ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
ipx router-filter	Filters the routers from which packets are accepted.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
prc-interval	Sets conditions for a named IPX access list.

ipx output-rip-delay

To set the interpacket delay for RIP updates sent on a single interface, use the **ipx output-rip-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipx output-rip-delay *delay*

no ipx output-rip-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. The **ipx output-rip-delay** command sets the interpacket delay for a single interface.

The system uses the interpacket delay specified by the **ipx output-rip-delay** command for periodic and triggered routing updates when no delay is set for triggered routing updates. When you set a delay for triggered routing updates, the system uses the delay specified by the **ipx output-rip-delay** command for only the periodic routing updates sent on the interface.

To set a delay for triggered routing updates, see the **ipx triggered-rip-delay** or **ipx default-triggered-rip-delay** commands.

You can also set a default RIP interpacket delay for all interfaces. See the **ipx default-output-rip-delay** command for more information.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Examples

The following example establishes a 55-ms interpacket delay on serial interface 0:

```
interface serial 0
```

```
ipx network 106A
ipx output-rip-delay 55
```

Related Commands

Command	Description
ipx default-output-rip-delay	Sets the default interpacket delay for RIP updates sent on all interfaces
ipx default-triggered-rip-delay	Sets the default interpacket delay for triggered RIP updates sent on all interfaces.
ipx triggered-rip-delay	Sets the interpacket delay for triggered RIP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx output-sap-delay

To set the interpacket delay for Service Advertising Protocol (SAP) updates sent on a single interface, use the **ipx output-sap-delay** command in interface configuration mode. To return to the default delay value, use the **no** form of this command.

ipx output-sap-delay *delay*

no ipx output-sap-delay

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. The **ipx output-sap-delay** command sets the interpacket delay for a single interface.

The system uses the interpacket delay specified by the **ipx output-sap-delay** command for periodic and triggered SAP updates when no delay is set for triggered updates. When you set a delay for triggered updates, the system uses the delay specified by the **ipx output-sap-delay** command only for the periodic updates sent on the interface.

To set a delay for triggered updates, see the **ipx triggered-sap-delay** or **ipx default-triggered-sap-delay** commands.

You can also set a default SAP interpacket delay for all interfaces. See the **ipx default-output-sap-delay** command for more information.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by the **ipx output-sap-delay** command forces the router to pace its output to the slower-processing needs of these servers.

The default delay on a NetWare 3.11 server is about 100 ms.

This command is also useful on limited bandwidth point-to-point links or X.25 and Frame Relay multipoint interfaces.

Examples

The following example establishes a 55-ms delay between packets in multiple-packet SAP updates on Ethernet interface 0:

```
interface ethernet 0
 ipx network 106A
 ipx output-sap-delay 55
```

Related Commands

Command	Description
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx default-triggered-sap-delay	Sets the default interpacket delay for triggered SAP updates sent on all interfaces.
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx triggered-sap-delay	Sets the interpacket delay for triggered SAP updates sent on a single interface.

ipx output-sap-filter

To control which services are included in Service Advertising Protocol (SAP) updates sent by Cisco IOS software, use the **ipx output-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx output-sap-filter {*access-list-number* | *name*}

no ipx output-sap-filter {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the SAP access list. All outgoing service advertisements are filtered by the entries in this access list. The argument *access-list-number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Cisco IOS software applies output SAP filters prior to sending SAP packets.

You can issue only one **ipx output-sap-filter** command on each interface.

When configuring SAP filters for NetWare 3.11 and later servers, use the server's internal network and node number (the node number is always 0000.0000.0001) as its address in the SAP **access-list** command. Do not use the *network.node* address of the particular interface board.

Examples

The following example denies service advertisements about server 0000.0000.0001 on network aa from being sent on network 4d (via Ethernet interface 1). All other services are advertised via this network. All services, included those from server aa.0000.0000.0001, are advertised via networks 3c and 2b.

```
access-list 1000 deny aa.0000.0000.0001
access-list 1000 permit -1

interface ethernet 0
 ipx network 3c

interface ethernet 1
 ipx network 4d
 ipx output-sap-filter 1000
```

```
interface serial 0
 ipx network 2b
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx gns-round-robin	Rotates using a round-robin selection method through a set of eligible servers when responding to GNS requests.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx router-sap-filter	Filters SAP messages received from a particular router.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.

ipx pad-process-switched-packets

To control whether odd-length packets are padded so as to be sent as even-length packets on an interface, use the **ipx pad-process-switched-packets** command in interface configuration mode. To disable padding, use the **no** form of this command.

ipx pad-process-switched-packets

no ipx pad-process-switched-packets

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled on Ethernet interfaces.
Disabled on Token Ring, FDDI, and serial interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command only under the guidance of a customer engineer or other service representative.

The **ipx pad-process-switched-packets** command affects process-switched packets only, so you must disable fast switching before the **ipx pad-process-switched-packets** command has any effect.

Some IPX end hosts reject Ethernet packets that are not padded. Certain topologies can result in such packets being forwarded onto a remote Ethernet network. Under specific conditions, padding on intermediate media can be used as a temporary workaround for this problem.

Examples

The following example configures the Cisco IOS software to pad odd-length packets so that they are sent as even-length packets on FDDI interface 1.

```
interface fddi 1
 ipx network 2A
 no ipx route-cache
 ipx pad-process-switched-packets
```

Related Commands

Command	Description
iipx route-cache	Enables IPX fast switching.

ipx per-host-load-share

To enable per-host load sharing, use the **ipx per-host-load-share** command in global configuration mode. To disable per-host load sharing, use the **no** form of this command.

ipx per-host-load-share

no ipx per-host-load-share

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to enable per-host load sharing. Per-host load sharing transmits traffic across multiple, equal-cost paths while guaranteeing that packets for a given end host always take the same path.

When you do not enable per-host load sharing, the software uses a round-robin algorithm to accomplish load sharing. Round-robin load sharing transmits successive packets over alternate, equal-cost paths, regardless of the destination host. With round-robin load sharing, successive packets destined for the same end host might take different paths. Thus, round-robin load sharing increases the possibility that successive packets to a given end host might arrive out of order or be dropped, but ensures true load balancing of a given workload across multiple links.

In contrast, per-host load sharing decreases the possibility that successive packets to a given end host will arrive out of order; but, there is a potential decrease in true load balancing across multiple links. True load sharing occurs only when different end hosts utilize different paths; equal link utilization cannot be guaranteed.

With per-host load balancing, the number of equal-cost paths set by the **ipx maximum-paths** command must be greater than one; otherwise, per-host load sharing has no effect.

Examples

The following command globally enables per-host load sharing:

```
ipx per-host-load share
```

Related Commands

Command	Description
ipx maximum-paths	Sets the maximum number of equal-cost paths the Cisco IOS software uses when forwarding packets.

ipx rip-max-packetsize

To configure the maximum packet size of RIP updates sent out the interface, use the **ipx rip-max-packetsize** command in interface configuration mode. To restore the default packet size, use the **no** form of this command.

ipx rip-max-packetsize *bytes*

no ipx rip-max-packetsize *bytes*

Syntax Description

bytes	Maximum packet size in bytes. The default is 432 bytes, which allows for 50 routes at 8 bytes each, plus 32 bytes of IPX network and RIP header information.

Defaults

432 bytes

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The maximum size is for the IPX packet including the IPX network and RIP header information.

Do not allow the maximum packet size to exceed the allowed maximum size of packets for the interface.

Examples

The following example sets the maximum RIP update packet to 832 bytes:

```
ipx rip-max-packetsize 832
```

Related Commands

Command	Description
ipx sap-max-packetsize	Configures the maximum packet size of SAP updates sent out the interface.

ipx rip-multiplier

To configure the interval at which a network's RIP entry ages out, use the **ipx rip-multiplier** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx rip-multiplier *multiplier*

no ipx rip-multiplier *multiplier*

Syntax Description

multiplier	Multiplier used to calculate the interval at which to age out RIP routing table entries. This can be any positive number. The value you specify is multiplied by the RIP update interval to determine the aging-out interval. The default is three times the RIP update interval.

Defaults

Three times the RIP update interval

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

All routers on the same physical cable should use the same multiplier value.

Examples

In the following example, in a configuration where RIP updates are sent once every 2 minutes, the interval at which RIP entries age out is set to 10 minutes:

```
interface ethernet 0
 ipx rip-multiplier 5
```

Related Commands

Command	Description
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx rip-queue-maximum

To set an IPX Routing Information Protocol (RIP) queue maximum to control how many RIP packets can be waiting to be processed at any given time, use the **ipx rip-queue-maximum** command in global configuration mode. To clear a set RIP queue maximum, use the **no** form of this command.

ipx rip-queue-maximum *milliseconds*

no ipx rip-queue-maximum *milliseconds*

Syntax Description

milliseconds	Specifies the queue limit as a number from 0 to the maximum unassigned integer.

Defaults

No queue limit is set.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

When you use the **ipx rip-queue-maximum** command to control how many RIP packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming RIP request packets are dropped. Be sure to set a large enough queue limit to handle normal incoming RIP requests on all interfaces, or else the RIP information may time out.

Examples

The following example sets a RIP queue maximum of 500 milliseconds:

```
ipx rip-queue-maximum 500
```

Related Commands

Command	Description
ipx rip-update-queue-maximum	Sets an IPX RIP queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time.
ipx sap-queue-maximum	Sets an IPX SAP queue maximum to control how many SAP packets can be waiting to be processed at any given time.
ipx sap-update-queue-maximum	Sets an IPX SAP queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time.

ipx rip-update-queue-maximum

To set an IPX Routing Information Protocol (RIP) queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time, use the **ipx rip-update-queue-maximum** command in global configuration mode. To clear a set RIP queue maximum, use the **no** form of this command.

ipx rip-update-queue-maximum *queue-maximum*

no ipx rip-update-queue-maximum *queue-maximum*

Syntax Description

queue-maximum	Specifies the queue limit as a number from 0 to the maximum unassigned integer.

Defaults

No queue limit

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

When you use the **ipx rip-update-queue-maximum** command to control how many incoming RIP update packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming RIP update packets are dropped.

Note When using the **ipx rip-update-queue-maximum** command, be sure to set this queue high enough to handle a full update on all interfaces, or else the RIP information may time out.

Examples

The following example sets a RIP update queue maximum of 500:

```
ipx rip-update-queue-maximum 500
```

Related Commands

Command	Description
ipx rip-queue-maximum	Sets an IPX RIP queue maximum to control how many RIP packets can be waiting to be processed at any given time.
ipx sap-queue-maximum	Sets an IPX SAP queue maximum to control how many SAP packets can be waiting to be processed at any given time.
ipx sap-update-queue-maximum	Sets an IPX SAP queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time.

ipx rip-response-delay

To change the delay when responding to Routing Information Protocol (RIP) requests, use the **ipx rip-response-delay** command in interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx rip-response-delay *ms*

no ipx rip-response-delay

Syntax Description

ms	Delay time, in milliseconds, for RIP responses.

Defaults

No delay in answering (0 ms).

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command slows down the Cisco router and allows another router to answer first and become the router of choice. A delay in responding to RIP requests can be imposed so that, in certain topologies, any local Novell IPX router or any third-party IPX router can respond to the RIP requests before the Cisco router responds.

Optimal delay time is the same as or slightly longer than the time it takes the other router to answer.

Examples

The following example sets the delay in responding to RIP requests to 55 ms (0.055 seconds):

```
ipx rip-response-delay 55
```

Related Commands

Command	Description
ipx gns-response-delay	Changes the delay when responding to GNS requests.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.

ipx route-cache inactivity-timeout

To adjust the period and rate of route cache invalidation because of inactivity, use the **ipx route-cache inactivity-timeout** command in global configuration mode. To return to the default values, use the **no** form of this command.

ipx route-cache inactivity-timeout *period* [*rate*]

no ipx route-cache inactivity-timeout

Syntax Description

period	Number of minutes that a valid cache entry may be inactive before it is invalidated. Valid values are 0 through 65,535. A value of zero disables this feature.
rate	(Optional) Maximum number of inactive entries that may be invalidated per minute. Valid values are 0 through 65,535. A value of zero means no limit.

Defaults

The default period is 2 minutes. The default rate is 0 (cache entries do not age).

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

IPX fast-switch cache entries that are not in use may be invalidated after a configurable period of time. If no new activity occurs, these entries will be purged from the route cache after one additional minute.

Cache entries that have been uploaded to the switch processor when autonomous switching is configured are always exempt from this treatment.

This command has no effect if silicon switching is configured.

Examples

The following example sets the inactivity period to 5 minutes, and sets a maximum of 10 entries that can be invalidated per minute:

```
ipx route-cache inactivity-timeout 5 10
```

Related Commands

Command	Description
clear ipx cache	Deletes entries from the IPX fast-switching cache.
iipx route-cache	Enables IPX fast switching.
ipx route-cache update-timeout	Adjusts the period and rate of route cache invalidation because of aging.
show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx route-cache max-size

To set a maximum limit on the number of entries in the IPX route cache, use the **ipx route-cache max-size** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipx route-cache max-size *size*

no ipx route-cache max-size

Syntax Description

size	Maximum number of entries allowed in the IPX route cache.

Defaults

The default setting is no limit on the number of entries.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

On large networks, storing too many entries in the route cache can use a significant amount of router memory, causing router processing to slow. This situation is most common on large networks that run network management applications for NetWare. If the network management station is responsible for managing all clients and servers in a very large (greater than 50,000 nodes) Novell network, the routers on the local segment can become inundated with route cache entries. The **ipx route-cache max-size** command allows you to set a maximum number of entries for the route cache.

If the route cache already has more entries than the specified limit, the extra entries are not deleted. However, all route cache entries are subject to being removed via the parameter set for route cache aging via the **ipx route-cache inactivity-timeout** command.

Examples

The following example sets the maximum route cache size to 10,000 entries.

