Cisco IOS AppleTalk Command Reference

October 2008

Americas 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: 408 527-0883

C O N T E N T S

About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

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

Documentation Objectives

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

Audience

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

Documentation Conventions

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

This section includes the following topics:

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

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

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

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

Software Conventions

Cisco IOS uses the following program code conventions:

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

Reader Alert Conventions

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

⚠

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

✎

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

⏱

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

Documentation Organization

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

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

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

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

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

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

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

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

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

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

Cisco IOS Documentation on Cisco.com

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

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

New Features List

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

Feature Guides

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

Configuration Guides

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

Command References

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

Cisco IOS Supplementary Documents and Resources

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

Configuration Guides, Command References, and Supplementary Resources

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 2   Cisco IOS Supplementary Documents and Resources

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

Additional Resources and Documentation Feedback

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

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

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

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

Last updated: August 6, 2008

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

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

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

Initially Configuring a Device

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

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

Changing the Default Settings for a Console or AUX Port

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

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

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

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

Using the CLI

This section describes the following topics:

- Understanding Command Modes, page xx
- Using the Interactive Help Feature, page xxiii
- Understanding Command Syntax, page xxiv
- Understanding Enable and Enable Secret Passwords, page xxvi
- Using the Command History Feature, page xxvi
- Abbreviating Commands, page xxvii
- Using Aliases for CLI Commands, page xxvii
- Using the no and default Forms of Commands, page xxviii
- Using the debug Command, page xxviii
- Filtering Output Using Output Modifiers, page xxviii
- Understanding CLI Error Messages, page xxix

Understanding Command Modes

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

Table 3 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 3   CLI Command Modes

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

Table 3 CLI Command Modes (continued)

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

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

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

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

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

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

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

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 4 describes how to use the Help feature.

Table 4   CLI Interactive Help Commands

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

The following examples show how to use the help commands:

help

```
Router> help
```

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

Two styles of help are provided:

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

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

?

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

*partial command***?**

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

partial command<Tab>

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

command?

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

command keyword?

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

Understanding Command Syntax

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

Specific conventions convey information about syntax and command elements. Table 5 describes these conventions.

Table 5   CLI Syntax Conventions

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

The following examples show syntax conventions:

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

Cisco IOS AppleTalk Command Reference ■

Understanding Enable and Enable Secret Passwords

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

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

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

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

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

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

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

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

Using the Command History Feature

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

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

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

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

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

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

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

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

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

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

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

Abbreviating Commands

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

Using Aliases for CLI Commands

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

Table 6 shows the default command aliases.

Table 6   Default Command Aliases

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

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

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

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

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

Using the no and default Forms of Commands

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

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

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

Using the debug Command

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

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

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

Filtering Output Using Output Modifiers

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

Three output modifiers are available and are described as follows:

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

- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.

- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

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

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

```
Router# show interface | include protocol

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

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 7 shows the common CLI error messages.

Table 7   Common CLI Error Messages

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

For more system error messages, see the following documents:

- *Cisco IOS Release 12.2SR System Message Guide*
- *Cisco IOS System Messages, Volume 1 of 2* (Cisco IOS Release 12.4)
- *Cisco IOS System Messages, Volume 2 of 2* (Cisco IOS Release 12.4)

Saving Changes to a Configuration

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

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

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

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

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

Additional Information

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

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

  or

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

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

- Cisco Product Support Resources

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

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

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

- *White Paper: Cisco IOS Reference Guide*

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

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

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

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

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

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

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

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

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

Cisco IOS AppleTalk Commands

AppleTalk is a LAN system designed and developed by Apple Computer, Inc. It runs over Ethernet, Token Ring, and FDDI networks, in addition to LocalTalk, Apple's proprietary twisted-pair media access system. AppleTalk specifies a protocol stack comprising several protocols that direct the flow of traffic over the network.

Apple Computer uses the name *AppleTalk* to refer to the Apple networking architecture. Apple refers to the actual transmission media used in an AppleTalk network as LocalTalk (Apple's proprietary twisted-pair transmission medium for AppleTalk), TokenTalk (AppleTalk over Token Ring), EtherTalk (AppleTalk over Ethernet), and FDDITalk (AppleTalk over FDDI).

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

access-list additional-zones

To define the default action to take for access checks that apply to zones, use the **access-list additional-zones** command in global configuration mode. To remove an access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **additional-zones**

no access-list *access-list-number* **additional-zones**

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **access-list additional-zones** command defines the action to take for access checks not explicitly defined with the **access-list zone** command. If you do not specify this command, the default action is to deny other access.

You apply access lists defined with the **access-list additional-zones** command to outgoing routing updates and GetZoneList (GZL) filters (using the **appletalk distribute-list out**, and **appletalk getzonelist-filter** commands). You cannot apply them to data-packet filters (using the **appletalk access-group** command) or to incoming routing update filters (using the **appletalk distribute-list in** command).

Examples

The following example creates an access list based on AppleTalk zones:

```
access-list 610 deny zone Twilight
access-list 610 permit additional-zones
```

Related Commands	Command	Description
	access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
	access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
	access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
	access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
	access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
	access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
	access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
	access-list zone	Defines an AppleTalk access list that applies to a zone.
	appletalk access-group	Assigns an access list to an interface.
	appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
	appletalk distribute-list out	Filters routing updates sent to other routers.
	appletalk getzonelist-filter	Filters GZL replies.
	appletalk permit-partial-zones	Permits access to the other networks in a zone when access to one of those networks is denied.

access-list cable-range

To define an AppleTalk access list for a cable range (for extended networks only), use the **access-list cable-range** command in global configuration mode. To remove an access list, use the **no** form of this command.

> **access-list** *access-list-number* {**deny** | **permit**} **cable-range** *cable-range*
>   [**broadcast-deny** | **broadcast-permit**]

> **no access-list** *access-list-number* [{**deny** | **permit**} **cable-range** *cable-range*
>   [**broadcast-deny** | **broadcast-permit**]]

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
cable-range	Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number.
broadcast-deny	(Optional) Denies access to broadcast packets if the conditions are matched.
broadcast-permit	(Optional) Permits access to broadcast packets if the conditions are met.

Defaults   No access lists are predefined.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   When used as a routing update filter, the **access-list cable-range** command affects matching on extended networks only. The conditions defined by this access list are used only when a cable range in a routing update exactly matches that specified in the **access-list cable-range** command. The conditions are never used to match a network number (for a nonextended network).

When used as a data-packet filter, the **access-list cable-range** command affects matching on any type of network number. The conditions defined by this access list are used only when the packet's source network lies in the range defined by the access list.

You apply access lists defined with the **access-list cable-range** command to data-packet and routing-update filters (using the **appletalk access-group**, **appletalk distribute-list in**, and **appletalk distribute-list out** commands). You cannot apply them to GZL filters (using the **appletalk getzonelist-filter** command).

To delete an 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**} **cable-range** *cable-range*

Priority queuing for AppleTalk operates on the destination network number, not the source network number.

Examples

The following access list forwards all packets except those from cable range 10 to 20:

```
access-list 600 deny cable-range 10-20
access-list 600 permit other-access
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk access-group	Assigns an access list to an interface.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk getzonelist-filter	Filters GZL replies.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list includes

To define an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks), use the **access-list includes** command in global configuration mode. To remove an access list, use the **no** form of this command.

> **access-list** *access-list-number* {**deny** | **permit**} **includes** *cable-range*
>   [**broadcast-deny** | **broadcast-permit**]

> **no access-list** *access-list-number* {**deny** | **permit**} **includes** *cable-range*
>   [**broadcast-deny** | **broadcast-permit**]]

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
cable-range	Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number. To specify a network number, set the starting and ending network numbers to the same value.
broadcast-deny	(Optional) Denies access to broadcast packets if the conditions are matched.
broadcast-permit	(Optional) Permits access to broadcast packets if the conditions are met.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When used as a routing update filter, the **access-list includes** command affects matching on extended and nonextended AppleTalk networks. The conditions defined by this access list are used when a cable range or network number overlaps, either partially or completely, one (or more) of those specified in the **access-list includes** command.

When used as a data-packet filter, the conditions defined by this access list are used when the packet's source network lies in the range defined in the **access-list includes** command.

You apply access lists defined with the **access-list includes** command to data-packet and routing-update filters (using the **appletalk access-group, appletalk distribute-list in**, and **appletalk distribute-list out** commands). You cannot apply them to GZL filters (using the **appletalk getzonelist-filter** command).

To delete an 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**} **includes** *cable-range*

Priority queuing for AppleTalk operates on the destination network number, not the source network number.

Examples

The following example defines an access list that permits access to any network or cable range that overlaps any part of the range 10 to 20. This means, for example, that cable ranges 13 to 16 and 17 to 25 will be permitted. This access list also permits all other ranges.

```
access-list 600 permit includes 10-20
access-list 600 permit other-access
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk access-group	Assigns an access list to an interface.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk getzonelist-filter	Filters GZL replies.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list nbp

To define an AppleTalk access list entry for a particular Name Binding Protocol (NBP) named entity, class of NBP named entities, NBP packet type, or NBP named entities that belong to a specific zone, use the **access-list nbp** command in global configuration mode. To remove an NBP access list entry from the access list, use the **no** form of this command.

> **access-list** *access-list-number* {**deny** | **permit**} **nbp** *sequence-number* {**BrRq** | **FwdRq** | **Lookup** | **LkReply** | **object** *string* | **type** *string* | **zone** *string*}

> **no access-list** *access-list-number* {**deny** | **permit**} **nbp** *sequence-number* {**BrRq** | **FwdRq** | **Lookup** | **LkReply** | **object** *string* | **type** *string* | **zone** *string*}

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if conditions are matched.
permit	Permits access if conditions are matched.
sequence-number	Number used to tie together two or three portions of an NBP name tuple and to keep track of the number of **access-list nbp** entries in an access list. Each command entry must have a sequence number.
BrRq	Broadcast Request packet type.
FwdRq	Forward Request packet type.
Lookup	Lookup packet type.
LkReply	Lookup Reply packet type.
object	Characterizes *string* as the portion of an NBP name that identifies a particular **object** or named entity.
string	Portion of an NBP name identifying the **object**, **type**, or **zone** of a named entity. The name string can be up to 32 characters long, and it can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For an NBP name with a leading space, enter the first character as the special sequence :20.
type	Characterizes *string* as the portion of an NBP name that identifies a category or **type** of named entity.
zone	Characterizes *string* as the portion of an NBP name that identifies an AppleTalk **zone**.

Defaults

No particular access list entry for an NBP named entity is defined, and the default filtering specified by the **access-list other-nbps** command takes effect.

Command Modes

Global configuration

Command History	Release	Modification
	11.0	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **access-list nbp** command defines the action to take for filtering NBP packets from a particular **object** (particular named entity), **type** (class of named entities), or **zone** (AppleTalk zone in which named entities reside), or for a particular NBP packet type, superseding the default action for NBP packets from all named entities specified by the **access-list other-nbps** command. For each command that you enter, you must specify a sequence number.

The sequence number serves two purposes:

- Its principal purpose is to allow you to associate two or three portions of an NBP three-part name, referred to as an NBP tuple. To do this, you enter two or three commands having the same sequence number but each specifying a different keyword and NBP name portion: **object**, **type**, or **zone**. The same sequence number binds them together. This provides you with the ability to restrict forwarding of NBP packets at any level, down to a single named entity.

- Its second purpose is to allow you to keep track of the number of **access-list nbp** entries you have made. You must enter a sequence number even if you do not use it to associate portions of an NBP name.

Examples

The following example adds entries to access list number 607 to allow forwarding of NBP packets from specific sources and deny forwarding of NBP packets from all other sources. The first command adds an entry that allows NBP packets from all printers of type LaserWriter. The second command adds an entry that allows NBP packets from all AppleTalk file servers of type AFPServer. The third command adds an entry that allows NBP packets from all applications called HotShotPaint. For example, there might be an application with a **zone** name of Accounting and an application with a **zone** name of engineering, both having the object name of HotShotPaint. NBP packets forwarded from both applications will be allowed.

The **access-list other-nbps** command denies forwarding of NBP packets from all other sources.

```
access-list 607 permit nbp 1 type LaserWriter
access-list 607 permit nbp 2 type AFPServer
access-list 607 permit nbp 3 object HotShotPaint
access-list 607 deny other-nbps
access-list 607 permit other-access
```

The following example adds entries to access list number 608 to deny forwarding of NBP packets from two specific servers whose fully qualified NBP names are specified. It permits forwarding of NBP packets from all other sources.

```
access-list 608 deny nbp 1 object ServerA
access-list 608 deny nbp 1 type AFPServer
access-list 608 deny nbp 1 zone Bld3
access-list 608 deny nbp 2 object ServerB
access-list 608 deny nbp 2 type AFPServer
access-list 608 deny nbp 2 zone Bld3
access-list 608 permit other-nbps
access-list 608 permit other-access
```

The following example denies forwarding of NBP Lookup Reply packets for all named entities. It permits forwarding of other NBP packet types from all other sources.

```
access-list 600 deny nbp 1 LkReply
access-list 600 permit other-nbps
access-list 600 permit other-access
```

The following example creates an access list that denies forwarding of these packets:

- All NBP Lookup Reply packets
- NBP packets from the server named Bob's Server
- Packets from all AppleTalk file servers of type AFPServer
- All NBP Lookup Reply packets that contain the specified named entities belonging to the zone *twilight*

```
access-list 600 deny nbp 1 LkReply
access-list 600 deny nbp 1 object Bob's Server
access-list 600 deny nbp 1 type AFPServer
access-list 600 deny nbp 1 zone twilight
access-list 600 permit other-nbps
access-list 600 permit other-access
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk access-group	Assigns an access list to an interface.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk getzonelist-filter	Filters GZL replies.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list network

To define an AppleTalk access list for a single network number (that is, for a nonextended network), use the **access-list network** command in global configuration mode. To remove an access list, use the **no** form of this command.

> **access-list** *access-list-number* {**deny** | **permit**} **network** *network*
> [**broadcast-deny** | **broadcast-permit**]

> **no access-list** *access-list-number* {**deny** | **permit**} **network** *network*
> [**broadcast-deny** | **broadcast-permit**]]

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
network	AppleTalk network number.
broadcast-deny	(Optional) Denies access to broadcast packets if the conditions are matched.
broadcast-permit	(Optional) Permits access to broadcast packets if the conditions are met.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When used as a routing-update filter, the **access-list network** command affects matching on nonextended networks only. The conditions defined by this access list are used only when the nonextended number in a routing update matches a network number specified in one of the **access-list network** commands. The conditions are never used to match a cable range (for an extended network) even if the cable range has the same starting and ending number.

When used as a data-packet filter, the conditions defined by this access list are used only when the packet's source network matches the network number specified in the **access-list network** command.

You apply access lists defined with the **access-list network** command to data-packet and routing-update filters (using the **appletalk access-group, appletalk distribute-list in**, and **appletalk distribute-list out** commands). You cannot apply access lists to GZL filters (using the **appletalk getzonelist-filter** command).

In software releases before 9.0, the syntax of this command was **access-list** *access-list-number* {**deny** | **permit**} *network*. The current version of the software is still able to interpret commands in this format if it finds them in a configuration or boot file. However, it is recommended that you update the commands in your configuration or boot files to match the current syntax.

Use the **no access-list** command with the *access-list-number* argument only to remove an entire access list from the configuration. Specify the optional arguments to remove a particular clause.

To delete an 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** *network*

Priority queuing for AppleTalk operates on the destination network number, not the source network number.

Examples

The following example defines an access list that forwards all packets except those destined for networks 1 and 2:

```
access-list 650 deny network 1
access-list 650 deny network 2
access-list 650 permit other-access
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk access-group	Assigns an access list to an interface.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.

Command	Description
appletalk getzonelist-filter	Filters GZL replies.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list other-access

To define the default action to take for subsequent access checks that apply to networks or cable ranges, use the **access-list other-access** command in global configuration mode. To remove an access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **other-access**

no access-list *access-list-number* **other-access**

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **access-list other-access** command defines the action to take for access checks not explicitly defined with an **access-list network, access-list cable-range, access-list includes,** or **access-list within** command. If you do not specify this command, the default action is to deny other access.

You apply access lists defined with the **access-list other-access** command to data-packet and routing-update filters (using the **appletalk access-group, appletalk distribute-list in**, and **appletalk distribute-list out** commands). You cannot apply them to GZL filters (using the **appletalk getzonelist-filter** command).

In software releases before 9.0, the syntax of this command was **access-list** *access-list-number* {**deny** | **permit**} **-1**. The current version of the software is still able to interpret commands in this format if it finds them in a configuration or boot file. However, it is recommended that you update the commands in your configuration or boot files to match the current syntax.

Priority queuing for AppleTalk operates on the destination network number, not the source network number.

Examples   The following example defines an access list that forwards all packets except those destined for networks 1 and 2:

```
access-list 650 deny network 1
access-list 650 deny network 2
access-list 650 permit other-access
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk access-group	Assigns an access list to an interface.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list other-nbps

To define the default action to take for access checks that apply to Name Binding Protocol (NBP) packets from named entities not otherwise explicitly denied or permitted, use the **access-list other-nbps** command in global configuration mode. To remove an access list, use the **no** form of this command.

> **access-list** *access-list-number* {**deny** | **permit**} **other-nbps**

> **no access-list** *access-list-number* {**deny** | **permit**} **other-nbps**

Syntax Description

access-list-number	Number of the access list for AppleTalk. This is a decimal number from 600 to 699.
deny	Denies access if conditions are matched.
permit	Permits access if conditions are matched.

Defaults

Access is denied.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **access-list other-nbps** command defines the action to take for filtering of NBP packets from named entities not explicitly defined by an **access-list nbp** command. It allows you to implement the default AppleTalk network security state at the named entity level. Any **access-list nbp** commands you enter affect a particular named entity object, class of named entities, or all named entities within a zone. This command sets the security state for all other NBP named entities. If you do not specify this command, the default action is to deny access.

You can use this command to create an entry in an access list before or after you issue **access-list nbp** commands. The order of the command in the access list is irrelevant.

Examples

The following example permits forwarding of all NBP packets from all sources except AppleTalk file servers of type AFPServer:

```
access-list 607 deny nbp 2 type AFPServer
access-list 607 permit other-nbps
```

Related Commands	Command	Description
	access-list additional-zones	Defines the default action to take for access checks that apply to zones.
	access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
	access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
	access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
	access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
	access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
	access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
	access-list zone	Defines an AppleTalk access list that applies to a zone.
	appletalk access-group	Assigns an access list to an interface.
	appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
	appletalk distribute-list out	Filters routing updates sent to other routers.
	appletalk getzonelist-filter	Filters GZL replies.
	priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list within

To define an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range, use the **access-list within** command in global configuration mode. To remove this access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **within** *cable-range*

no access-list *access-list-number* [{**deny** | **permit**} **within** *cable-range*]

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
cable-range	Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number. To specify a network number, set the starting and ending network numbers to the same value.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When used as a routing update filter, the **access-list within** command affects matching on extended and nonextended AppleTalk networks. The conditions defined by this access list are used when a cable range or network number overlaps, either partially or completely, one (or more) of those specified in the **access-list within** command.

When used as a data-packet filter, the conditions defined by this access list are used when the packet's source network lies in the range defined in the **access-list within** command.

You apply access lists defined with the **access-list within** command to data-packet and routing-update (using the **appletalk access-group, appletalk distribute-list in**, and **appletalk distribute-list out**). You cannot apply them to GZL filters (using the **appletalk getzonelist-filter** command).

To delete an 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**} **within** *cable-range*

Priority queuing for AppleTalk operates on the destination network number, not the source network number.