```
ipx route-cache max-size 10000
```

Related Commands

Command	Description
iipx route-cache	Enables IPX fast switching.
ipx route-cache inactivity-timeout	Adjusts the period and rate of route cache invalidation because of inactivity.
ipx route-cache update-timeout	Adjusts the period and rate of route cache invalidation because of aging.
show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx route-cache update-timeout

To adjust the period and rate of route cache invalidation because of aging, use the **ipx route-cache update-timeout** command in global configuration mode. To return to the default values, use the **no** form of this command.

ipx route-cache update-timeout *period* [*rate*]

no ipx route-cache update-timeout

Syntax Description

period	Number of minutes since a valid cache entry was created before it may be invalidated. A value of zero disables this feature.
rate	(Optional) Maximum number of aged entries that may be invalidated per minute. A value of zero means no limit.

Defaults

The default setting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

IPX fast-switch cache entries that exceed a minimum age may be invalidated after a configurable period of time. Invalidation occurs unless the cache entry was marked as active during the last minute. Following invalidation, if no new activity occurs, these entries will be purged from the route cache after one additional minute.

This capability is primarily useful when autonomous switching or silicon switching is enabled. In both cases, activity is not recorded for entries in the route cache, because data is being switched by the Switch Processor (SP) or Silicon Switch Processor (SSP). In this case, it may be desirable to periodically invalidate a limited number of older cache entries each minute.

If the end hosts have become inactive, the cache entries will be purged after one additional minute. If the end hosts are still active, the route cache and autonomous or SSP cache entries will be revalidated instead of being purged.

Examples

The following example sets the update timeout period to 5 minutes and sets a maximum of 10 entries that can be invalidated per minute:

```
ipx route-cache update-timeout 5 10
```

Related Commands

Command	Description
clear ipx cache	Deletes entries from the IPX fast-switching cache.
iipx route-cache	Enables IPX fast switching.
ipx route-cache inactivity-timeout	Adjusts the period and rate of route cache invalidation because of inactivity.
show ipx cache	Displays the contents of the IPX fast-switching cache.

ipx router-filter

To filter the routers from which packets are accepted, use the **ipx router-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx router-filter {*access-list-number* | *name*}

no ipx router-filter

Syntax Description

access-list-number	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can issue only one **ipx router-filter** command on each interface.

Examples

In the following example, access list 866 controls the routers from which packets are accepted. For Ethernet interface 0, only packets from the router at 3c.0000.00c0.047d are accepted. All other packets are implicitly denied.

```
access-list 866 permit 3c.0000.00c0.047d

interface ethernet 0
 ipx router-filter 866
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
access-list (IPX standard)	Defines a standard IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-list	Defines an IPX access list by name.
ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
ipx output-network-filter (RIP)	Controls the list of networks included in routing updates sent out an interface.
permit (IPX extended)	Sets conditions for a named IPX extended access list.
prc-interval	Sets conditions for a named IPX access list.

ipx router-sap-filter

To filter Service Advertising Protocol (SAP) messages received from a particular router, use the **ipx router-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx router-sap-filter {*access-list-number* | *name*}

no ipx router-sap-filter {*access-list-number* | *name*}

Syntax Description

access-list-number	Number of the access list. All incoming service advertisements are filtered by the entries in this access list. The argument *access-list-number* is a number from 1000 to 1099.
name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No filters are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can issue only one **ipx router-sap-filter** command on each interface.

Examples

In the following example, the Cisco IOS software will receive service advertisements only from router aa.0207.0104.0874:

```
access-list 1000 permit aa.0207.0104.0874
access-list 1000 deny -1

interface ethernet 0
 ipx router-sap-filter 1000
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-list	Defines an IPX access list by name.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx sap	Specifies static SAP entries.
permit (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

ipx routing

To enable IPX routing, use the **ipx routing** command in global configuration mode. To disable IPX routing, use the **no** form of this command.

ipx routing [*node*]

no ipx routing

Syntax Description

node	(Optional) Node number of the router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). It must not be a multicast address. If you omit the *node* argument, the Cisco IOS software uses the hardware MAC address currently assigned to it as its node address. This is the MAC address of the first Ethernet, Token Ring, or FDDI interface card. If no satisfactory interfaces are present in the router (such as only serial interfaces), you must specify a value for the *node* argument.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx routing** command enables IPX Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) services.

If you omit the argument *node* and if the MAC address later changes, the IPX node address automatically changes to the new address. However, connectivity may be lost between the time that the MAC address changes and the time that the IPX clients and servers learn the router's new address.

If you plan to use DECnet and IPX routing concurrently on the same interface, you should enable DECnet router first, then enable IPX routing without specifying the optional MAC node number. If you enable IPX before enabling DECnet routing, routing for IPX will be disrupted.

Examples

The following example enables IPX routing:

```
ipx routing
```

Related Commands

Command	Description
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

ipx sap

To specify static Service Advertising Protocol (SAP) entries, use the **ipx sap** command in global configuration mode. To remove static SAP entries, use the **no** form of this command.

ipx sap *service-type name network.node socket hop-count*

no ipx sap *service-type name network.node socket hop-count*

Syntax Description

service-type	SAP service-type number. See the **access-list** (SAP filtering) command earlier in this chapter for a table of some IPX SAP services.
name	Name of the server that provides the service.
network.node	Network number and node address of the server. The argument *network* is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA. The argument *node* is the node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
socket	Socket number for this service. See access-list (IPX extended) command earlier in this chapter for a table of some IPX socket numbers.
hop-count	Number of hops to the server.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ipx sap** command allows you to add static entries into the SAP table. Each entry has a SAP service associated with it. Static SAP assignments always override any identical entries in the SAP table that are learned dynamically, regardless of hop count. The router will not announce a static SAP entry unless it has a route to that network.

Examples

In the following example, the route to JOES_SERVER is not yet learned, so the system displays an informational message. The JOES_SERVER service will not be announced in the regular SAP updates until Cisco IOS software learns the route to it either by means of a RIP update from a neighbor or an **ipx sap** command.

```
ipx sap 107 MAILSERV 160.0000.0c01.2b72 8104 1
ipx sap 4 FILESERV 165.0000.0c01.3d1b 451 1
ipx sap 143 JOES_SERVER A1.0000.0c01.1234 8170 2
no route to A1, JOES_SERVER won't be announced until route is learned
```

Related Commands

Command	Description
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx output-sap-filter	Controls which services are included in SAP updates sent by the Cisco IOS software.
ipx router-sap-filter	Filters SAP messages received from a particular router.
show ipx servers	Lists the IPX servers discovered through SAP advertisements.

ipx sap follow-route-path

To enable a router to accept IPX Service Advertising Protocol (SAP) entries from SAP updates received on an interface only if that interface is one of the best paths to reach the destination networks of those SAPs, use the **ipx sap follow-route-path** command in global configuration mode. To disable this router function, use **no** form of this command.

ipx sap follow-route-path

no ipx sap follow-route-path

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

In redundantly connected networks that use IPX-Enhanced IGRP routing in which multiple IPX paths exist, IPX SAP services can be learned on nonoptimal interfaces, causing SAP loops, also known as phantom SAPs, when those services become obsolete. Use the **ipx sap follow-route-path** command to prevent the occurrence of SAP loops.

When the **ipx sap follow-route-path** command is used, the router screens individual services (SAPs) in SAP updates. The router looks at the destination network number of each SAP entry's . If the receiving interface is one of the best interfaces to reach the destination network of the SAP, that SAP entry is accepted. Otherwise, the SAP entry is discarded.

Caution When the **ipx sap follow-route-path** command is globally enabled in conjunction with SAP input filters on interfaces that are considered the best paths to reach the destination networks, the SAPs that are being filtered will no longer be learned by the router, even if other less optimal interfaces are capable of receiving those SAP updates.

Examples

The following example enables the router to accept only the IPX SAP entries from SAP updates received on an interface deemed to be one of the best paths to the destination address of those SAPs:

```
ipx sap follow-route-path
```

Related Commands

Command	Description
ipx server-split-horizon-on-server-paths	Controls whether Service Information split horizon checking should be based on RIP or SAP.

ipx sap-helper

To set an address, which should be another Cisco router that is adjacent to the router being configured, to which all Service Advertising Protocol (SAP) request packets are received, use the **ipx sap-helper** command in interface configuration mode. To remove the address and stop forwarding SAP request packets, use the **no** form of this command.

ipx sap-helper *network.node*

no ipx sap-helper *network.node*

Syntax Description

network.node	The argument *network* is the network on which the SAP helper router resides. This eight-digit hexadecimal number uniquely identifies a network cable segment. It can be a number in the range from 1 to FFFFFFFD. You do not need to specify the leading zeros in the network number. For example, for the network number 000000AA, you can enter AA. The argument *node* is the node number of the SAP helper router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

Defaults

No helper address is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

Use this command to redirect SAP packet requests that are sent to a remote router that has a limited memory size, CPU speed, and often a slow WAN link joining it to the main corporate backbone. The SAP helper target is usually much a much larger router that has a much larger routing table and a complete SAP table.

Examples

The following example assigns a router with the address 1000.0000.0c00.1234 as the SAP helper:

```
interface ethernet 0
 ipx sap-helper 1000.0000.0c00.1234
```

Related Commands

Command	Description
ipx helper-address	Forwards broadcast packets to a specified server.

ipx sap-incremental (EIGRP)

To send Service Advertising Protocol (SAP) updates only when a change occurs in the SAP table, use the **ipx sap-incremental** command in interface configuration mode. To send periodic SAP updates, use the **no** form of this command.

ipx sap-incremental eigrp *autonomous-system-number* [**rsup-only**]

no ipx sap-incremental eigrp *autonomous-system-number* [**rsup-only**]

Syntax Description

eigrp *autonomous-system-number*	IPX Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
rsup-only	(Optional) Indicates that the system uses Enhanced IGRP on this interface to carry reliable SAP update information only. RIP routing updates are used, and Enhanced IGRP routing updates are ignored.

Defaults

Enabled on serial interfaces

Disabled on LAN media (Ethernet, Token Ring, FDDI)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To use the **ipx sap-incremental** command, you must enable Enhanced IGRP. This is the case even if you want to use only RIP routing. You must do this because the incremental SAP feature requires the Enhanced IGRP reliable transport mechanisms.

With this functionality enabled, if an IPX Enhanced IGRP peer is found on the interface, SAP updates will be sent only when a change occurs in the SAP table. Periodic SAP updates are not sent. When no IPX Enhanced IGRP peer is present on the interface, periodic SAPs are always sent, regardless of how this command is set.

If you configure the local router to send incremental SAP updates on an Ethernet, and if the local device has at least one IPX Enhanced IGRP neighbor and any servers, clients, or routers that do not have IPX Enhanced IGRP configured on the Ethernet interface, these devices will not receive complete SAP information from the local router.

If the incremental sending of SAP updates on an interface is configured and no IPX Enhanced IGRP peer is found, SAP updates will be sent periodically until a peer is found. Then, updates will be sent only when changes occur in the SAP table.

To take advantage of Enhanced IGRP's incremental SAP update mechanism while using the RIP routing protocol instead of the Enhanced IGRP routing protocol, specify the **rsup-only** keyword. SAP updates are then sent only when changes occur, and only changes are sent. Use this feature only when you want to use RIP routing; Cisco IOS software disables the exchange of route information via Enhanced IGRP for that interface.

Examples

The following example sends SAP updates on Ethernet interface 0 only when there is a change in the SAP table:

```
interface ethernet 0
 ipx sap-incremental eigrp 200
```

ipx sap-incremental split-horizon

To configure incremental SAP split horizon, use the **ipx sap-incremental split-horizon** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipx sap-incremental split-horizon

no ipx sap-incremental split-horizon

Syntax Description

This command has no argument or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Caution For IPX incremental SAP split horizon to work properly, IPX Enhanced **IGRP** should be turned on. Otherwise, a warning message like the following will be displayed:

```
%IPX EIGRP not running.
```

When split horizon is enabled, Enhanced IGRP incremental SAP update packets are not sent back to the same interface from where the SAP is received. This reduces the number of Enhanced IGRP packets on the network.

Split horizon blocks information about SAPs from being advertised by a router to the same interface from where that SAP is received. Typically, this behavior optimizes communication among multiple routers, particularly when links are broken. However, with nonbroadcast networks, such as Frame Relay and SMDS, situations can arise for which this behavior is less than ideal. For these situations, you may wish to disable split horizon.

Note IPX incremental SAP split horizon is off for WAN interfaces and subinterfaces, and on for LAN interfaces. The global default stays off. The interface setting takes precedence if the interface setting is modified or when both the global and interface settings are unmodified. The global setting is used only when global setting is modified and the interface setting is unmodified.

Examples

The following example disables split horizon on serial interface 0:

```
interface serial 0
```

```
no ipx sap-incremental split-horizon
```

Related Commands

Command	Description
ipx eigrp-sap-split-horizon	Configures Enhanced IGRP SAP split horizon.
ipx split-horizon eigrp	Configures split horizon.
show ipx eigrp neighbors	Displays the neighbors discovered by Enhanced IGRP.

ipx sap-max-packetsize

To configure the maximum packet size of Service Advertising Protocol (SAP) updates sent out the interface, use the **ipx sap-max-packetsize** command in interface configuration mode. To restore the default packet size, use the **no** form of this command.

ipx sap-max-packetsize *bytes*

no ipx sap-max-packetsize *bytes*

Syntax Description

bytes	Maximum packet size, in bytes. The default is 480 bytes, which allows for 7 servers (64 bytes each), plus 32 bytes of IPX network and SAP header information.

Defaults

480 bytes

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The maximum size is for the IPX packet, including the IPX network and SAP header information. For example, to allow 10 servers per SAP packet, you would configure (32 + (10 * 64)), or 672 bytes for the maximum packet size.

You are responsible for guaranteeing that the maximum packet size does not exceed the allowed maximum size of packets for the interface.

Examples

The following example sets the maximum SAP update packet size to 672 bytes:

```
ipx sap-max-packetsize 672
```

Related Commands

Command	Description
ipx rip-max-packetsize	Configures the maximum packet size of RIP updates sent out the interface.

ipx sap-multiplier

To configure the interval at which a Service Advertising Protocol (SAP) entry for a network or server ages out, use the **ipx sap-multiplier** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx sap-multiplier *multiplier*

no ipx sap-multiplier *multiplier*

Syntax Description

multiplier	Multiplier used to calculate the interval at which to age out SAP routing table entries. This can be any positive number. The value you specify is multiplied by the SAP update interval to determine the aging-out interval. The default is three times the SAP update interval.

Defaults

Three times the SAP update interval.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

All routers on the same physical cable should use the same multiplier value.

Examples

In the following example, in a configuration where SAP updates are sent once every 1 minute, the interval at which SAP entries age out is set to 10 minutes:

```
interface ethernet 0
 ipx sap-multiplier 10
```

Related Commands

Command	Description
ipx sap-max-packetsize	Configures the maximum packet size of SAP updates sent out the interface.

ipx sap-queue-maximum

To set an IPX Service Advertising Protocol (SAP) queue maximum to control how many SAP packets can be waiting to be processed at any given time, use the **ipx sap-queue-maximum** command in global configuration mode. To clear a set SAP queue maximum, use the **no** form of this command.

ipx sap-queue-maximum *queue-maximum*

no ipx sap-queue-maximum *queue-maximum*

Syntax Description

queue-maximum	Specifies the queue limit as a number from 0 to the maximum unassigned integer.

Defaults

No queue limit

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

When you use the **ipx sap-queue-maximum** command to control how many SAP packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming SAP request packets are dropped. Be sure to set a large enough queue limit to handle normal incoming SAP requests on all interfaces, or else the SAP information may time out.

Examples

The following example sets a SAP queue maximum of 500 milliseconds:

```
ipx sap-queue-maximum 500
```

Related Commands

Command	Description
ipx rip-queue-maximum	Sets an IPX RIP queue maximum to control how many RIP packets can be waiting to be processed at any given time.
ipx rip-update-queue-maximum	Sets an IPX RIP queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time.
ipx sap-update-queue-maximum	Sets an IPX SAP queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time.

ipx sap-update-queue-maximum

To set an IPX Service Advertising Protocol (SAP) queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time, use the **ipx sap-update-queue-maximum** command in global configuration mode. To clear a set SAP queue maximum, use the **no** form of this command.

ipx sap-update-queue-maximum *queue-maximum*

no ipx sap-update-queue-maximum *queue-maximum*

Syntax Description

queue-maximum	Specifies the queue limit as a number from 0 to the maximum unassigned integer.

Defaults

No queue limit

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

When you use the **ipx sap-update-queue-maximum** command to control how many incoming SAP update packets can be waiting to be processed at any given time, remember that if the queue limit is reached, the incoming SAP update packets are dropped.

Note When using the **ipx sap-update-queue-maximum** command, be sure to set this queue high enough to handle a full update on all interfaces, or else the SAP information may time out.

Examples

The following example sets a SAP update queue maximum of 500:

```
ipx sap-update-queue-maximum 500
```

Related Commands

Command	Description
ipx rip-queue-maximum	Sets an IPX RIP queue maximum to control how many RIP packets can be waiting to be processed at any given time.
ipx rip-update-queue-maximum	Sets an IPX RIP queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time.
ipx sap-queue-maximum	Sets an IPX SAP queue maximum to control how many SAP packets can be waiting to be processed at any given time.

ipx server-split-horizon-on-server-paths

To control whether Service Information split horizon checking should be based on Router Information Protocol (RIP) paths or Service Advertising Protocol (SAP) paths, use the **ipx server-split-horizon-on-server-paths** command in global configuration mode. To return to the normal mode of following route paths, use the **no** form of this command.

ipx server-split-horizon-on-server-paths

no ipx server-split-horizon-on-server-paths

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

By default, split horizon prevents information about periodic SAPs from being advertised by a router to the same interface in which the best route to that SAP is learned. However, in an instance where the SAP may be learned from interfaces other than, or in addition to, the interface on which the best route to that SAP is learned, using the **ipx server-split-horizon-on-server-paths** command may reduce the number of unnecessary periodic SAP updates. The reduction in the number of SAP updates occurs because each SAP will not be advertised on the interface or interfaces it was learned from. The reduction in the number of SAP updates will also prevent a potential SAP loop in the network.

Examples

The following example shows the application of split horizon blocks:

```
ipx server-split-horizon-on-server-paths
```

Related Commands

Command	Description
ipx eigrp-sap-split-horizon	Configures EIGRP SAP split horizon.
ipx maximum-paths	Sets the maximum number of equal-cost paths the Cisco IOS software uses when forwarding packets.
ipx sap-incremental split-horizon	Configures incremental SAP split horizon.
ipx split-horizon eigrp	Configures split horizon.

ipx split-horizon eigrp

To configure split horizon, use the **ipx split-horizon eigrp** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipx split-horizon eigrp *autonomous-system-number*

no ipx split-horizon eigrp *autonomous-system-number*

Syntax Description

autonomous-system-number	Enhanced Interior Gateway Routing Protocol (EIGRP) autonomous system number. It can be a number from 1 to 65,535.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When split horizon is enabled, Enhanced IGRP update and query packets are not sent for destinations that have next hops on this interface. This reduces the number of Enhanced IGRP packets on the network.

Split horizon blocks information about routes from being advertised by Cisco IOS software to any interface from which that information originated. Typically, this behavior optimizes communication among multiple routers, particularly when links are broken. However, with nonbroadcast networks, such as Frame Relay and Switched Multimegabit Data Service (SMDS), situations can arise for which this behavior is less than ideal. For these situations, you may wish to disable split horizon.

Examples

The following example disables split horizon on serial interface 0:

```
interface serial 0
 no ipx split-horizon eigrp 200
```

ipx spx-idle-time

To set the amount of time to wait before starting the spoofing of Sequenced Packet Exchange (SPX) keepalive packets following inactive data transfer, use the **ipx spx-idle-time** command in interface configuration mode. To disable the current delay time set by this command, use the **no** form of this command.

ipx spx-idle-time *delay-in-seconds*

no ipx spx-idle-time

Syntax Description

delay-in-seconds	The amount of time, in seconds, to wait before spoofing SPX keepalives after data transfer has stopped.

Defaults

60 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command sets the elapsed time in seconds after which spoofing of keepalive packets occurs, following the end of data transfer; that is, after the acknowledgment and sequence numbers of the data being transferred have stopped increasing. By default, SPX keepalive packets are sent from servers to clients every 15 to 20 seconds.

If you turn on SPX spoofing and you do not set an idle time, the default of 60 seconds is assumed. This means that the dialer idle time begins when SPX spoofing begins. For example, if the dialer idle time is 3 minutes, the elapse time before SPX spoofing begins is 4 minutes: 3 minutes of dialer idle time plus 1 minute of SPX spoofing idle time.

For this command to take effect, you must first use the **ipx spx-spoof** interface configuration command to enable SPX spoofing for the interface.

Examples

The following example enables spoofing on serial interface 0 and sets the idle timer to 300 seconds:

```
interface serial 0
 ipx spx-spoof
 no ipx route-cache
 ipx spx-idle-time 300
```

Related Commands

Command	Description
ipx spx-spoof	Configures Cisco IOS software to respond to a client or server SPX keepalive packets on behalf of a remote system so that a DDR link will go idle when data has stopped being transferred.
show ipx spx-spoof	Displays the table of SPX connections through interfaces for which SPX spoofing is enabled.

ipx spx-spoof

To configure Cisco IOS software to respond to a client or server's Sequenced Packet Exchange (SPX) keepalive packets on behalf of a remote system so that a dial-on-demand (DDR) link will go idle when data has stopped being transferred, use the **ipx spx-spoof** command in interface configuration mode. To disable spoofing, use the **no** form of this command.

ipx spx-spoof [**session-clear** *session-clear-minutes* | **table-clear** *table-clear-hours*]

no ipx spx-spoof [**session-clear** | **table-clear**]

Syntax Description

session-clear	(Optional) Sets the time to clear inactive entries. Values are 0 through 4,294,967,295.
table-clear	(Optional) Sets the time to clear the SPX table.
session-clear-minutes	(Optional) Number of minutes before inactive entries are cleared from the session. Values are 0 through 4,294,967,295.
table-clear-hours	(Optional) Number of hours before the IPX table is cleared. Values are 0 through 4,294,967,295.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

You can use the **ipx spx-spoof** command on any serial dialer or point-to-point interface. Fast switching and autonomous switching must be disabled on the interface; otherwise, SPX spoofing will not be permitted.

SPX keepalive packets are sent from servers to clients every 15 to 20 seconds after a client session has been idle for a certain period of time following the end of data transfer and after which only unsolicited acknowledgments are sent. The idle time may vary, depending on parameters set by the client and server.

Because of acknowledgment packets, a session would never go idle on a DDR link. On pay-per-packet or byte networks, these keepalive packets can incur for the customer large phone connection charges for idle time. You can prevent these calls from being made by configuring the software to respond to the server's keepalive packets on a remote client's behalf. This is sometimes referred to as "spoofing the server."

You can use the **ipx spx-idle-time** command to set the elapsed time in seconds after which spoofing of keepalive packets occurs, following the end of data transfer. If you turn on SPX spoofing and you do not set an idle time, the default of 60 seconds is assumed. This means that the dialer idle time begins when SPX spoofing begins. For example, if the dialer idle time is 3 minutes, the elapse time before the line goes "idle-spoofing" is 4 minutes: 3 minutes of dialer idle time plus 1 minute of SPX spoofing idle time.

Examples

The following example enables spoofing on serial interface 0:

```
interface serial 0
 ipx spx-spoof
 no ipx route-cache
```

Related Commands

Command	Description
ipx throughput	Configures the throughput.
show ipx spx-spoof	Displays the table of SPX connections through interfaces for which SPX spoofing is enabled.

ipx throughput

To configure the throughput, use the **ipx throughput** command in interface configuration mode. To revert to the current bandwidth setting for the interface, use the **no** form of this command.

ipx throughput *bits-per-second*

no ipx throughput *bits-per-second*

Syntax Description

bits-per-second	Throughput, in bits per second.

Defaults

Current bandwidth setting for the interface

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The value you specify with the **ipx throughput** command overrides the value measured by IPXWAN when it starts.

Examples

The following example changes the throughput to 1,000,000 bits per second:

```
ipx throughput 1000000
```

Related Commands

Command	Description
ipx ipxwan	Enables the IPXWAN protocol on a serial interface.

ipx triggered-rip-delay

To set the interpacket delay for triggered Routing Information Protocol (RIP) updates sent on a single interface, use the **ipx triggered-rip-delay** command in interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx triggered-rip-delay *delay*

no ipx triggered-rip-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet routing update. A triggered routing update is one that the system sends in response to a "trigger" event, such as a request packet, interface up/down, route up/down, or server up/down.

The **ipx triggered-rip-delay** command sets the interpacket delay for triggered routing updates sent on a single interface. The delay value set by this command overrides the delay value set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for triggered routing updates sent on the interface.

If the delay value set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command is high, then we strongly recommend a low delay value for triggered routing updates so that updates triggered by special events are sent in a more timely manner than periodic routing updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX machines. These machines may lose RIP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX machines.

The default delay on a NetWare 3.11 server is about 100 ms.

When you do not set the interpacket delay for triggered routing updates, the system uses the delay specified by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for both periodic and triggered routing updates.

When you use the **no** form of the **ipx triggered-rip-delay** command, the system uses the global default delay set by the **ipx default-triggered-rip-delay** command for triggered RIP updates, if it is set. If it is not set, the system uses the delay set by the **ipx output-rip-delay** or **ipx default-output-rip-delay** command for triggered RIP updates, if set. Otherwise, the system uses the initial default delay as described in the "Defaults" section.

This command is also useful on limited bandwidth point-to-point links, or X.25 and Frame Relay multipoint interfaces.

Examples

The following example sets an interpacket delay of 55 ms for triggered routing updates sent on interface FDDI 0:

```
interface FDDI 0
 ipx triggered-rip-delay 55
```

Related Commands

Command	Description
ipx default-output-rip-delay	Sets the default interpacket delay for RIP updates sent on all interfaces.
ipx default-triggered-rip-delay	Sets the default interpacket delay for triggered RIP updates sent on all interfaces.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.

ipx triggered-rip-holddown

To set the amount of time for which an IPX Routing Information Protocol (RIP) process will wait before sending flashes about RIP changes, use the **ipx triggered-rip-holddown** command in interface configuration mode. To remove the RIP hold-down, use the **no** form of this command.

ipx triggered-rip-holddown *milliseconds*

no ipx triggered-rip-holddown *milliseconds*

Syntax Description

milliseconds	Amount of time, in milliseconds, for which the router will wait before sending flashes about RIP changes.

Defaults

55 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

To set a default hold-down used for all interfaces, use the **ipx default-triggered-rip-holddown** command in global configuration mode.

Examples

The following example shows a hold-down time of 100 milliseconds:

```
interface ether 0
 ipx triggered-rip-holddown 100
```

Related Commands

Command	Description
ipx default-triggered-rip-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-rip-holddown** command.
ipx default-triggered-sap-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-sap-holddown** command.
ipx triggered-sap-holddown	Sets an amount of time a SAP process will wait before sending flashes about SAP changes.

ipx triggered-sap-delay

To set the interpacket delay for triggered Service Advertising Protocol (SAP) updates sent on a single interface, use the **ipx triggered-sap-delay** command in interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx triggered-sap-delay *delay*

no ipx triggered-sap-delay [*delay*]

Syntax Description

delay	Delay, in milliseconds, between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

Defaults

55 ms

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The interpacket delay is the delay between the individual packets sent in a multiple-packet SAP update. A triggered SAP update is one that the system sends in response to a "trigger" event, such as a request packet, interface up/down, route up/down, or server up/down.

The **ipx triggered-sap-delay** command sets the interpacket delay for triggered updates sent on a single interface. The delay value set by this command overrides the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered updates sent on the interface.

If the delay value set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command is high, then we strongly recommend a low delay value for triggered updates so that updates triggered by special events are sent in a more timely manner than periodic updates.

Novell recommends a delay of 55 ms for compatibility with older and slower IPX servers. These servers may lose SAP updates because they process packets more slowly than the router sends them. The delay imposed by this command forces the router to pace its output to the slower-processing needs of these IPX servers.

The default delay on a NetWare 3.11 server is about 100 ms.

When you do not set the interpacket delay for triggered updates, the system uses the delay specified by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for both periodic and triggered SAP updates.

When you use the **no** form of the **ipx triggered-sap-delay** command, the system uses the global default delay set by the **ipx default-triggered-sap-delay** command for triggered SAP updates, if it is set. If it is not set, the system uses the delay set by the **ipx output-sap-delay** or **ipx default-output-sap-delay** command for triggered SAP updates, if set. Otherwise, the system uses the initial default delay as described in the "Defaults" section.

This command is also useful on limited bandwidth point-to-point links, or X.25 and Frame Relay multipoint interfaces.

Examples

The following example sets an interpacket delay of 55 ms for triggered SAP updates sent on interface FDDI 0:

```
interface FDDI 0
 ipx triggered-sap-delay 55
```

Related Commands

Command	Description
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx default-triggered-sap-delay	Sets the default interpacket delay for triggered SAP updates sent on all interfaces.
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.

ipx triggered-sap-holddown

To set the amount of time for which a Service Advertising Protocol (SAP) process will wait before sending flashes about SAP changes, use the **ipx triggered-sap-holddown** command in interface configuration mode. To remove the SAP hold-down, use the **no** form of this command.

ipx triggered-sap-holddown *milliseconds*

no ipx triggered-sap-holddown *milliseconds*

Syntax Description

milliseconds	Amount of time, in milliseconds, for which the router will wait before sending flashes about RIP changes.

Defaults

55 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

To set a default hold-down used for all interfaces, use the **ipx default-triggered-sap-holddown** command in global configuration mode.

Examples

The following example shows a hold-down time of 100 milliseconds:

```
interface ethernet 0
 ipx triggered-sap-holddown 100
```

Related Commands

Command	Description
ipx default-triggered-rip-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-rip-holddown** command.
ipx-default-triggered-sap-holddown	Sets a default hold-down time used for all interfaces for the **ipx triggered-sap-holddown** command.
ipx triggered-rip-holddown	Sets an amount of time an IPX RIP process will wait before sending flashes about RIP changes.

ipx type-20-helpered

To forward IPX type 20 propagation packet broadcasts to specific network segments, use the **ipx type-20-helpered** command in global configuration mode. To disable this function, use the **no** form of this command.

ipx type-20-helpered

no ipx type-20-helpered

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **ipx type-20-helpered** command disables the input and output of type 20 propagation packets as done by the **ipx type-20-propagation** interface configuration command.

The **ipx type-20-propagation** command broadcasts type 20 packets to all nodes on the network and imposes a hop-count limit of eight routers for broadcasting these packets. These functions are in compliance with the Novell IPX router specification. In contrast, the **ipx type-20-helpered** command broadcasts type 20 packets to only those nodes indicated by the **ipx helper-address** interface configuration command and extends the hop-count limit to 16 routers.

Use of the **ipx type-20-helpered** command does not comply with the Novell IPX router specification; however, you may need to use this command if you have a mixed internetwork that contains routers running Software Release 9.1 and routers running later versions of Cisco IOS software.

Examples

The following example forwards IPX type 20 propagation packet broadcasts to specific network segments:

```
interface ethernet 0
 ipx network aa
 ipx type-20-helpered
 ipx helper-address bb.ffff.ffff.ffff
```

Related Commands

Command	Description
ipx helper-address	Forwards broadcast packets to a specified server.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx type-20-input-checks

To restrict the acceptance of IPX type 20 propagation packet broadcasts, use the **ipx type-20-input-checks** command in global configuration mode. To remove these restrictions, use the **no** form of this command.

ipx type-20-input-checks

no ipx type-20-input-checks

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

By default, Cisco IOS software is configured to block type 20 propagation packets. When type 20 packet handling is enabled on multiple interfaces, you can use the **ipx type-20-input-checks** command to impose additional restrictions on the acceptance of type 20 packets. Specifically, the software will accept type 20 propagation packets only on the single network that is the primary route back to the source network. Similar packets received via other networks will be dropped. This behavior can be advantageous in redundant topologies, because it reduces unnecessary duplication of type 20 packets.

Examples

The following example imposes additional restrictions on incoming type 20 broadcasts:

```
ipx type-20-input-checks
```

Related Commands

Command	Description
ipx type-20-output-checks	Restricts the forwarding of IPX type 20 propagation packet broadcasts.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx type-20-output-checks

To restrict the forwarding of IPX type 20 propagation packet broadcasts, use the **ipx type-20-output-checks** command in global configuration mode. To remove these restrictions, use the **no** form of this command.

ipx type-20-output-checks

no ipx type-20-output-checks

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

By default, Cisco IOS software is configured to block type 20 propagation packets. When type 20 packet handling is enabled on multiple interfaces, you can use the **ipx type-20-output-checks** command to impose additional restrictions on outgoing type 20 packets. Specifically, the software will forward these packets only to networks that are not routes back to the source network. (The software uses the current routing table to determine routes.) This behavior can be advantageous in redundant topologies, because it reduces unnecessary duplication of type 20 packets.

Examples

The following example imposes restrictions on outgoing type 20 broadcasts:

```
ipx type-20-output-checks
```

Related Commands

Command	Description
ipx type-20-input-checks	Restricts the acceptance of IPX type 20 propagation packet broadcasts.
ipx type-20-propagation	Forwards IPX type 20 propagation packet broadcasts to other network segments.

ipx type-20-propagation

To forward IPX type 20 propagation packet broadcasts to other network segments, use the **ipx type-20-propagation** command in interface configuration mode. To disable both the reception and forwarding of type 20 broadcasts on an interface, use the **no** form of this command.

ipx type-20-propagation

no ipx type-20-propagation

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Routers normally block all broadcast requests. To allow input and output of type 20 propagation packets on an interface, use the **ipx type-20-propagation** command. Note that type 20 packets are subject to loop detection and control as specified in the IPX router specification.

Additional input and output checks may be imposed by the **ipx type-20-input-checks** and **ipx type-20-output-checks** commands.

IPX type 20 propagation packet broadcasts are subject to any filtering defined by the **ipx helper-list** command.

Examples

The following example enables both the reception and forwarding of type 20 broadcasts on Ethernet interface 0:

```
interface ethernet 0
 ipx type-20-propagation
```

The following example enables the reception and forwarding of type 20 broadcasts between networks 123 and 456, but does not enable reception and forwarding of these broadcasts to and from network 789:

```
interface ethernet 0
 ipx network 123
 ipx type-20-propagation
!
interface ethernet 1
 ipx network 456
 ipx type-20-propagation
!
interface ethernet 2
 ipx network 789
```

Related Commands

Command	Description
ipx helper-list	Assigns an access list to an interface to control broadcast traffic (including type 20 propagation packets).
ipx type-20-input-checks	Restricts the acceptance of IPX type 20 propagation packet broadcasts.
ipx type-20-output-checks	Restricts the forwarding of IPX type 20 propagation packet broadcasts.

ipx update interval

To adjust the Routing Information Protocol (RIP) or Service Advertising Protocol (SAP) update interval, use the **ipx update interval** command in interface configuration mode. To restore the default values, use the **no** form of this command.

ipx update interval {**rip** | **sap**} {*value* | **changes-only**}

no ipx update interval {**rip** | **sap**}

Syntax Description

rip	Adjusts the interval at which RIP updates are sent. The minimum interval is 10 seconds.
sap	Adjusts the interval at which SAP updates are sent. The minimum interval is 10 seconds.
value	The interval specified in seconds.
changes-only	Specifies the sending of a SAP or RIP update when the link comes up, when the link is downed administratively, or when service information changes. This parameter is supported for both SAP and RIP updates.

Defaults

The default interval is 60 seconds for both IPX routing updates and SAP updates.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command replaces two commands found in previous releases of Cisco IOS software: **ipx sap-interval** and **ipx update-time**.

Routers exchange information about routes by sending broadcast messages when they are started up and shut down, and periodically while they are running. The **ipx update interval** command enables you to modify the periodic update interval. By default, this interval is 60 seconds (this default is defined by Novell).

You should set RIP timers only in a configuration in which all routers are Cisco routers or in which all other IPX routers allow configurable timers. The timers should be the same for all devices connected to the same cable segment.

The update value you choose affects the internal IPX timers as follows:

- IPX routes are marked invalid if no routing updates are heard within three times the value of the update interval and are advertised with a metric of infinity.
- IPX routes are removed from the routing table if no routing updates are heard within four times the value of the update interval.

Setting the interval at which SAP updates are sent is most useful on limited-bandwidth links, such as slower-speed serial interfaces.

You should ensure that all IPX servers and routers on a given network have the same SAP interval. Otherwise, they may decide that a server is down when it is really up.

It is not possible to change the interval at which SAP updates are sent on most PC-based servers. This means that you should never change the interval for an Ethernet or Token Ring network that has servers on it.

You can set the router to send an update only when changes have occurred. Using the **changes-only** keyword specifies the sending of a SAP update only when the link comes up, when the link is downed administratively, or when the databases change. The **changes-only** keyword causes the router to do the following:

- Send a single, full broadcast update when the link comes up.
- Send appropriate triggered updates when the link is shut down.
- Send appropriate triggered updates when specific service information changes.

Examples

The following example configures the update timers for RIP updates on two interfaces in a router:

```
interface serial 0
 ipx update interval rip 40

interface ethernet 0
 ipx update interval rip 20
```

The following example configures SAP updates to be sent (and expected) on serial interface 0 every 300 seconds (5 minutes) to reduce periodic update overhead on a slow-speed link:

```
interface serial 0
 ipx update interval sap 300
```

Related Commands

Command	Description
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx output-sap-delay	Sets the interpacket delay for SAP updates sent on a single interface.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.
show ipx interface	Displays the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface.

ipx update sap-after-rip

To configure the router to send a Service Advertising Protocol (SAP) update immediately following a Routing Information Protocol (RIP) broadcast, use the **ipx update sap-after-rip** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx update sap-after-rip

no ipx update sap-after-rip

Syntax Description

This command has no arguments or keywords.

Defaults

RIP and SAP updates are sent every 60 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **ipx update sap-after-rip** command causes the router to issue a SAP update immediately following a RIP broadcast. This ensures that the SAP update follows the RIP broadcast, and that the SAP update is sent using the RIP update interval. It also ensures that the receiving router has learned the route to the service interface via RIP prior to getting the SAP broadcast.

Examples

The following example configures the router to issue a SAP broadcast immediately following a RIP broadcast on serial interface 0.

```
interface serial 0
 ipx update sap-after-rip
```

Related Commands

Command	Description
ipx linkup-request	Enables the sending of a general RIP or SAP query when an interface comes up.
ipx update interval	Adjusts the RIP or SAP update interval.
show ipx interface	Displays the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface.

ipx watchdog

To enable watchdog, use the **ipx watchdog** command in interface configuration mode. To specify filtering, spoofing, or how long spoofing is to be enabled or disabled, use arguments and keywords. To disable filtering or spoofing, use the **no** form of this command.

ipx watchdog {**filter** | **spoof** [*enable-time-hours disable-time-minutes*]}

no ipx watchdog {**filter** | **spoof**}

Syntax Description

filter	Discards IPX server watchdog packets when a DDR link is not connected.
spoof	Answers IPX server watchdog packets when a DDR link is not connected.
enable-time-hours	(Optional) Number of consecutive hours spoofing is to stay enabled. Values are 1 through 24.
disable-time-minutes	(Optional) Number of consecutive minutes spoofing is to stay disabled. Values are 18 through 1440.

Defaults

There is no watchdog processing.

Command Modes

Interface configuration

Command History

Release	Modification
11.2(9.1)	This command was introduced. This command replaces the **ipx watchdog-spoof** command.

Usage Guidelines

Use the **ipx watchdog** command when you want to enable watchdog processing. Use this command only on a serial interface with dial-on-demand (DDR) routing enabled.

Using the **filter** keyword when the DDR link is not connected will cause IPX server watchdog packets to be discarded, preventing them from bringing the DDR link up again.

Using the **spoof** keyword will allow IPX server watchdog packets to be answered when the DDR link is not connected. You can control how long spoofing is to be enabled or disabled by using the *enable-time-hours* and *disable-time-minutes* arguments.

Related Commands

Command	Description
ipx route-cache	Enables IPX fast switching.
ipx spx-spoof	Configures Cisco IOS software to respond to a client or server SPX keepalive packets on behalf of a remote system so that a DDR link will go idle when data has stopped being transferred.

ipx watchdog-spoof

The **ipx watchdog-spoof** command is replaced by the **ipx watchdog** command. See the description of the **ipx watchdog** command in this chapter for more information.

log-neighbor-changes (EIGRP)

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **log-neighbor-changes** command in IPX-router configuration mode. To disable this function, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Defaults

No adjacency changes are logged.

Command Modes

IPX-router configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Enable the logging of neighbor adjacency changes in order to monitor the stability of the routing system and to help detect problems. Log messages are of the following form:

`%DUAL-5-NBRCHANGE: IPX EIGRP` *as-number* `: Neighbor` *address* `(`*interface*`) is` *state*`:` *reason*

where the arguments have the following meanings:

as-number	Autonomous system number
address (interface)	Neighbor address
state	Up or down
reason	Reason for change

Examples

The following configuration will log neighbor changes for Enhanced IGRP process 209:

```
ipx router eigrp 209
 log-neighbor-changes
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

lsp-gen-interval (IPX)

To set the minimum interval at which link-state packets (LSPs) are generated, use the **lsp-gen-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

lsp-gen-interval *seconds*

no lsp-gen-interval *seconds*

Syntax Description

seconds	Minimum interval, in seconds. It can be a number in the range 0 to 120. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **lsp-gen-interval** command controls the rate at which LSPs are generated on a per-LSP basis. For instance, if a link is changing state at a high rate, the default value of the LSP generation interval limits the signaling of this change to once every 5 seconds. Because the generation of an LSP may cause all routers in the area to perform the SPF calculation, controlling this interval may have area-wide impact. Raising this interval can reduce the load on the network imposed by a rapidly changing link.

Examples

The following example sets the minimum interval at which LSPs are generated to 10 seconds:

```
lsp-gen-interval 10
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
spf-interval	Controls how often Cisco IOS software performs the SPF calculation.

lsp-mtu (IPX)

To set the maximum size of a link-state packet (LSP) generated by Cisco IOS software, use the **lsp-mtu** command in router configuration mode. To restore the default Maximum Transmission Unit (MTU) size, use the **no** form of this command.

lsp-mtu *bytes*

no lsp-mtu *bytes*

Syntax Description

bytes	MTU size, in bytes. It can be a number in the range 512 to 4096. The default is 512 bytes.

Defaults

512 bytes

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

You can increase the LSP MTU if there is a very large amount of information generated by a single router, because each device is limited to approximately 250 LSPs. In practice, this should never be necessary.

The LSP MTU must never be larger than the smallest MTU of any link in the area. This is because LSPs are flooded throughout the area.

The **lsp-mtu** command limits the size of LSPs generated by this router only; Cisco IOS software can receive LSPs of any size up to the maximum.

Examples

The following example sets the maximum LSP size to 1500 bytes:

```
lsp-mtu 1500
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

lsp-refresh-interval (IPX)

To set the link-state packet (LSP) refresh interval, use the **lsp-refresh-interval** command in router configuration mode. To restore the default refresh interval, use the **no** form of this command.

lsp-refresh-interval *seconds*

no lsp-refresh-interval *seconds*

Syntax Description

seconds	Refresh interval, in seconds. It can be a value in the range 1 to 50,000 seconds. The default is 7200 seconds (2 hours).

Defaults

7200 seconds (2 hours)

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The refresh interval determines the rate at which Cisco IOS software periodically transmits the route topology information that it originates. This is done in order to keep the information from becoming too old. By default, the refresh interval is 2 hours.

LSPs must be periodically refreshed before their lifetimes expire. The refresh interval must be less than the LSP lifetime specified with the **max-lsp-lifetime (IPX)** router configuration command. Reducing the refresh interval reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. (This is an extremely unlikely event, however, because there are other safeguards against corruption.) Increasing the interval reduces the link utilization caused by the flooding of refreshed packets (although this utilization is very small).

Examples

The following example changes the LSP refresh interval to 10,800 seconds (3 hours):

```
lsp-refresh-interval 10800
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
max-lsp-lifetime (IPX)	Sets the maximum time that LSPs persist without being refreshed.

max-lsp-lifetime (IPX)

To set the maximum time for which link-state packets (LSPs) persist without being refreshed, use the **max-lsp-lifetime** command in router configuration mode. To restore the default time, use the **no** form of this command.

max-lsp-lifetime [**hours**] *value*

no max-lsp-lifetime

Syntax Description

hours	(Optional) If specified, the lifetime of the LSP is set in hours. If not specified, the lifetime is set in seconds.
value	Lifetime of LSP, in hours or seconds. It can be a number in the range 1 to 32,767. The default is 7500 seconds.

Defaults

7500 seconds (2 hours, 5 minutes)

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **hours** keyword enables the router to interpret the maximum lifetime field in hours, allowing the router to keep LSPs for a much longer time. Keeping LSPs longer reduces overhead on slower-speed serial links and keeps ISDN links from becoming active unnecessarily.

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval (IPX)** router configuration command. The maximum LSP lifetime must be greater than the LSP refresh interval.

Examples

The following example sets the maximum time that the LSP persists to 11,000 seconds (more than 3 hours):

```
max-lsp-lifetime 11000
```

The following example sets the maximum time that the LSP persists to 15 hours:

```
max-lsp-lifetime hours 15
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
lsp-refresh-interval (IPX)	Sets the LSP refresh interval.

netbios access-list (IPX)

To define an IPX NetBIOS FindName access list filter, use the **netbios access-list** command in global configuration mode. To remove a filter, use the **no** form of this command.

netbios access-list host *name* {**deny** | **permit**} *string*

no netbios access-list host *name* {**deny** | **permit**} *string*

netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*

no netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*

Syntax Description

host	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.
name	Name of the access list being defined. The name can be an alphanumeric string.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
string	Character string that identifies one or more NetBIOS host names. It can be up to 14 characters long. The argument *string* can include the following wildcard characters: • *—Matches one or more characters. You can use this wildcard character only at the end of a string. • ?—Matches any single character.
bytes	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.
offset	Decimal number that indicates the number of bytes into the packet at which the byte comparison should begin. An offset of 0 indicates the beginning of the NetBIOS packet header, which is at the end of the IPX header.
byte-pattern	Hexadecimal pattern that represents the byte pattern to match. It can be up to 16 bytes (32 digits) long and must be an even number of digits. The argument *byte-pattern* can include the double asterisk (**) wildcard character to match any digits for that byte.