Examples

The following example defines an access list that permits access to any network or cable range that is completely included in the range 10 to 20. This means, for example, that cable range 13 to 16 will be permitted, but cable range 17 to 25 will not be. The second line of the access list permits all other packets.

```
access-list 600 permit within 10-20
access-list 600 permit other-access
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk access-group	Assigns an access list to an interface.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk getzonelist-filter	Filters GZL replies.
priority-list protocol	Establishes queueing priorities based on the protocol type.

access-list zone

To define an AppleTalk access list that applies to a zone, use the **access-list zone** command in global configuration mode. To remove an access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **zone** *zone-name*

no access-list *access-list-number* [{**deny** | **permit**} **zone** *zone-name*]

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
zone-name	Name of the zone. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

Defaults

No access lists are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You apply access lists defined with the **access-list zone** command to outgoing routing update and GZL filters (using the **appletalk distribute-list out** and **appletalk getzonelist-filter** commands). You cannot apply them to data-packet filters (using the **appletalk access-group** command) or to incoming routing update filters (using the **appletalk distribute-list in** command).

To delete an 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**} **zone** *zone-name*

Use the **access-list additional-zones** command to define the action to take for access checks not explicitly defined with the **access-list zone** command.

Note AppleTalk zone access lists on an Enhanced Internet Gateway Routing Protocol (Enhance IGRP) interface will not filter the distribution of Enhanced IGRP routes. When the **appletalk distribute-list out** command is applied to an Enhanced IGRP interface, any **access-list zone** commands in the specified access list will be ignored.

Examples The following example creates an access list based on AppleTalk zones:

```
access-list 610 deny zone Twilight
access-list 610 permit additional-zones
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
appletalk access-group	Assigns an access list to an interface.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk getzonelist-filter	Filters GZL replies.
appletalk permit-partial-zones	Permits access to the other networks in a zone when access to one of those networks is denied.

appletalk access-group

To assign an access list to an interface, use the **appletalk access-group** command in interface configuration mode. To remove the access list, use the **no** form of this command.

appletalk access-group *access-list-number* [**in** | **out**]

no appletalk access-group *access-list-number*

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
in	(Optional) Filters on incoming packets.
out	(Optional) Filters on outgoing packets. This is the default direction.

Defaults

No access lists are predefined. The default interface direction is out.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **appletalk access-group** command applies data-packet filters or NBP-packet filters to an inbound or outbound interface. These filters check data packets being received or sent on an interface. If the source network of the packets has access denied, these packets are not processed and are discarded.

When you apply a data-packet filter to an interface, you should ensure that all networks or cable ranges within a zone are governed by the same filters.

Examples

The following example applies access list 601 to outbound Ethernet interface 0:

```
access-list 601 deny cable-range 1-10
access-list 601 permit other-access
interface ethernet 0
 appletalk access-group 601
```

The following example applies access list 600 to inbound Ethernet interface 0:

```
interface ethernet 0
 appletalk access-group 600 in
```

	Command	Description
Related Commands	**access-list cable-range**	Defines an AppleTalk access list for a cable range (for extended networks only).
	access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
	access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
	access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
	access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
	appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
	appletalk distribute-list out	Filters routing updates sent to other routers.

appletalk address

To enable nonextended AppleTalk routing on an interface, use the **appletalk address** command in interface configuration mode. To disable nonextended AppleTalk routing, use the **no** form of this command.

appletalk address *network.node*

no appletalk address [*network.node*]

Syntax Description	*network.node*	AppleTalk network address assigned to the interface. The argument *network* is the 16-bit network number in the range 0 to 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal and separated by a period.

Defaults   Disabled

Command Modes   Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   You must enable routing on the interface before assigning zone names.

Specifying an address of 0.0, or 0.*node*, places the interface into *discovery mode*. When in this mode, the Cisco IOS software attempts to determine network address information from another router on the network. You also can enable discovery mode with the **appletalk discovery** command. Discovery mode does not run over serial lines.

Examples   The following example enables nonextended AppleTalk routing on Ethernet interface 0:

```
appletalk routing
interface ethernet 0
 appletalk address 1.129
```

Related Commands	Command	Description
	access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
	appletalk discovery	Places an interface into discovery mode.
	appletalk zone	Sets the zone name for the connected AppleTalk network.

appletalk alternate-addressing

To display network numbers in a two-octet format, use the **appletalk alternate-addressing** command in global configuration mode. To return to displaying network numbers in the format *network.node*, use the **no** form of this command.

appletalk alternate-addressing

no appletalk alternate-addressing

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **appletalk alternate-addressing** command displays cable ranges in the alternate format wherever applicable. This format consists of printing the upper and lower bytes of a network number as 8-bit decimal values separated by a decimal point. For example, the cable range 511-512 would be printed as 1.255-2.0.

Examples   The following example enables the display of network numbers in a two-octet format:

```
appletalk alternate-addressing
```

appletalk arp interval

To specify the time interval between retransmissions of Address Resolution Protocol (ARP) packets, use the **appletalk arp interval** command in global configuration mode. To restore both default intervals, use the **no** form of this command.

appletalk arp [**probe** | **request**] **interval** *interval*

no appletalk arp [**probe** | **request**] **interval** *interval*

Syntax Description		
probe		(Optional) Interval to be used with AppleTalk Address Resolution Protocol (AARP) requests that are trying to determine the address of the local router when the Cisco IOS software is being configured. If you omit **probe** and **request**, **probe** is the default.
request		(Optional) Indicates that the interval specified is to be used when AARP is attempting to determine the hardware address of another node so that AARP can deliver a packet.
interval		Interval, in milliseconds, between AARP transmissions. The minimum value is 33 milliseconds. When used with the **probe** keyword, the default interval is 200 milliseconds. When used with the **request** keyword, the default interval is 1000 milliseconds.

Defaults

If you omit the keywords, probe is the default.

probe—200 milliseconds
request—1000 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The time interval you specify takes effect immediately.

Lengthening the interval between AARP transmissions permits responses from devices that respond slowly (such as printers and overloaded file servers) to be received.

AARP uses the **appletalk arp probe interval** value when obtaining the address of the local router. This is done when the Cisco IOS software is being configured. You should not change the default value of this interval unless absolutely necessary, because this value directly modifies the AppleTalk dynamic node assignment algorithm.

AARP uses the **appletalk arp request interval** value when attempting to determine the hardware address of another node so that it can deliver a packet. You can change this interval as desired, although the default value is optimal for most sites.

The **no appletalk arp interval** command restores both the **probe** and **request** intervals specified in the **appletalk arp interval** and **appletalk arp retransmit-count** commands to their default values.

Examples

The following example lengthens the AppleTalk ARP retry interval to 2000 milliseconds:

```
appletalk arp request interval 2000
```

Related Commands

Command	Description
appletalk arp retransmit-count	Specifies the number of ARP probe or request transmissions.
appletalk arp-timeout	Specifies the interval at which entries are aged out of the ARP table.
appletalk glean-packets	Derives ARP table entries from incoming packets.
show appletalk globals	Displays information and settings about the AppleTalk internetwork and other parameters.

appletalk arp retransmit-count

To specify the number of AppleTalk Address Resolution Protocol (AARP) probe or request transmissions, use the **appletalk arp retransmit-count** command in global configuration mode. To restore both default values, use the **no** form of this command.

appletalk arp [**probe** | **request**] **retransmit-count** *number*

no appletalk arp [**probe** | **request**] **retransmit-count** *number*

Syntax Description		
probe		(Optional) Indicates that the number specified is to be used with AARP requests that are trying to determined the address of the local router when the Cisco IOS software is being configured. If you omit **probe** and **request**, **probe** is the default.
request		(Optional) Indicates that the number specified is to be used when AARP is attempting to determine the hardware address of another node so that AARP can deliver a packet.
number		Number of AARP retransmissions that will occur. The minimum number is 1. When used with the **probe** keyword, the default value is 10 retransmissions. When used with the **request** keyword, the default value is 5 retransmissions. Specifying 0 selects the default value.

Defaults

If you omit the keyword, probe is the default.

probe—10 transmissions
request—5 transmissions

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The value you specify takes effect immediately.

Increasing the number of retransmissions permits responses from devices that respond slowly (such as printers and overloaded file servers) to be received.

AARP uses the **appletalk arp probe retransmit-count** value when obtaining the address of the local router. This is done when the Cisco IOS software is being configured. You should not change the default value unless absolutely necessary, because this value directly modifies the AppleTalk dynamic node assignment algorithm.

AARP uses the **appletalk arp request retransmit-count** value when attempting to determine the hardware address of another node so that it can deliver a packet. You can change this interval as desired, although the default value is optimal for most sites.

The **no appletalk arp interval** command restores both the **probe** and **request** intervals specified in the **appletalk arp interval** and **appletalk arp retransmit-count** commands to their default values.

Examples

The following example specifies an AARP retransmission count of 10 for AARP packets that are requesting the hardware address of another node on the network:

```
appletalk arp request retransmit-count 10
```

Related Commands

Command	Description
appletalk arp interval	Specifies the time interval between retransmissions of ARP packets.
appletalk arp-timeout	Specifies the interval at which entries are aged out of the ARP table.
appletalk glean-packets	Derives ARP table entries from incoming packets.
show appletalk globals	Displays information and settings about the AppleTalk internetwork and other parameters.

appletalk arp-timeout

To specify the interval at which entries are aged out of the Address Resolution Protocol (ARP) table, use the **appletalk arp-timeout** command in interface configuration mode. To return to the default timeout, use the **no** form of this command.

    appletalk arp-timeout *interval*

    no appletalk arp-timeout *interval*

Syntax Description

interval	Time, in minutes, after which an entry is removed from the AppleTalk ARP table. The default is 240 minutes (4 hours).

Defaults

240 minutes (4 hours)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example changes the ARP timeout interval on Ethernet interface 0 to 2 hours:

```
interface ethernet 0
appletalk cable-range 2-2
 appletalk arp-timeout 120
```

Related Commands

Command	Description
appletalk arp interval	Specifies the time interval between retransmissions of ARP packets.
appletalk arp retransmit-count	Specifies the number of ARP probe or request transmissions.
appletalk glean-packets	Derives ARP table entries from incoming packets.

appletalk aurp tickle-time

To set the Apple Update-Based Routing Protocol (AURP) last-heard-from timer value, use the **appletalk aurp tickle-time** command in interface configuration mode. To return to the default last-heard-from timer value, use the **no** form of this command.

appletalk aurp tickle-time *seconds*

no appletalk aurp tickle-time *seconds*

Syntax Description	*seconds*	Timeout value, in seconds. This value can be a number from 30 to infinity. The default is 90 seconds.

Defaults 90 seconds

Command Modes Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines If the tunnel peer has not been heard from within the time specified by the least-heard-from timer value, the Cisco IOS software sends tickle packets to check that the tunnel peer is still up.

You can use this command only on tunnel interfaces.

Examples The following example changes the AURP last-heard-from timer value on tunnel interface 0 to 120 seconds:

```
interface tunnel 0
 appletalk aurp tickle-time 120
```

Related Commands

Command	Description
show appletalk interface	Displays the status of the AppleTalk interfaces configured in the Cisco IOS software and the parameters configured on each interface.

appletalk aurp update-interval

To set the minimum interval between Apple Update-Based Routing Protocol (AURP) routing updates, use the **appletalk aurp update-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

appletalk aurp update-interval *seconds*

no appletalk aurp update-interval *seconds*

Syntax Description

seconds	AURP routing update interval, in seconds. This interval must be a multiple of 10. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The AURP routing update interval applies only to tunnel interfaces.

Examples

The following example changes the AURP routing update interval on tunnel interface 0 to 40 seconds:

```
interface tunnel 0
 appletalk aurp update-interval 40
```

Related Commands

Command	Description
show appletalk globals	Displays information and settings about the AppleTalk internetwork and other parameters.

appletalk cable-range

To enable an extended AppleTalk network, use the **appletalk cable-range** command in interface configuration mode. To disable an extended AppleTalk network, use the **no** form of this command.

appletalk cable-range *cable-range* [*network***.***node*]

no appletalk cable-range *cable-range* [*network***.***node*]

Syntax Description

cable-range	Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 0 to 65279. The starting network number must be less than or equal to the ending network number.
*network***.***node*	(Optional) Suggested AppleTalk address for the interface. The argument *network* is the 16-bit network number, and the argument *node* is the 8-bit node number. Both numbers are decimal and separated by a period. The suggested network number must fall within the specified range of network numbers.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must enable routing on the interface before assigning zone names.

Specifying a cable range value of 0-0 places the interface into *discovery mode*. When in this mode, the Cisco IOS software attempts to determine cable range information from another router on the network. You can also enable discovery mode with the **appletalk discovery** command. Discovery mode does not run over serial lines.

Examples

The following example assigns a cable range of 3 to 3 to the interface:

```
interface ethernet 0
 appletalk cable-range 3-3
```

Related Commands	Command	Description
	appletalk address	Enables nonextended AppleTalk routing on an interface.
	appletalk discovery	Places an interface into discovery mode.
	appletalk zone	Sets the zone name for the connected AppleTalk network.

appletalk checksum

To enable the generation and verification of checksums for all AppleTalk packets (except routed packets), use the **appletalk checksum** command in global configuration mode. To disable checksum generation and verification, use the **no** form of this command.

appletalk checksum

no appletalk checksum

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   When the **appletalk checksum** command is enabled, the Cisco IOS software discards incoming Datagram Delivery Protocol (DDP) packets when the checksum is not zero and is incorrect, and when the router is the final destination for the packet.

You might want to disable checksum generation and verification if you have very early devices (such as LaserWriter printers) that cannot receive packets that contain checksums.

The Cisco IOS software does not check checksums on routed packets, thereby eliminating the need to disable checksum to allow operation of some networking applications.

Examples   The following example disables the generation and verification of checksums:

```
no appletalk checksum
```

Related Commands

Command	Description
show appletalk globals	Displays information and settings about the AppleTalk internetwork and other parameters.

appletalk client-mode

To allow users to access an AppleTalk zone when dialing into an asynchronous line (on Cisco routers, only via the auxiliary port) use the **appletalk client-mode** command in interface configuration mode. To disable this function, use the **no** form of this command.

> **appletalk client-mode**

> **no appletalk client-mode**

Syntax Description   This command has no arguments or keywords.

Defaults   Client mode is disabled.

Command Modes   Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **appletalk client-mode** command allows a remote client to use an asynchronous interface to access AppleTalk zones, use networked peripherals, and share files with other Macintosh users.

This command works only on asynchronous interfaces on which Point-to-Point Protocol (PPP) encapsulation is enabled. Also, you must first create an internal network for the Macintosh client using the **appletalk virtual-net** global configuration command.

An interface configured with the **appletalk client-mode** interface configuration and **appletalk virtual-net** global configuration commands does not support routing.

Examples   The following example allows a user to access AppleTalk functionality on an asynchronous line using PPP:

```
interface asynchronous 1
 appletalk client-mode
```

Related Commands	Command	Description
	appletalk virtual-net	Adds AppleTalk users logging in on an asynchronous line and using PPP encapsulation to an internal network.
	encapsulation	Sets the encapsulation method used by the interface.
	interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
	ppp	Starts an asynchronous connection using PPP.

appletalk discovery

To place an interface into discovery mode, use the **appletalk discovery** command in interface configuration mode. To disable discovery mode, use the **no** form of this command.

> **appletalk discovery**

> **no appletalk discovery**

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   If an interface is connected to a network that has at least one other operational AppleTalk router, you can dynamically configure the interface using *discovery mode*. In discovery mode, an interface acquires network address information about the attached network from an operational router and then uses this information to configure itself.

If you enable discovery mode on an interface, when the Cisco router starts up, that interface must acquire information to configure itself from another operational router on the attached network. If no operational router is present on the connected network, the interface will not start.

If you do not enable discovery mode, the interface must acquire its configuration from memory when the router starts. If the stored configuration is not complete, the interface will not start. If there is another operational router on the connected network, the router will verify the interface's stored configuration with that router. If there is any discrepancy, the interface will not start. If there are no neighboring operational routers, the router will assume the interface's stored configuration is correct and will start.

Once an interface is operational, it can seed the configurations of other routers on the connected network regardless of whether you have enabled discovery mode on any of the routers.

If you enable **appletalk discovery** and the interface is restarted, another operational router must still be present on the directly connected network in order for the interface to start.

It is not advisable to have all routers on a network configured with discovery mode enabled. If all routers were to restart simultaneously (for instance, after a power failure), the network would become inaccessible until at least one router were restarted with discovery mode disabled.

You can also enable discovery mode by specifying an address of 0.0. in the **appletalk address** command or a cable range of 0-0 in the **appletalk cable-range** command.

Discovery mode is useful when you are changing a network configuration, or when you are adding a router to an existing network.

Discovery mode does not run over serial lines.

Use the **no appletalk discovery** command to disable discovery mode. If the interface is not operational when you issue this command (that is, if you have not issued an **access-list zone** command on the interface), you must configure the zone name next. If the interface is operational when you issue the **no appletalk discovery** command, you can save the current configuration (in running memory) in nonvolatile memory by issuing the **copy running-config startup-config** command. (The **copy running-config startup-config** command replaces the **write memory** command. Refer to the description of the **copy running-config startup-config** command for more information.)

Examples

The following example enables discovery mode on Ethernet interface 0:

```
interface ethernet 0
 appletalk discovery
```

Related Commands

Command	Description
appletalk address	Enables nonextended AppleTalk routing on an interface.
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
show appletalk interface	Displays the status of the AppleTalk interfaces configured in the Cisco IOS software and the parameters configured on each interface.

appletalk distribute-list in

To filter routing updates received from other routers over a specified interface, use the **appletalk distribute-list in** command in interface configuration mode. To remove the routing table update filter, use the **no** form of this command.

appletalk distribute-list *access-list-number* **in**

no appletalk distribute-list [*access-list-number*] **in**

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.

Defaults

No routing filters are preconfigured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **appletalk distribute-list in** command controls which networks and cable ranges in routing updates will be entered into the local routing table.

Filters for incoming routing updates use access lists that define conditions for networks and cable ranges only. They cannot use access lists that define conditions for zones. All zone information in an access list assigned to the interface with the **appletalk distribute-list in** command is ignored.

An input distribution list filters network numbers received in an incoming routing update. When AppleTalk routing updates are received on the specified interface, each network number and cable range in the update is checked against the access list. Only network numbers and cable ranges that are permitted by the access list are inserted into the Cisco IOS software AppleTalk routing table.

Examples

The following example prevents the router from accepting routing table updates received from network 10 and on Ethernet interface 3:

```
access-list 601 deny network 10
access-list 601 permit other-access
interface ethernet 3
 appletalk distribute-list 601 in
```

Related Commands	Command	Description
	access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
	access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
	access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
	access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
	access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
	appletalk distribute-list out	Filters routing updates sent to other routers.

appletalk distribute-list out

To filter routing updates transmitted to other routers, use the **appletalk distribute-list out** command in interface configuration mode. To remove the routing table update filter, use the **no** form of this command.

appletalk distribute-list *access-list-number* **out**

no appletalk distribute-list [*access-list-number*] **out**

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.

Defaults

No routing filters are preconfigured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **appletalk distribute-list out** command controls which network numbers and cable ranges are included in routing updates and which zones the local router includes in its GetZoneList (GZL) replies.

When an AppleTalk routing update is generated on the specified interface, each network number and cable range in the routing table is checked against the access list. If an undefined access list is used, all network numbers and cable ranges are added to the routing update. Otherwise, if an access list is defined, only network numbers and cable ranges that satisfy the following conditions are added to the routing update:

• The network number or cable range is not explicitly or implicitly denied.

• The network number or cable range is not a member of a zone that is explicitly or implicitly denied.

• If **appletalk permit-partial-zones** is disabled (the default), the network number or cable range is not a member of a zone that is partially obscured.

A zone is considered partially obscured when one or more network numbers or cable ranges that are members of the zone is explicitly or implicitly denied.

When a Zone Information Protocol (ZIP) GZL reply is generated, only zones that satisfy the following conditions are included:

• If **appletalk permit-partial-zones** is enabled, at least one network number or cable range that is a member of the zone is explicitly or implicitly permitted.

- If **appletalk permit-partial-zones** is disabled, all network numbers or cable ranges are explicitly or implicitly permitted.

- The zone is explicitly or implicitly permitted.

Note AppleTalk zone access lists on an Enhanced IGRP interface will not filter the distribution of Enhanced IGRP routes. When the **appletalk distribute-list out** command is applied to an Enhanced IGRP interface, any **access-list zone** commands in the specified access list will be ignored.