Defaults

No filters are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Keep the following points in mind when configuring IPX NetBIOS access control:

- Host (node) names are case-sensitive.
- Host and byte access lists can have the same names. They are independent of each other.
- When filtering by node name for IPX NetBIOS, the names in the access lists are compared with the destination name field for IPX NetBIOS "find name" requests.
- When filtering by byte offset, note that these access filters can have a significant impact on the packets' transmission rate across the bridge because each packet must be examined. You should use these access lists only when absolutely necessary.
- If a node name is not found in an access list, the default action is to deny access.

These filters apply only to IPX NetBIOS FindName packets. They have no effect on LLC2 NetBIOS packets.

To delete an IPX NetBIOS access list, specify the minimum number of keywords and arguments needed to delete the proper list. For example, to delete the entire list, use the following command:

no netbios access-list {**host** | **bytes**} *name*

To delete a single entry from the list, use the following command:

no netbios access-list host *name* {**permit** | **deny**} *string*

Examples

The following example defines the IPX NetBIOS access list engineering:

```
netbios access-list host engineering permit eng-ws1 eng-ws2 eng-ws3
```

The following example removes a single entry from the engineering access list:

```
netbios access-list host engineering deny eng-ws3
```

The following example removes the entire engineering NetBIOS access list:

```
no netbios access-list host engineering
```

Related Commands

Command	Description
ipx netbios input-access-filter	Controls incoming IPX NetBIOS FindName messages.
ipx netbios output-access-filter	Controls outgoing NetBIOS FindName messages.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

network (IPX Enhanced IGRP)

To enable Enhanced Interior Gateway Routing Protocol (EIGRP), use the **network** (IPX Enhanced IGRP) command in router configuration mode. To disable Enhanced IGRP, use the **no** form of this command.

network {*network-number* | **all**}

no network {*network-number* | **all**}

Syntax Description

network-number	IPX network number.
all	Enables the routing protocol for all IPX networks configured on the router.

Defaults

Disabled

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use the **network** (IPX Enhanced IGRP) command to enable the routing protocol specified in the **ipx router** command on each network.

Examples

The following commands disable RIP on network 10 and enable Enhanced IGRP on networks 10 and 20:

```
ipx router rip
 no network 10

ipx router eigrp 12
 network 10
 network 20
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.

permit (IPX extended)

To set conditions for a named IPX extended access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

no permit *protocol* [*source-network*][[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*][[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-nodemask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description

protocol	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. You can also use the keyword **any** to match all protocol types.
source-network	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword **any** to match all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
.source-node	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
source-network-mask.	(Optional) Mask to be applied to the *source-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *source-node-mask* argument.
source-socket	Socket name or number (hexadecimal) from which the packet is being sent. You can also use the word **all** to match all sockets.

destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword **any** to match all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.destination-node	(Optional) Node on destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network-mask.	(Optional) Mask to be applied to the *destination-network* argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the *destination-node-mask* argument.
destination-socket	(Optional) Socket name or number (hexadecimal) to which the packet is being sent.
log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.

Defaults

There is no specific condition under which a packet passes the named access list.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(1)T	The following keyword and argument were added: • **time-range** • *time-range-name*

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on IPX protocol names and numbers, and IPX socket names and numbers, see the **access-list** (IPX extended) command.

Examples

The following example creates an extended access list named *sal* that denies all SPX packets and permits all others:

```
ipx access-list extended sal
 deny spx any all any all log
 permit any
```

The following example provides a time range to permit access:

```
time-range no-spx
 periodic weekdays 8:00 to 18:00
!
ipx access-list extended test
 permit spx any all any all time-range no spx
```

Related Commands

Command	Description
access-list (IPX extended)	Defines an extended Novell IPX access list.
deny (extended)	Sets conditions for a named IPX extended access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

permit (IPX standard)

To set conditions for a named IPX access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *source-network*[.*source-node* [*source-node-mask*]]
[*destination-network*[.*destination-node*[*destination-node-mask*]]]

no permit *source-network*[.*source-node* [*source-node-mask*]]
[*destination-network*[.*destination-node*[*destination-node-mask*]]]

Syntax Description

source-network	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*source-node*	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
source-node-mask	(Optional) Mask to be applied to the *source-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.
destination-network	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.*destination-node*	(Optional) Node on the destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
destination-node-mask	(Optional) Mask to be applied to the *destination-node* argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on creating IPX access lists, see the **access-list** (IPX standard) command.

Examples

The following example creates a standard access list named *fred*. It permits communication with only IPX network number 5678.

```
ipx access-list standard fred
 permit 5678 any
 deny any
```

Related Commands

Command	Description
access-list (IPX standard)	Defines a standard IPX access list.
deny (standard)	Sets conditions for a named IPX access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

permit (SAP filtering)

To set conditions for a named IPX Service Advertising Protocol (SAP) filtering access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *network*[*.node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

no permit *network*[*.node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]

Syntax Description

network	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of –1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
.node	(Optional) Node on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).
network-mask.node-mask	(Optional) Mask to be applied to the *network* and *node* arguments. Place ones in the bit positions to be masked.
service-type	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.
server-name	(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

Defaults

No access lists are defined.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use this command following the **ipx access-list** command to specify conditions under which a packet passes the named access list.

For additional information on IPX SAP service types, see the **access-list** (SAP filtering) command.

Examples

The following example creates a SAP access list named MyServer that allows only MyServer to be sent in SAP advertisements:

```
ipx access-list sap MyServer
 permit 1234 4 MyServer
```

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
deny (SAP filtering)	Sets conditions for a named IPX SAP filtering access list.
ipx access-group	Applies generic input and output filters to an interface.
ipx access-list	Defines an IPX access list by name.
show ipx access-list	Displays the contents of all current IPX access lists.

prc-interval (IPX)

To control the hold-down period between partial route calculations, use the **prc-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds*

no prc-interval *seconds*

Syntax Description

seconds	Minimum amount of time between partial route calculations, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **prc-interval** command controls how often Cisco IOS software can performs a partial route (PRC) calculation. The PRC calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially on slower router models. Increasing the PRC interval reduces the processor load of the router, but potentially slows down the rate of convergence.

This command is analogous to the **spf-interval** command, which controls the hold-down period between shortest path first calculations.

Examples

The following example sets the PRC calculation interval to 20 seconds:

```
prc-interval 20
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
spf-interval	Controls how often Cisco IOS software performs the SPF calculation.

redistribute (IPX)

To redistribute from one routing domain into another, and vice versa, use one of the following **redistribute** commands in router configuration mode. To disable this feature, use the **no** form of these commands.

For Enhanced Interior Gateway Routing Protocol (EIGRP) or Routing Information Protocol (RIP) environments, use the following command to redistribute from one routing domain into another, and vice versa:

redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **rip** | **static**}

no redistribute {**connected** | **eigrp** *autonomous-system-number* | **floating-static** | **rip** | **static**}

Syntax Description

connected	Specifies connected routes.
eigrp *autonomous-system-number*	Specifies the Enhanced IGRP protocol and the Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
floating-static	Specifies a floating static route. This is a static route that can be overridden by a dynamically learned route.
rip	Specifies the RIP protocol. You can configure only one RIP process on the router. Thus, you cannot redistribute RIP into RIP.
static	Specifies static routes.
access-list *name*	(Optional) Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

Redistribution is enabled between all routing domains except between separate Enhanced IGRP processes.

Redistribution of floating static routes is disabled.

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	The **access-list** keyword and *access-list-number* argument have been removed.

Usage Guidelines

Redistribution provides for routing information generated by one protocol to be advertised in another.

The only connected routes affected by this redistribute command are the routes not specified by the **network** command.

If you have enabled floating static routes by specifying the **floating** keyword in the **ipx route** global configuration command and you redistribute floating static routes into a dynamic IPX routing protocol, any nonhierarchical topology causes the floating static destination to be redistributed immediately via a dynamic protocol back to the originating router, causing a routing loop. This occurs because dynamic protocol information overrides floating static routes. For this reason, automatic redistribution of floating static routes is off by default. If you redistribute floating static routes, you should specify filters to eliminate routing loops.

- Enhanced IGRP version 1.1 environments
- RIP version 1.1 environments

Examples

The following example does not redistributes RIP routing information:

```
ipx router eigrp 222
 no redistribute rip
```

The following example redistributes Enhanced IGRP routes from autonomous system 100 into Enhanced IGRP autonomous system 300:

```
ipx router eigrp 300
 redistribute eigrp 100
```

Related Commands

Command	Description
ipx access-list	Defines an IPX access list by name.
ipx router	Specifies the routing protocol to use.

show ipx access-list

To display the contents of all current IPX access lists, use the **show ipx access-list** command in EXEC mode.

show ipx access-list [*access-list-number* | *name*]

Syntax Description

access-list-number	(Optional) Number of the IPX access list to display. This is a number from 800 to 899, 900 to 999, 1000 to 1099, or 1200 to 1299.
name	(Optional) Name of the IPX access list to display.

Defaults

Displays all standard, extended, and Service Advertising Protocol (SAP) IPX access lists.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **show ipx access-list** command provides output identical to the **show access-lists** command, except that it is IPX specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ipx access-list** command when all access lists are requested:

```
Router# show ipx access-list

IPX extended access list 900
 deny any 1
IPX sap access list London
 deny FFFFFFFF 107
 deny FFFFFFFF 301C
 permit FFFFFFFF 0
```

The following is sample output from the **show ipx access-list** command when the name of a specific access list is requested:

```
Router# show ipx access-list London

IPX sap access list London
 deny FFFFFFFF 107
 deny FFFFFFFF 301C
 permit FFFFFFFF 0
```

show ipx accounting

To display the active or checkpoint accounting database, use the **show ipx accounting** command in EXEC mode.

show ipx accounting [**checkpoint**]

Syntax Description

checkpoint	(Optional) Displays entries in the checkpoint database.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ipx accounting** command:

```
Router# show ipx accounting

Source                  Destination               Packets           Bytes
0000C003.0000.0c05.6030 0000C003.0260.8c9b.4e33         72            2880
0000C001.0260.8c8d.da75 0000C003.0260.8c9b.4e33         14             624
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.da75         62            3110
0000C001.0260.8c8d.e7c6 0000C003.0260.8c9b.4e33         20            1470
0000C003.0260.8c9b.4e33 0000C001.0260.8c8d.e7c6         20            1470

Accounting data age is     6
```

Table 8 describes the fields shown in the display.

Table 8 show ipx accounting Field Descriptions

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets transmitted from the source address to the destination address.
Bytes	Number of bytes transmitted from the source address to the destination address.
Accounting data age is ...	Time since the accounting database has been cleared. It can be in one of the following formats: *mm*, *hh*:*mm*, *dd*:*hh*, and *ww*:*dd*, where *m* is minutes, *h* is hours, *d* is days, and *w* is weeks.

Related Commands

Command	Description
clear ipx accounting	Deletes all entries in the accounting database when IPX accounting is enabled.
ipx accounting	Enables IPX accounting.
ipx accounting-list	Filters networks for which IPX accounting information is kept.
ipx accounting-threshold	Sets the maximum number of accounting database entries.
ipx accounting-transits	Sets the maximum number of transit entries that will be stored in the IPX accounting database.

show ipx cache

To display the contents of the IPX fast-switching cache, use the **show ipx cache** command in EXEC mode.

show ipx cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ipx cache** command:

```
Router# show ipx cache

Novell routing cache version is 9
Destination          Interface              MAC Header
*1006A               Ethernet 0             00000C0062E600000C003EB0064
*14BB                Ethernet 1             00000C003E2A00000C003EB0064
```

Table 9 describes the fields shown in the display.

Table 9 show ipx cache Field Descriptions

Field	Description
Novell routing cache version is ...	Number identifying the version of the fast-switching cache table. It increments each time the table changes.
Destination	Destination network for this packet. Valid entries are marked by an asterisk (*).
Interface	Route interface through which this packet is transmitted.
MAC Header	Contents of this packet's MAC header.