Examples
The following example prevents routing updates sent on Ethernet 0 from mentioning any networks in zone Admin:

```
access-list 601 deny zone Admin
access-list 601 permit other-access
interface Ethernet 0
 appletalk distribute-list 601 out
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk getzonelist-filter	Filters GZL replies.
appletalk permit-partial-zones	Permits access to the other networks in a zone when access to one of those networks is denied.

appletalk domain hop-reduction

To reduce the hop-count value in packets that are traveling between segments of a domains, use the **appletalk domain hop-reduction** command in global configuration mode. To disable the reduction of hop-count values, use the **no** form of this command.

> **appletalk domain** *domain-number* **hop-reduction**

> **no appletalk domain** *domain-number* **hop-reduction**

Syntax Description

domain-number	Number of an AppleTalk domain. It can be a decimal integer from 1 to 1,000,000.

Defaults

Reduction of hop-count values is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before you can specify the **appletalk domain hop-reduction** global configuration command, you must have created a domain with that domain number using the **appletalk domain name** global configuration command.

DDP and Routing Table Maintenance Protocol (RTMP) both impose a 15-hop limit when forwarding packets. A packet ages out and is no longer forwarded when its hop count reaches 16. To overcome RTMP's 15-hop limit, the domain router represents all networks accessible to routers on its local network as one hop away. This allows routers to maintain and send routing information about networks beyond the 15-hop limit and achieve full connectivity.

When you enable hop-count reduction, delivery of packets from networks that are farther than 15 hops apart is guaranteed.

When you enable hop-count reduction, the hop count in a packet is set to 1 as it passes from one domain to another. For example, if the hop count was 8 when the packet left one domain, its hop count is 1 when it enters the next segment of the domain.

Examples

The following example enables hop-count reduction for domain number 1:

```
appletalk domain 1 name Delta
appletalk domain 1 hop-reduction
```

Related Commands	Command	Description
	appletalk domain name	Creates a domain and assigns it a name and number.
	show appletalk domain	Displays all domain-related information.

appletalk domain name

To create a domain and assign it a name and number, use the **appletalk domain name** command in global configuration mode. To remove a domain, use the **no** form of this command.

appletalk domain *domain-number* **name** *domain-name*

no appletalk domain *domain-number* **name** *domain-name*

Syntax Description

domain-number	Number of an AppleTalk domain. It can be a decimal integer from 1 to 1000000.
domain-name	Name of an AppleTalk domain. The name must be unique across the AppleTalk internetwork. It can be up to 32 characters long and can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

Defaults

No domain is created.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example creates domain number 1 and assigns it the domain name *Delta*:

```
appletalk domain 1 name Delta
```

Related Commands

Command	Description
appletalk routing	Enables AppleTalk routing.
show appletalk domain	Displays all domain-related information.

appletalk domain remap-range

To remap ranges of AppleTalk network numbers or cable ranges between two segments of a domain, use the **appletalk domain remap-range** command in global configuration mode. To disable remapping, use the **no** form of this command.

appletalk domain *domain-number* **remap-range** {**in** | **out**} *cable-range*

no appletalk domain *domain-number* **remap-range** {**in** | **out**} [*cable-range*]

Syntax Description		
	domain-number	Number of an AppleTalk domain. It can be a decimal integer from 1 to 1,000,000.
	in	Specifies that the remapping is performed on inbound packets (that is, on packets arriving into the local interenterprise network). All network numbers or cable ranges coming from the domain are remapped into the specified range.
	out	Specifies that the remapping is performed on outbound packets (that is, on packets exiting from the local interenterprise network). All network numbers or cable ranges going to the domain are remapped into the specified range.
	cable-range	Specifies the start and end of the cable range, separated by a hyphen. The starting network must be the first AppleTalk network number or the beginning of the cable range to remap. The number must be immediately followed by a hyphen. The ending network must be the last AppleTalk network number or the end of the cable range to remap.

Defaults

No remapping is performed.

Command Modes

Global configuration

Command History	Release	Modification
	10.3	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before you can specify the **appletalk domain remap-range** command, you must create a domain with that domain number using the **appletalk domain name** global configuration command.

Inbound and outbound packets are relative to the domain router.

Ensure that the domain range you specify does not overlap any network addresses or cable ranges that already exist in the AppleTalk interenterprise network.

Each domain can have two domain mapping ranges to which to remap all incoming or outgoing network numbers or cable ranges. Incoming remapping ranges cannot overlap. However, outbound remapping ranges can overlap.

When an AppleTalk network in a domain becomes inactive, its remapped entry is removed from the remapping table. This frees the space for another network to be remapped.

If there are more remote domains than available remapping range numbers, the Cisco IOS software displays an error message and shuts down domains.

Examples   The following example remaps all network addresses and cable ranges for packets inbound from domain 1 into the address range 1000 to 1999. It also remaps packets inbound from domain 2.

```
appletalk domain 1 name Delta
appletalk domain 2 name Echo
appletalk domain 1 remap-range in 10000-10999
appletalk domain 2 remap-range in 20000-20999
```

Related Commands

Command	Description
appletalk domain name	Creates a domain and assigns it a name and number.
show appletalk remap	Displays domain remapping information.

appletalk domain-group

To assign a predefined domain number to an interface, use the **appletalk domain-group** command in interface configuration mode. To remove an interface from a domain, use the **no** form of this command.

appletalk domain-group *domain-number*

no appletalk domain-group [*domain-number*]

Syntax Description

domain-number	Number of an AppleTalk domain. It can be a decimal integer from 1 to 1,000,000.

Defaults

No domain number is assigned to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before you can assign a domain number to an interface, you must create a domain with that domain number using the **appletalk domain name** global configuration command.

One or more interfaces on a router can be members of the same domain. However, a given interface can be in only one domain.

After you assign AppleTalk interenterprise features to an AppleTalk domain, you can attribute those features to a tunnel interface configured for AURP by assigning the AppleTalk domain-group number to the tunnel interface.

Examples

The following example assigns domain group 1 to Ethernet interface 0:

```
interface ethernet 0
 appletalk domain-group 1
```

The following example assigns domain group 1 to tunnel interface 2. Assuming that domain group 1 is configured for AppleTalk interenterprise and that tunnel interface 2 is configured for AURP, any features configured for domain group 1 are ascribed to AURP on tunnel interface 2.

```
interface tunnel 2
 appletalk domain-group 1
```

Related Commands	Command	Description
	appletalk domain name	Creates a domain and assigns it a name and number.
	show appletalk domain	Displays all domain-related information.

appletalk eigrp active-time

To specify the length of time for which Enhanced Interior Gateway Routing Protocol (EIGRP) routes can be active, use the **appletalk eigrp active-time** command in global configuration mode. To return to the default value of 1 minute, use the **no** form of the command.

appletalk eigrp active-time {*minutes* | **disabled**}

no appletalk eigrp active-time

Syntax Description

minutes	Enhanced IGRP active state time (in minutes). Valid values are from 1 to 4,294,967,295 minutes.
disabled	Disables the Enhanced IGRP active state time limit. Routes remain active indefinitely.

Defaults

1 minute

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The command allows you to configure the length of time that Enhanced IGRP routes can remain active. When a route reaches the active state time limit, the Cisco IOS software logs an error and removes the route from the routing table. You can view the current setting of the Enhance IGRP active state time by using the **show appletalk globals** command.

Examples

The following example shows the current setting of the Enhanced IGRP active state time using the **show appletalk globals** command, changes the setting using the **appletalk eigrp active-time** command, and then displays the changed setting (using the **show appletalk globals** command again):

```
Router# show appletalk globals

AppleTalk global information:
  Internet is incompatible with older, AT Phase1, routers.
  There are 4 routes in the internet.
  There are 7 zones defined.
```

```
                    Logging of significant AppleTalk events is disabled.
                    ZIP resends queries every 10 seconds.
                    RTMP updates are sent every 10 seconds.
                    RTMP entries are considered BAD after 20 seconds.
                    RTMP entries are discarded after 60 seconds.
                    AARP probe retransmit count: 10, interval: 200 msec.
                    AARP request retransmit count: 5, interval: 1000 msec.
                    DDP datagrams will be checksummed.
                    RTMP datagrams will be strictly checked.
                    RTMP routes may not be propagated without zones.
                    Routes will be distributed between routing protocols.
                    Routing between local devices on an interface will not be performed.
                    EIGRP router id is: 1
                    EIGRP maximum active time is 1 minutes
                    IPTalk uses the udp base port of 768 (Default).
                    Alternate node address format will not be displayed.
                    Access control of any networks of a zone hides the zone.
                  Router#
                  Router# configure terminal
                  Enter configuration commands, one per line.  End with CNTL/Z.
                  Router(config)# appletalk eigrp active-time 5
                  Router(config)# end
                  Router#

                  Router# show appletalk globals

                  AppleTalk global information:
                    Internet is incompatible with older, AT Phase1, routers.
                    There are 4 routes in the internet.
                    There are 7 zones defined.
                    Logging of significant AppleTalk events is disabled.
                    ZIP resends queries every 10 seconds.
                    RTMP updates are sent every 10 seconds.
                    RTMP entries are considered BAD after 20 seconds.
                    RTMP entries are discarded after 60 seconds.
                    AARP probe retransmit count: 10, interval: 200 msec.
                    AARP request retransmit count: 5, interval: 1000 msec.
                    DDP datagrams will be checksummed.
                    RTMP datagrams will be strictly checked.
                    RTMP routes may not be propagated without zones.
                    Routes will be distributed between routing protocols.
                    Routing between local devices on an interface will not be performed.
                    EIGRP router id is: 1
                    EIGRP maximum active time is 5 minutes
                    IPTalk uses the udp base port of 768 (Default).
                    Alternate node address format will not be displayed.
                    Access control of any networks of a zone hides the zone.
```

Related Commands	Command	Description
	show appletalk globals	Displays information and settings about the AppleTalk internetwork and other parameters.

appletalk eigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Protocol (EIGRP) neighbor adjacencies, use the **appletalk eigrp log-neighbor-changes** command in global configuration mode. To disable this function, use the **no** form of this command.

> **appletalk eigrp log-neighbor-changes**

> **no appletalk eigrp log-neighbor-changes**

Syntax Description This command has no arguments or keywords.

Defaults No adjacency changes are logged.

Command Modes Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems. Log messages are of the form:

```
%DUAL-5-NBRCHANGE: AT/EIGRP 1: Neighbor address (interface) is state: reason
```

The arguments have the following meanings:

- *address*—Neighbor address
- *state*—Up or down
- *reason*—Reason for change

Examples The following configuration will log neighbor changes for AppleTalk Enhanced IGRP:

```
appletalk eigrp log-neighbor-changes
```

Related Commands	Command	Description
	appletalk routing	Enables AppleTalk routing.

appletalk eigrp-bandwidth-percentage

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

> **appletalk eigrp-bandwidth-percentage** *router-number percent*

> **no appletalk eigrp-bandwidth-percentage**

Syntax Description		
	router-number	Router ID.
	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.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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:

```
interface serial 0
 bandwidth 56
 appletalk eigrp-bandwidth-percentage 1 75
```

Related Commands

Command	Description
appletalk routing	Enables AppleTalk routing.
bandwidth (interface)	Sets a bandwidth value for an interface.

appletalk eigrp-splithorizon

To enable split horizon, use the **appletalk eigrp-splithorizon** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

appletalk eigrp-splithorizon

no appletalk eigrp-splithorizon

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled

Command Modes   Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   If you enable split horizon on an interface, AppleTalk Enhanced Interior Gateway Protocol (EIGRP) update and query packets are not sent if this interface is the next hop to that destination. This reduces the number of Enhanced IGRP packets of the network.

Split horizon blocks information about routes from being advertised by a router out any interface from which that information originated. This behavior usually 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 appletalk eigrp-splithorizon
```

appletalk eigrp-timers

To configure the AppleTalk Enhanced Interior Gateway Protocol (EIGRP) hello packet interval and the route hold time, use the **appletalk eigrp-timers** command in interface configuration mode. To return to the default values for these timers, use the **no** form of this command.

appletalk eigrp-timers *hello-interval hold-time*

no appletalk eigrp-timers *hello-interval hold-time*

Syntax Description		
	hello-interval	Interval between hello packets, in seconds. The default interval is 5 seconds. It can be a maximum of 30 seconds.
	hold-time	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 hold time can be in the range 15 to 90 seconds.

Defaults

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

hold-time argument:
For low-speed NBMA networks: 180 seconds
For all other networks: 15 seconds

Command Modes   Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   If the current value for the hold time is less than two times the hello interval, the hold time is reset to three times the hello interval.

If the Cisco IOS software does not receive a hello packet within the specified hold time, routes through this device are considered available.

Increasing the hold time delays route convergence across the network.

✎

Note   Do not adjust the hold time without advising technical support.

The default of 180 seconds for the *hold-time* argument 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.

The default of 60 seconds for the *hello-interval* argument 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. 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
 appletalk eigrp-timers 10 45
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

appletalk event-logging

To log significant network events, use the **appletalk event-logging** command in global configuration mode. To disable this function, use the **no** form of this command.

appletalk event-logging

no appletalk event-logging

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **appletalk event-logging** command logs a subset of messages produced by **debug appletalk** command. These messages include routing changes, zone creation, port status, and address.

Examples   The following example enables logging of AppleTalk events:

```
appletalk routing
appletalk event-logging
```

Related Commands

Command	Description
debug appletalk	Displays information about routing changes, zone creation, port status, and address.
show appletalk globals	Displays information and settings about the AppleTalk internetwork and other parameters.

appletalk free-trade-zone

To establish a free-trade zone, use the **appletalk free-trade-zone** command in interface configuration mode. To disable a free-trade zone, use the **no** form of this command.

> **appletalk free-trade-zone**

> **no appletalk free-trade-zone**

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   A *free-trade zone* is a part of an AppleTalk internetwork that is accessible by two other parts of the internetwork, neither of which can access the other. You might want to create a free-trade zone to allow the exchange of information between two organizations that otherwise want to keep their internetworks isolated from each other or that do not have physical connectivity with one another.

You apply the **appletalk free-trade-zone** command to each interface attached to the common-access network. This command has the following effect on the interface:

- All incoming RTMP updates are ignored.
- All outgoing RTMP updates contain no information.
- NBP conversion of BrRq packets to FwdReq packets is not performed.

The GZL for free-trade zone nodes will be empty.

Examples   The following example establishes a free-trade zone on Ethernet interface 0:

```
interface ethernet 0
 appletalk cable-range 5-5
 appletalk zone FreeAccessZone
 appletalk free-trade-zone
```

appletalk getzonelist-filter

To filter GetZoneList (GZL) replies, use the **appletalk getzonelist-filter** command in interface configuration mode. To remove a filter, use the **no** form of this command.

appletalk getzonelist-filter *access-list-number*

no appletalk getzonelist-filter [*access-list-number*]

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.

Defaults

No filters are preconfigured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

GZL filters define conditions for zones only. They cannot use access lists that define conditions for network numbers or cable ranges. All network number and cable range information in the access list assigned to an interface with the **appletalk getzonelist-filter** command is ignored.

Using a GZL filter is not a complete replacement for anonymous network numbers. In order to prevent users from seeing a zone, all routers must implement the GZL filter. If there are any routers from other vendors on the network, the GZL filter will not have a consistent effect.

The Macintosh Chooser uses ZIP GZL requests to compile a list of zones from which the user can select services. Any router on the same network as the Macintosh can respond to these requests with a GZL reply. You can create a GZL filter on the router to control which zones the router mentions in its GZL replies. This has the effect of controlling the list of zones that are displayed by the Chooser.

When defining GZL filters, you should ensure that all routers on the same network filter GZL reply identically. Otherwise, the Chooser will list different zones depending upon which router responded to the request. Also, inconsistent filters can result in zones appearing and disappearing every few seconds when the user remains in the Chooser. Because of these inconsistencies, you should normally use the **appletalk getzonelist-filter** command only when all routers in the internetwork are our routers, unless the routers from other vendors have a similar feature.

Replies to GZL requests are also filtered by any **appletalk distribute-list out** filter that has been applied to the same interface. You must specify an **appletalk getzonelist-filter** command only if you want additional filtering to be applied to GZL replies. This filter is rarely needed except to eliminate zones that do not contain user services.

Examples   The following example does not include the zone Engineering in GZL replies sent out Ethernet
interface 0:

```
access-list 600 deny zone Engineering
interface ethernet 0
 appletalk getzonelist-filter 600
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk permit-partial-zones	Permits access to the other networks in a zone when access to one of those networks is denied.

appletalk glean-packets

To derive AppleTalk Address Resolution Protocol (AARP) table entries from incoming packets, use the **appletalk glean-packets** command in interface configuration mode. To disable this function, use the **no** form of this command.

appletalk glean-packets

no appletalk glean-packets

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled

Command Modes   Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The Cisco IOS software automatically derives AARP table entries from incoming packets. This process, referred to as *gleaning*, speeds up the process of populating the AARP table.

Our implementation of AppleTalk does not forward packets with local source and destination network addresses. This behavior does not conform with the definition of AppleTalk in Apple Computer's *Inside AppleTalk* publication. However, this behavior is designed to prevent any possible corruption of the AARP table in any AppleTalk node that is performing MAC-address gleaning.

Examples   The following example disables the building of the AARP table using information derived from incoming packets:

```
interface ethernet 0
 appletalk address 33
 no appletalk glean-packets
```

appletalk ignore-verify-errors

To allow the Cisco IOS software to start functioning even if the network is misconfigured, use the **appletalk ignore-verify-errors** command in global configuration mode. To disable this function, use the **no** form of this command.

appletalk ignore-verify-errors

no appletalk ignore-verify-errors

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Use this command only under the guidance of a customer engineer or other service representative. A router that starts routing in a misconfigured network will serve only to make a bad situation worse; it will not correct other misconfigured routers.

Examples   The following example allows a router to start functioning without verifying network misconfiguration:

```
appletalk ignore-verify-errors
```

appletalk iptalk

To enable IPTalk encapsulation on a tunnel interface, use the **appletalk iptalk** command in interface configuration mode. To disable IPTalk encapsulation, use the **no** form of this command.

appletalk iptalk *network zone*

no appletalk iptalk [*network zone*]

Syntax Description		
network		AppleTalk network address assigned to the interface. The argument *network* is the 16-bit network number in decimal.
zone		Name of the zone for the connected AppleTalk network.

Defaults   Disabled

Command Modes   Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Use the **appletalk iptalk** command to enable IPTalk encapsulation on a tunnel interface. This command encapsulates AppleTalk in IP packets in a manner compatible with the Columbia AppleTalk Package (CAP) IPTalk and the Kinetics IPTalk implementations. IPTalk is configured on a tunnel interface.

This command allows AppleTalk communication with UNIX hosts running older versions of CAP that do not support native AppleTalk EtherTalk encapsulations. Typically, Apple Macintosh users wishing to communicate with these servers would have their connections routed through a Kinetics FastPath router running Kinetics IPTalk software.

This command is provided as a migration command; newer versions of CAP provide native AppleTalk EtherTalk encapsulations, and the IPTalk encapsulation is no longer required. Our implementation of IPTalk assumes that AppleTalk is already being routed on the backbone; there is currently no LocalTalk hardware interface for our routers.

Our implementation of IPTalk does not support manually configured AppleTalk-to-IP address mapping (atab). The address mapping provided is the same as the Kinetics IPTalk implementation when the atab facility is not enabled. This address mapping functions as follows: The IP subnet mask used on the Ethernet interface on which IPTalk is enabled is inverted (ones complement). This result is then masked against 255 (0xFF hexadecimal). This is then masked against the low-order 8 bits of the IP address to obtain the AppleTalk node number.

Examples   The following example configuration illustrates how to configure IPTalk:

```
interface Ethernet0
 ip address 172.31.255.118 255.255.255.0
 interface Tunnel0
 tunnel source Ethernet0
 tunnel mode iptalk
 appletalk iptalk 30 UDPZone
```

In this configuration, the IP subnet mask would be inverted:

```
255.255.255.0 inverted yields: 0.0.0.255
```

Masked with 255 it yields 255, and masked with the low-order 8 bits of the interface IP address it yields 118.

This means that the AppleTalk address of the Ethernet 0 interface seen in the UDPZone zone is 30.118. This caveat should be noted, however: Should the host field of an IP subnet mask for an interface be more than 8 bits wide, it will be possible to obtain conflicting AppleTalk node numbers. For instance, consider a situation where the subnet mask for the Ethernet 0 interface above is 255.255.240.0, meaning that the host field is 12 bits wide.

Related Commands

Command	Description
appletalk iptalk-baseport	Specifies the UDP port number when configuring IPTalk.
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel source	Sets the source address of a tunnel interface.

appletalk iptalk-baseport

To specify the User Datagram Protocol (UDP) port number when configuring IPTalk, use the **appletalk iptalk-baseport** command in global configuration mode. To return to the default UDP port number, use the **no** form of this command.

appletalk iptalk-baseport *port-number*

no appletalk iptalk-baseport [*port-number*]

Syntax Description

port-number	First UDP port number in the range of UDP ports used in mapping AppleTalk well-known Datagram Delivery Protocol (DDP) socket numbers to UDP ports.

Defaults   768

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Implementations of IPTalk prior to April 1988 mapped well-known DDP socket numbers to privileged UDP ports starting at port number 768. In April 1988, the Network Information Center (NIC) assigned a range of UDP ports for the defined DDP well-known sockets starting at UDP port number 200 and assigned these ports the names at-nbp, at-rtmp, at-echo, and at-zis. Release 6 and later of the CAP program dynamically decides which port mapping to use. If there are no AppleTalk service entries in the UNIX system's */etc/services* file, CAP uses the older mapping starting at UDP port number 768.

The default UDP port mapping supported by our implementation of IPTalk is 768. If there are AppleTalk service entries in the UNIX system's */etc/services* file, you should specify the beginning of the UDP port mapping range with the **appletalk iptalk-baseport** command.

Examples   The following example sets the base UDP port number to 200, which is the official NIC port number, and configures IPTalk on Ethernet interface 0:

```
appletalk routing
appletalk iptalk-baseport 200
!
interface Ethernet 0
ip address 172.31.255.118 255.255.255.0
appletalk address 20.129
```

```
appletalk zone Native AppleTalk
appletalk iptalk 30.0 UDPZone
```

Related Commands	Command	Description
	appletalk iptalk	Enables IPTalk encapsulation on a tunnel interface.

appletalk lookup-type

To specify which Name Binding Protocol (NBP) service types are retained in the name cache, use the **appletalk lookup-type** command in global configuration mode. To disable the caching of services, use the **no** form of this command.

appletalk lookup-type *service-type*

no appletalk lookup-type *service-type*

Syntax Description

service-type	AppleTalk service types. The name of a service type can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal numbers. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of possible types, see Table 1 in the "Usage Guidelines" section.

Defaults The entries from active adjacent Cisco routers are retained in the name cache.

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines You can issue multiple **appletalk lookup-type** commands. The Cisco IOS software does not query the entire zone, but instead polls only the connected networks. This reduces network overhead and means that the name cache contains entries only for selected services that are in a directly connected network or zone, not for all the selected services in a network or zone.

Table 8 lists some AppleTalk service types.

Table 8   AppleTalk Service Types

Service Type[1]	Description
Services for Cisco Routers	
ciscoRouter	Active adjacent Cisco routers. This service type is initially enabled by default.
IPADDRESS	Addresses of active MacIP server.
IPGATEWAY	Names of active MacIP server.

Table 8   AppleTalk Service Types (continued)

Service Type[1]	Description
Services for Other Vendors' Routers	
AppleRouter	Apple internetwork router.
FastPath	Shiva LocalTalk gateway.
GatorBox	Cayman LocalTalk gateway.
systemRouter	Cisco's OEM router name.
Workstation	Macintosh running System 7. The machine type also is defined, so it is possible to easily identify all user nodes.

1. Type all service names exactly as shown. Spaces are valid. Do not use leading or trailing spaces when entering service names.

If you omit the *service-type* argument from the **no appletalk lookup-type** command, no service types except those relating to our devices are cached.

To display information that is stored in the name cache about the services being used by our routers and other vendors' routers, use the **show appletalk name-cache** command.

If a neighboring router is not our device or is running our software that is earlier than Release 9.0, it is possible our device will be unable to determine the name of the neighbor. This is normal behavior, and there is no workaround.

If AppleTalk routing is enabled, enabling Simple Network Management Protocol (SNMP) will automatically enable SNMP over DDP.

Name cache entries are deleted after several interval periods expire without being refreshed. (You set the interval with the **appletalk name-lookup-interval** command.) At each interval, a single request is sent via each interface that has valid addresses.

Examples

The following example caches information about GatorBox services, Apple internetwork routers, MacIP services, and workstations. Information about our devices is automatically cached.

```
appletalk lookup-type GatorBox
appletalk lookup-type AppleRouter
appletalk lookup-type IPGATEWAY
appletalk lookup-type Workstation
```

Related Commands

Command	Description
appletalk name-lookup-interval	Sets the interval between service pollings by the router on its AppleTalk interfaces.
show appletalk name-cache	Displays a list of NBP services offered by nearby routers and other devices that support NBP.
show appletalk nbp	Displays the contents of the NBP name registration table.

appletalk macip dynamic

To allocate IP addresses to dynamic MacIP clients, use the **appletalk macip dynamic** command in global configuration mode. To delete a MacIP dynamic address assignment, use the **no** form of this command.

appletalk macip dynamic *ip-address* [*ip-address*] **zone** *server-zone*

no appletalk macip dynamic *ip-address* [*ip-address*] **zone** *server-zone*

Syntax Description

ip-address	IP address, in four-part, dotted decimal notation. To specify a range, enter two IP addresses, which represent the first and last addresses in the range.
zone *server-zone*	Zone in which the MacIP server resides. The argument *server-zone* can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to Apple Computer's *Inside AppleTalk* publication.

Defaults

No IP addresses are allocated.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **appletalk macip dynamic** command when configuring MacIP.

Dynamic clients are those that accept *any* IP address assignment within the dynamic range specified.

In general, it is recommended that you do not use fragmented address ranges in configuring ranges for MacIP. However, if this is unavoidable, use the **appletalk macip dynamic** command to specify as many addresses or ranges as required and use the **appletalk macip static** command to assign a specific address or address range.

To shut down all running MacIP services, use the following command:

no appletalk macip

To delete a particular dynamic address assignment from the configuration, use the following command:

no appletalk macip dynamic *ip-address* [*ip-address*] **zone** *server-zone*

Examples

The following example illustrates MacIP support for dynamically addressed MacIP clients with IP addresses in the range 172.16.1.28 to 172.16.1.44:

```
! This global statement specifies the MacIP server address and zone:
appletalk macip server 172.16.1.27 zone Engineering
!
! This global statement identifies the dynamically addressed clients:
appletalk macip dynamic 172.16.1.28 172.16.1.44 zone Engineering
!
! These statements assign the IP address and subnet mask for Ethernet interface 0:
interface ethernet 0
ip address 172.16.1.27 255.255.255.0
!
! This global statement enables AppleTalk routing on the router.
appletalk routing
!
! These statements enable AppleTalk routing on the interface and
! set the zone name for the interface
interface ethernet 0
 appletalk cable-range 69-69 69.128
 appletalk zone Engineering
```

Related Commands

Command	Description
appletalk macip server	Establishes a MacIP server for a zone.
appletalk macip static	Allocates an IP address to be used by a MacIP client that has reserved a static IP address.
ip address	Sets a primary or secondary IP address for an interface.
show appletalk macip-servers	Displays status information about related servers.

appletalk macip server

To establish a MacIP server for a zone, use the **appletalk macip server** command in global configuration mode. To shut down a MacIP server, use the **no** form of this command.

appletalk macip server *ip-address* **zone** *server-zone*

no appletalk macip server *ip-address* **zone** *server-zone*

Syntax Description

ip-address	IP address, in four-part dotted decimal notation. It is suggested that this address match the address of an existing IP interface.
zone *server-zone*	Zone in which the MacIP server resides. The argument *server-zone* can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to Apple Computer's *Inside AppleTalk* publication.

Defaults

No MacIP server is established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **appletalk macip server** command when configuring MacIP.

You can configure only one MacIP server per AppleTalk zone, and the server must reside in the default zone. A server is not registered via NBP until at least one MacIP resource is configured.

You can configure multiple MacIP servers for a router, but you can assign only one MacIP server to a particular zone and only one IP interface to each MacIP server. In general, you must be able to establish an alias between the IP address you assign with the **appletalk macip server** command and an existing IP interface. For implementation simplicity, it is suggested that the address specified in this command match an existing IP interface address.

To shut down all active MacIP servers, use the following command:

no appletalk macip

To delete a specific MacIP server from the MacIP configuration, use the following command:

no appletalk macip server *ip-address* **zone** *server-zone*

Examples
The following example establishes a MacIP server on Ethernet interface 0 in AppleTalk zone Engineering. It then assigns an IP address to the Ethernet interface and enables AppleTalk routing on a router and its Ethernet interface.

```
appletalk macip server 172.19.1.27 zone Engineering
ip address 172.19.1.27 255.255.255.0
appletalk routing
interface ethernet 0
 appletalk cable-range 69-69 69.128
 appletalk zone Engineering
```

Related Commands

Command	Description
appletalk macip dynamic	Allocates IP addresses to dynamic MacIP clients.
appletalk macip static	Allocates an IP address to be used by a MacIP client that has reserved a static IP address.
ip address	Sets a primary or secondary IP address for an interface.
show appletalk macip-servers	Displays status information about related servers.

appletalk macip static

To allocate an IP address to be used by a MacIP client that has reserved a static IP address, use the **appletalk macip static** command in global configuration mode. To delete a MacIP static address assignment, use the **no** form of this command.

> **appletalk macip static** *ip-address* [*ip-address*] **zone** *server-zone*

> **no appletalk macip static** *ip-address* [*ip-address*] **zone** *server-zone*

Syntax Description

ip-address	IP address, in four-part, dotted decimal format. To specify a range, enter two IP addresses, which represent the first and last addresses in the range.
zone *server-zone*	Zone in which the MacIP server resides. The argument *server-zone* can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to Apple Computer's *Inside AppleTalk* publication.

Defaults   No IP address is allocated.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Use the **appletalk macip static** command when configuring MacIP.

Static addresses are for users who require fixed addresses for IP name domain name service and for administrators who do want addresses to change so they can always know who has what IP address.

In general, it is recommended that you do not use fragmented address ranges in configuring ranges for MacIP. However, if this is unavoidable, use the **appletalk macip dynamic** command to specify as many addresses or ranges as required, and then use the **appletalk macip static** command to assign a specific address or address range.

To shut down all running MacIP services, use the following command:

> **no appletalk macip**

To delete a particular static address assignment from the configuration, use the following command:

no appletalk macip static *ip-address* [*ip-address*] **zone** *server-zone*

Examples

The following example illustrates MacIP support for MacIP clients with statically allocated IP addresses. The IP addresses range is from 172.31.1.50 to 172.31.1.66. The three nodes that have the specific addresses are 172.31.1.81, 172.31.1.92, and 172.31.1.101.