Related Commands

Command	Description
clear ipx cache	Deletes entries from the IPX fast-switching cache.
ipx route-cache	Enables IPX fast switching.

show ipx eigrp interfaces

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ipx eigrp interfaces** command in EXEC mode.

show ipx eigrp interfaces [*type number*] [*as-number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
as-number	(Optional) Autonomous system number.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **show ipx eigrp interfaces** command to determine on which interfaces Enhanced IGRP is active and to find out information about Enhanced IGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which Enhanced IGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all Enhanced IGRP processes are displayed.

Examples

The following is sample output from the **show ipx eigrp interfaces** command:

```
Router> show ipx eigrp interfaces

IPX EIGRP interfaces for process 109

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
Di0           0         0/0          0      11/434          0          0
Et0           1         0/0        337       0/10           0          0
SE0:1.16      1         0/0         10       1/63         103          0
Tu0           1         0/0        330       0/16           0          0
```

Table 10 describes the fields shown in the display.

Table 10 show ipx eigrp interfaces Field Descriptions

Field	Description
process 109	Autonomous system number of the process.
Interface	Interface name.
Peers	Number of neighbors on the interface.

Table 10 show ipx eigrp interfaces Field Descriptions (continued)

Field	Description
Xmit Queue	Count of unreliable and reliable packets queued for transmission.
Mean SRTT	Average round-trip time for all neighbors on the interface.
Pacing Time	Number of milliseconds to wait after transmitting unreliable and reliable packets.
Multicast Flow Timer	Number of milliseconds to wait for acknowledgment of a multicast packet by all neighbors before transmitting the next multicast packet.
Pending Routes	Number of routes still to be transmitted on this interface.

Related Commands

Command	Description
show ipx eigrp neighbors	Displays the neighbors discovered by Enhanced IGRP.

show ipx eigrp neighbors

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ipx eigrp neighbors** command in EXEC mode.

show ipx eigrp neighbors [**servers**] [*autonomous-system-number* | *interface*] [**regexp** *name*]

Syntax Description

servers	(Optional) Displays the server list advertised by each neighbor. This is displayed only if the **ipx sap incremental** command is enabled on the interface on which the neighbor resides.
autonomous-system-number	(Optional) Autonomous system number. It can be a number from 1 to 65,535.
interface	(Optional) Interface type and number.
regexp *name*	(Optional) Displays the IPX servers whose names match the regular expression.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0	The following keyword and argument were added: • **regexp** • *name*

Examples

The following is sample output from the **show ipx eigrp neighbors** command:

```
Router# show ipx eigrp neighbors

IPX EIGRP Neighbors for process 1
H   Address                 Interface   Hold    Uptime   SRTT   RTO  Q  Seq
                                        (sec)            (ms)       Cnt Num
0   200.0000.0c34.d83b        Et0/2      11     00:00:18   2    200  0  10
2 total IPX servers for this peer
Type      Name                    Address             Port  Hops
          4 server                2037.0000.0000.0001:0001  2
          4 server2               2037.0000.0000.0001:0001  2
1   200.0000.0c34.d83c        Et0/2      11     00:00:18   2    200  0  10
1 total IPX servers for this peer
Type      Name                    Address             Port  Hops
          4 server                2037.0000.0000.0001:0001  2
```

Table 11 describes the fields shown in the display.

Table 11 show ipx eigrp neighbors Field Descriptions

Field	Description
process 200	Autonomous system number specified in the **ipx router** configuration command.
H	Handle. An arbitrary and unique number inside this router that identifies the neighbor.
Address	IPX address of the Enhanced IGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Length of time, in seconds, that Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, it will be reflected here.
Uptime	Elapsed time (in hours, minutes, and seconds) since the local router first heard from this neighbor.
Q Cnt	Number of IPX Enhanced IGRP packets (Update, Query, and Reply) that Cisco IOS software is waiting to send.
Seq Num	Sequence number of the last Update, Query, or Reply packet that was received from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds it takes for an IPX Enhanced IGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout, in milliseconds. This is the amount of time Cisco IOS software waits before retransmitting a packet from the retransmission queue to a neighbor.
RTO	Retransmission timeout, in milliseconds. This is the amount of time Cisco IOS software waits before retransmitting a packet from the retransmission queue to a neighbor.
Q Cnt	Number of IPX Enhanced IGRP packets (Update, Query, and Reply) that Cisco IOS software is waiting to send.
Seq Num	Sequence number of the last Update, Query, or Reply packet that was received from this neighbor.
Type	Contains codes from the Codes field to indicates how service was learned.
Name	Name of server.
Address	Network address of server.
Port	Source socket number.

Related Commands

Command	Description
ipx sap-incremental	Sends SAP updates only when a change occurs in the SAP table.

show ipx eigrp topology

To display the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show ipx eigrp topology** command in EXEC mode.

show ipx eigrp topology [*network-number*]

Syntax Description

network-number	(Optional) IPX network number whose topology table entry is to be displayed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ipx eigrp topology** command:

```
Router# show ipx eigrp topology

IPX EIGRP Topology Table for process 109
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 42, 1 successors, FD is 0
     via 160.0000.0c00.8ea9 (345088/319488), Ethernet0
P 160, 1 successor via Connected, Ethernet
     via 160.0000.0c00.8ea9 (307200/281600), Ethernet0
P 165, 1 successors, FD is 307200
     via Redistributed (287744/0)
     via 160.0000.0c00.8ea9 (313344/287744), Ethernet0
P 164, 1 successors, flags: U, FD is 200
     via 160.0000.0c00.8ea9 (307200/281600), Ethernet1
     via 160.0000.0c01.2b71 (332800/307200), Ethernet1
P A112, 1 successors, FD is 0
     via Connected, Ethernet2
     via 160.0000.0c00.8ea9 (332800/307200), Ethernet0
P AAABBB, 1 successors, FD is 10003
     via Redistributed (287744/0),
     via 160.0000.0c00.8ea9 (313344/287744), Ethernet0
A A112, 0 successors, 1 replies, state: 0, FD is 0
     via 160.0000.0c01.2b71 (307200/281600), Ethernet1
     via 160.0000.0c00.8ea9 (332800/307200), r, Ethernet1
```

Table 12 describes the fields shown in the display.

Table 12 show ipx eigrp topology Field Descriptions

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the Enhanced IGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P – Passive	No Enhanced IGRP computations are being performed for this destination.
A – Active	Enhanced IGRP computations are being performed for this destination.
U – Update	Indicates that an update packet was sent to this destination.
Q – Query	Indicates that a query packet was sent to this destination.
R – Reply	Indicates that a reply packet was sent to this destination.
r – Reply status	Flag that is set after Cisco IOS software has sent a query and is waiting for a reply.
42, 160, and so on	Destination IPX network number.
successors	Number of successors. This number corresponds to the number of next hops in the IPX routing table.
FD	Feasible distance. This value is used in the feasibility condition check. If the neighbor's reported distance (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the router determines it has a feasible successor, it does not have to send a query for that destination.
replies	Number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in Active state.
state	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
via	IPX address of the peer who told Cisco IOS software about this destination. The first *n* of these entries, where *n* is the number of successors, are the current successors. The remaining entries on the list are feasible successors.
(345088/319488)	The first number is the Enhanced IGRP metric that represents the cost to the destination. The second number is the Enhanced IGRP metric that this peer advertised.
Ethernet0	Interface from which this information was learned.

The following is sample output from the **show ipx eigrp topology** command when you specify an IPX network number:

```
Router# show ipx eigrp topology 160
```

```
IPX-EIGRP topology entry for 160
State is Passive, Query origin flag is 1, 1 Successor(s)
Routing Descriptor Blocks:
  Next hop is Connected (Ethernet0), from 0.0000.0000.0000
  Composite metric is (0/0), Send flag is 0x0, Route is Internal
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 1000000 nanoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 0
Next hop is 164.0000.0c00.8ea9 (Ethernet1), from 164.0000.0c00.8ea9
  Composite metric is (307200/281600), Send flag is 0x0, Route is External
  This is an ignored route
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 2000000 nanoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 1
  External data:
    Originating router is 0000.0c00.8ea9
    External protocol is RIP, metric is 1, delay 2
    Administrator tag is 0 (0x00000000)
    Flag is 0x00000000
```

Table 13 describes the fields shown in the display.

Table 13 show ipx eigrp topology Field Descriptions—Specific Network

Field	Description
160	IPX network number of the destination.
State is ...	State of this entry. It can be either Passive or Active. Passive means that no Enhanced IGRP computations are being performed for this destination, and Active means that they are being performed.
Query origin flag	Exact Enhanced IGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is Active.
Successor(s)	Number of successors. This number corresponds to the number of next hops in the IPX routing table.
Next hop is ...	Indicates how this destination was learned. It can be one of the following: • Connected—The destination is on a network directly connected to this router. • Redistributed—The destination was learned via RIP or another Enhanced IGRP process. • IPX host address—The destination was learned from that peer via this Enhanced IGRP process.
Ethernet0	Interface from which this information was learned.

Table 13 show ipx eigrp topology Field Descriptions—Specific Network (continued)

Field	Description
from	Peer from whom the information was learned. For connected and redistributed routers, this is 0.0000.0000.0000. For information learned via Enhanced IGRP, this is the peer's address. Currently, for information learned via Enhanced IGRP, the peer's IPX address always matches the address in the "Next hop is" field.
Composite metric is	Enhanced IGRP composite metric. The first number is this device's metric to the destination, and the second is the peer's metric to the destination.
Send flag	Numeric representation of the "flags" field described in Table 11. It is 0 when nothing is being sent, 1 when an Update is being sent, 3 when a Query is being sent, and 4 when a Reply is being sent. Currently, 2 is not used.
Route is ...	Type of router. It can be either internal or external. Internal routes are those that originated in an Enhanced IGRP autonomous system, and external are routes that did not. Routes learned through RIP are always external.
This is an ignored route	Indicates that this path is being ignored because of filtering.
Vector metric:	This section describes the components of the Enhanced IGRP metric.
Minimum bandwidth	Minimum bandwidth of the network used to reach the next hop.
Total delay	Delay time to reach the next hop.
Reliability	Reliability value used to reach the next hop.
Load	Load value used to reach the next hop.
Minimum MTU	Minimum MTU size of the network used to reach the next hop.
Hop count	Number of hops to the next hop.
External data:	This section describes the original protocol from which this route was redistributed. It appears only for external routes.
Originating router	Network address of the router that first distributed this route into Enhanced IGRP.
External protocol..metric..delay	External protocol from which this route was learned. The metric will match the external hop count displayed by the **show ipx route** command for this destination. The delay is the external delay.
Administrator tag	Not currently used.
Flag	Not currently used.

show ipx interface

To display the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface, use the **show ipx interface** command in EXEC mode.

show ipx interface [*type number*]

Syntax Description

type	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), FDDI, loopback, null, serial, Token Ring, or tunnel.
number	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to add Get General Service (GGS) filters and some counters per interface.

Examples

The following is sample output from the **show ipx interface** command:

```
Router# show ipx interface serial 2/0

Serial2/0 is up, line protocol is up
  IPX address is 123.00e0.1efc.0b01 [up]
  Delay of this IPX network, in ticks is 6 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 60 seconds
  IPX type 20 propagation packet forwarding is disabled
  Incoming access list is 900
  Outgoing access list is not set
  IPX helper access list is not set
  SAP GGS output filter list is 1000
  SAP GNS processing enabled, delay 0 ms, output filter list is not set
  SAP Input filter list is not set
  SAP Output filter list is not set
  SAP Router filter list is not set
  Input filter list is not set
  Output filter list is not set
  Router filter list is not set
  Netbios Input host access list is not set
  Netbios Input bytes access list is not set
  Netbios Output host access list is not set
  Netbios Output bytes access list is not set
  Updates each 60 seconds aging multiples RIP:3 SAP:3
  SAP interpacket delay is 55 ms, maximum size is 480 bytes
  RIP interpacket delay is 55 ms, maximum size is 432 bytes
  RIP response delay is not set
   Watchdog spoofing is currently enabled
        On duration 1 hour(s), 00:24:50 remaining
        Off duration 18 minute(s), 00:00:00 remaining
```

```
SPX spoofing is disabled, idle time 60
IPX accounting is disabled
IPX fast switching is configured (enabled)
RIP packets received 0, RIP packets sent 906, 0 Throttled
RIP specific requests received 0, RIP specific replies sent 0
RIP general requests received 0, 0 ignored, RIP general replies sent 0
SAP packets received 0, SAP packets sent 25, 0 Throttled
SAP GNS packets received 0,k SAP GNS replies sent 0
SAP GGS packets received 0, 0 ignored, SAP GGS replies sent 0
```

Table 14 describes the fields shown in the display.

Table 14 show ipx interface Field Descriptions

Field	Description
Serial is ..., line protocol is...	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
IPX address is ...	Network and node address of the local router interface, followed by the type of encapsulation configured on the interface and the status of the interface. See the **ipx network** command for a list of possible values.
[up]	Indicates whether IPX routing is enabled (up) or disabled (down) on the interface.
NOVELL-ETHER	Type of encapsulation being used on the interface, if any.
Delay of this IPX network, in ticks ...	Value of the ticks field (configured with the **ipx delay** command).
throughput	Throughput of the interface (configured with the **ipx spx-idle-time** interface configuration command).
link delay	Link delay of the interface (configured with the **ipx link-delay** interface configuration command).
IPXWAN processing...	Indicates whether IPXWAN processing has been enabled on this interface with the **ipx ipxwan** command.
IPX SAP update interval	Indicates the frequency of outgoing Service Advertising Protocol (SAP) updates (configured with the **ipx update interval** command).
IPX type 20 propagation packet forwarding...	Indicates whether forwarding of IPX type 20 propagation packets (used by NetBIOS) is enabled or disabled on this interface, as configured with the **ipx type-20-propagation** command.
Incoming access list	Indicates whether an incoming access list has been configured on this interface.
Outgoing access list	Indicates whether an access list has been enabled with the **ipx access-group** command.
IPX helper access list	Number of the broadcast helper list applied to the interface with the **ipx helper-list** command.
SAP GGS output filter list	Number of the Get General Server (GGS) response filter applied to the interface with the **ipx output-ggs-filter** command.

Table 14 show ipx interface Field Descriptions (continued)

Field	Description
SAP GNS processing ...	Indicates if GNS processing is enabled, what the response delay set is, and if there is any GNS output access-list configured
delay	Indicates the delay of this ipx network, represented in metric ticks for routers on this interface using the IPX RIP routing protocol.
output filter list	Number of the Get Nearest Server (GNS) response filter applied to the interface with the **ipx output-gns-filter** command.
SAP Input filter list	Number of the input SAP filter applied to the interface with the **ipx input-sap-filter** command.
SAP Output filter list	Number of the output SAP filter applied to the interface with the **ipx input-sap-filter** command.
SAP Router filter list	Number of the router SAP filter applied to the interface with the **ipx router-sap-filter** command.
Input filter list	Number of the input filter applied to the interface with the **ipx input-network-filter** command.
Output filter list	Number of the output filter applied to the interface with the **ipx output-network-filter** command.
Router filter list	Number of the router entry filter applied to the interface with the **ipx router-filter** command.
Netbios Input host access list	Name of the IPX NetBIOS input host filter applied to the interface with the **ipx netbios input-access-filter host** command.
Netbios Input bytes access list	Name of the IPX NetBIOS input bytes filter applied to the **ipx netbios input-access-filter** interface with the **ipx netbios input-access-filter bytes** command.
Netbios Output host access list	Name of the IPX NetBIOS output host filter applied to the interface with the **ipx netbios input-access-filter host** command.
Netbios Output bytes access list	Name of the IPX NetBIOS output bytes filter applied to the interface with the **input netbios input-access-filter bytes** command.
Updates each ...	How often Cisco IOS software sends Routing Information Protocol (RIP) updates, as configured with the **ipx update sap-after-rip** command.
SAP interpacket delay	Interpacket delay for SAP updates.
RIP interpacket delay	Interpacket delay for RIP updates.
RIP response delay	Delay for RIP responses.
Watchdog spoofing ...	Indicates whether watchdog spoofing is enabled or disabled for this interface, as configured with the **ipx watchdog spoof** command. This information is displayed only on serial interfaces.

Table 14 show ipx interface Field Descriptions (continued)

Field	Description
SPX spoofing ...	Indicates whether SPX spoofing is enabled or disabled for this interface.
IPX accounting	Indicates whether IPX accounting has been enabled with the **ipx accounting** command.
IPX fast switching IPX autonomous switching	Indicates whether IPX fast switching is enabled (default) or disabled for this interface, as configured with the **ipx route-cache** command. (If IPX autonomous switching is enabled, it is configured with the **ipx route-cache cbus** command.)
RIP packets received, RIP packets sent, Throttled	Number of RIP packets received, sent, or dropped.
RIP specific requests received, RIP specific replies sent,	Number of RIP specific requests received and the number of RIP specific replies sent.
RIP general requests received, ignored, RIP general replies sent	Number of RIP general requests received and ignored. Number of RIP general replies sent.
SAP GNS packets received, SAP GNS packets sent, Throttled	Number of SAP Get Nearest Server (GNS) packets received, sent, or dropped.
SAP GGS packets received, SAP GGS packets sent, Throttled	Number of SAP Get General Server (GGS) packets received, sent, or dropped.
SAP packets received, SAP packets sent, Throttled	Number of SAP packets received, sent, or dropped.

Related Commands

Command	Description
access-list (SAP filtering)	Defines an access list for filtering SAP requests.
access-list (IPX standard)	Defines a standard IPX access list.
ipx accounting	Enables IPX accounting.
ipx default-output-rip delay	Sets the default interpacket delay for RIP updates sent on all interfaces.
ipx default-output-sap-delay	Sets a default interpacket delay for SAP updates sent on all interfaces.
ipx delay	Sets the tick count.
ipx helper-list	Assigns an access list to an interface to control broadcast traffic (including type 20 propagation packets).
ipx input-network-filter	Controls which networks are added to the routing table of the Cisco IOS software.
ipx input-sap-filter	Controls which services are added to the routing table of the Cisco IOS software SAP table.
ipx ipxwan	Enables the IPXWAN protocol on a serial interface.
ipx netbios input-access-filter	Controls incoming IPX NetBIOS FindName messages.
ipx netbios output-access-filter	Controls outgoing IPX NetBIOS FindName messages.
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

Command	Description
ipx output-gns-filter	Controls which servers are included in the GNS responses sent by Cisco IOS software.
ipx output-network-filter	Controls which servers are included in the GNS responses sent by Cisco IOS software.
ipx output-rip-delay	Sets the interpacket delay for RIP updates sent on a single interface.
ipx output-sap-filter	Controls which services are included in SAP updates sent by Cisco IOS software.
ipx route-cache	Enables IPX fast switching.
ipx router-filter	Filters the routers from which packets are accepted.
ipx router-sap-filter	Filters SAP messages received from a particular router.
ipx routing	Enables IPX routing.
ipx update sap-after-rip	Configures the router to send a SAP update immediately following a RIP broadcast.
ipx watchdog	Enables watchdog processing.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.

show ipx servers

To list the IPX servers discovered through Service Advertising Protocol (SAP) advertisements, use the **show ipx servers** command in EXEC mode.

show ipx servers [**detailed**] [**network** *network-number*] [**type** *service-type-number*] [**unsorted** | [**sorted** [**name** | **network** | **type**]]] [**regexp** *name*]

Syntax Description

detailed	(Optional) Displays comprehensive information including path details.
network	(Optional) Displays IPX SAP services on a specified network.
network-number	(Optional) IPX network number. 1 to FFFFFFFF.
type	(Optional) Displays the IPX servers numerically by SAP service type. This is the default.
service-type-number	(Optional) IPX service type number. 1 to FFFF. When used with the **network** keyword, displays a list of all SAPs known to a particular network number.
unsorted	(Optional) Does not sort entries when displaying IPX servers.
sorted	(Optional) Sorts the display of IPX servers according to the keyword that follows.
name	(Optional) Displays the IPX servers alphabetically by server name.
network	(Optional) Displays the IPX servers numerically by network number.
regexp *name*	(Optional) Displays the IPX servers whose names match the regular expression.

Defaults

IPX servers are displayed numerically by SAP service type.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **unsorted** keyword was added.

Examples

The following example uses a regular expression to display SAP table entries corresponding to a particular group of servers in the accounting department of a company:

```
Router# show ipx servers regexp ACCT\_SERV.+

Codes: S - Static, P - Periodic, E - EIGRP, H - Holddown, + = detail
9 Total IPX Servers

Table ordering is based on routing and server info

 Type  Name            Net  Address        Port  Route  Hops Itf
S 108  ACCT_SERV_1     7001.0000.0000.0001:0001   1/01   2   Et0
```

```
S 108  ACCT_SERV_2     7001.0000.0000.0001:0001   1/01   2   Et0
S 108  ACCT_SERV_3     7001.0000.0000.0001:0001   1/01   2   Et0
```

For more information on regular expressions, refer to the “Regular Expressions” appendix in *Cisco IOS Dial Technologies Command Reference*.

Related Commands

Command	Description
ipx sap	Specifies static SAP entries.

show ipx spx-spoof

To display the table of Sequenced Packet Exchange (SPX) connections through interfaces for which SPX spoofing is enabled, use the **show ipx spx-spoof** command in EXEC mode.

show ipx spx-spoof

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample output from the **show ipx spx-spoof** command:

```
Router> show ipx spx-spoof

Local SPX Network.Host:sock Cid  Remote SPX Network.Host:sock Cid   Seq  Ack  Idle
CC0001.0000.0000.0001:8104  0D08 200.0260.8c8d.e7c6:4017      7204  09   0021 120
CC0001.0000.0000.0001:8104  0C08 200.0260.8c8d.c558:4016      7304  07   0025 120
```

Table 15 describes the fields shown in the display.

Table 15 show ipx spx-spoof Field Descriptions

Field	Description
Local SPX Network.Host:sock	Address of the local end of the SPX connection. The address is composed of the SPX network number, host, and socket.
Cid	Connection identification of the local end of the SPX connection.
Remote SPX Network.Host:sock	Address of the remote end of the SPX connection. The address is composed of the SPX network number, host, and socket.
Cid	Connection identification of the remote end of the SPX connection.
Seq	Sequence number of the last data packet transferred.
Ack	Number of the last solicited acknowledge received.
Idle	Amount of time elapsed since the last data packet was transferred.

Related Commands

Command	Description
ipx spx-idle-time	Sets the amount of time to wait before starting the spoofing of SPX keepalive packets following inactive data transfer.
ipx spx-spoof	Configures Cisco IOS software to respond to a client or server SPX keepalive packets on behalf of a remote system so that a DDR link will go idle when data has stopped being transferred.

show sse summary

To display a summary of Silicon Switch Processor (SSP) statistics, use the **show sse summary** command in EXEC mode.

show sse summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample output from the **show sse summary** command:

```
Router# show sse summary

SSE utilization statistics

               Program words  Rewrite bytes  Internal nodes  Depth
Overhead                 499              1               8
IP                         0              0               0      0
IPX                        0              0               0      0
SRB                        0              0               0      0
CLNP                       0              0               0      0
IP access lists            0              0               0
Total used               499              1               8
Total free             65037         262143
Total available        65536         262144

Free program memory
  [499..65535]
Free rewrite memory
  [1..262143]

Internals
  75032 internal nodes allocated, 75024 freed
  SSE manager process enabled, microcode enabled, 0 hangs
  Longest cache computation 4ms, longest quantum 160ms at 0x53AC8
```

spf-interval

To control how often Cisco IOS software performs the Shortest Path First (SPF) calculation, use the **spf-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

spf-interval *seconds*

no spf-interval *seconds*

Syntax Description

seconds	Minimum amount of time between SPF calculations, in seconds. It can be a number from 1 to 120. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval** command controls how often Cisco IOS software can perform the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often this is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but potentially slows down the rate of convergence.

Examples

The following example sets the SPF calculation interval to 30 seconds:

```
spf-interval 30
```

Related Commands

Command	Description
ipx router	Specifies the routing protocol to use.
log-neighbor-changes	Enables the logging of changes in Enhanced IGRP neighbor adjacencies.
prc-interval	Controls the hold-down period between partial route calculations.