```
! This global statement specifies the MacIP server address and zone:
appletalk macip server 172.31.1.27 zone Engineering
!
! These global statements identify the statically addressed clients:
appletalk macip static 172.31.1.50 172.31.1.66 zone Engineering
appletalk macip static 172.31.1.81 zone Engineering
appletalk macip static 172.31.1.92 zone Engineering
appletalk macip static 172.31.1.101 zone Engineering
!
! These statements assign the IP address and subnet mask for Ethernet interface 0:
interface ethernet 0
 ip address 172.31.1.27 255.255.255.0
!
! This global statement enables AppleTalk routing on the router.
appletalk routing
!
! These statements enable AppleTalk routing on the interface and
! set the zone name for the interface
interface ethernet 0
 appletalk cable-range 69-69 69.128
 appletalk zone Engineering
```

Related Commands

Command	Description
appletalk macip dynamic	Allocates IP addresses to dynamic MacIP clients.
appletalk macip server	Establishes a MacIP server for a zone.
ip address	Sets a primary or secondary IP address for an interface.
show appletalk macip-servers	Displays status information about related servers.

appletalk maximum-paths

To define the maximum number of equal-cost paths that the router should use when balancing the traffic load, use the **appletalk maximum-paths** command in global configuration mode. To restore the default value, use the **no** form of this command.

appletalk maximum-paths [*paths*]

no appletalk maximum-paths [*paths*]

Syntax Description

paths	(Optional) Maximum number of equal-cost paths to be used for balancing the traffic load. The *paths* argument is a decimal number in the range of 1 to 16.

Defaults
The default value is 1.

Command Modes
Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines
Use the **appletalk maximum-paths** command when configuring AppleTalk load balancing.

The **appletalk 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 the value of *paths* is greater than 1, packets are distributed over the multiple equal-cost paths in round-robin fashion on a packet-by-packet basis.

Examples
The following example defines four equal-cost paths:

```
! Sets the maximum number of equal-cost paths to 4.
appletalk maximum-paths 4
```

The following example restores the default value:

```
! Restores the default value.
no appletalk maximum-paths 4
```

appletalk name-lookup-interval

To set the interval between service pollings by the router on its AppleTalk interfaces, use the **appletalk name-lookup-interval** command in global configuration mode. To purge the name cache and return to the default polling interval, use the **no** form of this command.

appletalk name-lookup-interval *seconds*

no appletalk name-lookup-interval [*seconds*]

Syntax Description

seconds	Interval, in seconds, between NBP lookup pollings. This can be any positive integer; there is no upper limit. It is recommended that you use an interval between 300 seconds (5 minutes) and 1200 seconds (20 minutes). The smaller the interval, the more packets are generated to handle the names. Specifying an interval of 0 purges all entries from the name cache and disables the caching of service type information that is controlled by the **appletalk lookup-type** command, including the caching of information about our routers.

Defaults

The default is 0, which purges all entries from the name cache and disables the caching of service type information.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software collects name information only for entities on connected AppleTalk networks. This reduces overhead.

If you enter an interval of 0, all polling for services (except ciscoRouter) is disabled. If you reenter a nonzero value, the configuration specified by the **appletalk lookup-type** command is reinstated. You cannot disable the lookup of ciscoRouter.

Examples

The following example sets the lookup interval to 20 minutes:

```
appletalk name-lookup-interval 1200
```

Related Commands	Command	Description
	appletalk lookup-type	Specifies which NBP service types are retained in the name cache.
	show appletalk name-cache	Displays a list of NBP services offered by nearby routers and other devices that support NBP.

appletalk permit-partial-zones

To permit access to the other networks in a zone when access to one of those networks is denied, use the **appletalk permit-partial-zones** command in global configuration mode. To deny access to all networks in a zone if access to one of those networks is denied, use the **no** form of this command.

> **appletalk permit-partial-zones**

> **no appletalk permit-partial-zones**

Syntax Description   This command has no arguments or keywords.

Defaults   Access is denied.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The permitting of partial zones provides IP-style access control.

When you enable the use of partial zones, the NBP protocol cannot ensure the consistency and uniqueness of name bindings.

If you enable the use of partial zones, access control behavior is compatible with that of Cisco IOS Release 8.3.

Examples   The following example allows partial zones:

```
appletalk permit-partial-zones
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk getzonelist-filter	Filters GZL replies.

appletalk pre-fdditalk

To enable the recognition of pre-FDDITalk packets, use the **appletalk pre-fdditalk** command in global configuration mode. To disable this function, use the **no** form of this command.

appletalk pre-fdditalk

no appletalk pre-fdditalk

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Use this command to have the Cisco IOS software recognize AppleTalk packets sent on the FDDI ring from routers that are running Cisco software releases prior to Release 9.0(3) or Release 9.1(2).

Examples   The following example disables the recognition of pre-FDDITalk packets:

```
no appletalk pre-fdditalk
```

appletalk protocol

To specify the routing protocol to use on an interface, use the **appletalk protocol** command in interface configuration mode. To disable a routing protocol, use the **no** form of this command.

appletalk protocol {**aurp** | **rtmp**}

no appletalk protocol {**aurp** | **rtmp**}

Syntax Description		
	aurp	Specifies that the routing protocol to use is AppleTalk Update-Based Routing Protocol (AURP). You can enable AURP only on tunnel interfaces.
	rtmp	Specifies that the routing protocol to use is Routing Table Maintenance Protocol (RTMP), which is enabled by default.

Defaults   RTMP

Command Modes   Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.
	12.2(13)T	The **eigrp** keyword was removed.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   You can configure an interface to use RTMP. The Cisco IOS software will continue to send out RTMP routing updates.

You cannot disable RTMP without first enabling AURP.

Enabling AURP automatically disables RTMP.

You can enable AURP only on tunnel interfaces.

Examples   The following example enables AURP on tunnel interface 1:

```
interface tunnel 1
 appletalk protocol aurp
```

The following example disables RTMP on serial interface 0:

```
interface serial 0
 no appletalk protocol rtmp
```

Related Commands	Command	Description
	appletalk routing	Enables AppleTalk routing.

appletalk proxy-nbp

To assign a proxy network number for each zone in which there is a router that supports only nonextended AppleTalk, use the **appletalk proxy-nbp** command in global configuration mode. To delete the proxy, use the **no** form of this command.

appletalk proxy-nbp *network-number zone-name*

no appletalk proxy-nbp [*network-number zone-name*]

Syntax Description	*network-number*	Network number of the proxy. It is a 16-bit decimal number and must be unique on the network. This is the network number that will be advertised by the Cisco IOS software as if it were a real network number.
	zone-name	Name of the zone that contains the devices that support only nonextended AppleTalk. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

Defaults   No proxy network number is assigned.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **appletalk proxy-nbp** command provides compatibility between AppleTalk Phase 1 and AppleTalk Phase 2 networks.

Proxy routes are included in outgoing RTMP updates as if they were directly connected routes, although they are not really directly connected, since they are not associated with any interface. Whenever an NBQ BrRq for the zone in question is generated by anyone anywhere in the internetwork, an NBP FwdReq is directed to any router connected to the proxy route. The Phase 2 router, which is the only router directly connected, converts the FwdReq to LkUps, which are understood by Phase 1 routers, and sends them to every network in the zone.

In an environment in which there are Phase 1 and Phase 2 networks, you must specify at least one **appletalk proxy-nbp** command for each zone that has a nonextended-only AppleTalk router.

The proxy network number you assign with the **appletalk proxy-nbp** command cannot also be assigned to a router, nor can it also be associated with a physical network.

You must assign only one proxy network number for each zone. However, you can define additional proxies with different network numbers to provide redundancy. Each proxy generates one or more packets for each forward request it receives. All other packets sent to the proxy network address are discarded. Defining redundant proxy network numbers increases the NBP traffic linearly.

Examples

The following example defines network number 60 as an NBP proxy for the zone *Twilight*:

```
appletalk proxy-nbp 60 Twilight
```

Related Commands

Command	Description
show appletalk route	Displays all entries or specified entries in the AppleTalk routing table.

appletalk require-route-zones

To prevent the advertisement of routes (network numbers or cable ranges) that have no assigned zone, use the **appletalk require-route-zones** command in global configuration mode. To disable this option and allow the Cisco IOS software to advertise to its neighbors routes that have no network-zone association, use the **no** form of this command.

    appletalk require-route-zones

    no appletalk require-route-zones

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **appletalk require-route-zones** command ensures that all networks have zone names prior to advertisement to neighbors.

The **no appletalk require-route-zones** command enables behavior compatible with Cisco IOS Release 8.3.

Using this command helps prevent ZIP protocol storms. ZIP protocol storms can arise when corrupt routes are propagated and routers broadcast ZIP requests to determine the network/zone associations.

When the **appletalk require-route-zones** command is enabled, the Cisco IOS software will not advertise a route to its neighboring routers until it has obtained the network-zone associations. This effectively limits the storms to a single network rather than the entire internet.

As an alternative to disabling this option, use the **appletalk getzonelist-filter** interface configuration command to filter *empty* zones from the list presented to users.

You can configure different zone lists on different interfaces. However, you are discouraged from doing this because AppleTalk users expect to have the same user zone lists at any end node in the internet.

The filtering provided by the **appletalk require-route-zones** command does not prevent explicit access via programmatic methods, but should be considered a user optimization to suppress unused zones. You should use other forms of AppleTalk access control lists to actually *secure* a zone or network.

Examples   The following example configures a router to prevent the advertisement of routes that have no assigned zone:

```
appletalk require-route-zones
```

appletalk route-cache

To enable fast switching on all supported interfaces, use the **appletalk route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

appletalk route-cache

no appletalk route-cache

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled on all interfaces that support fast switching.

Command Modes   Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Fast switching allows higher throughput by switching a packet using a cache created by previous packets. Fast-switching is enabled by default on all interfaces that support fast switching, including Token Ring, Frame Relay, PPP, High-Level Data Link Control (HDLC), SMDS, and ATM. Note that fast switching is not supported over X.25 and Link Access Procedure, Balanced (LAPB), encapsulations, or on the CSC-R16, CSC-1R, or CSC-2R STR Token Ring adapters.

Packet transfer performance is generally better when fast switching is enabled. However, you may want to disable fast switching in order to save memory space on interface cards and to help avoid congestion when high-bandwidth interfaces are writing large amounts of information to low-bandwidth interfaces.

Fast switching of extended AppleTalk is supported on serial lines with several encapsulation types (for example, SMDS and HDLC). Fast switching of nonextended AppleTalk is not supported on serial lines.

Examples   The following example disables fast switching on an interface:

```
interface ethernet 0
 appletalk cable-range 10-20
 appletalk zone Twilight
 no appletalk route-cache
```

Related Commands	Command	Description
	show appletalk cache	Displays the routes in the AppleTalk fast-switching table on an extended AppleTalk network.

appletalk route-redistribution

To redistribute Routing Table Maintenance Protocol (RTMP) routes into AppleTalk Enhanced Interior Gateway Routing Protocol (EIGRP) and vice versa, use the **appletalk route-redistribution** command in global configuration mode. To keep Enhanced IGRP and RTMP routes separate, use the **no** form of this command.

appletalk route-redistribution

no appletalk route-redistribution

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled when Enhanced IGRP is enabled.

Command Modes   Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Redistribution allows routing information generated by one protocol to be advertised in another.

In the automatic redistribution of routes between Enhanced IGRP and RTMP, an RTMP hop is treated as having a slightly worse metric than an equivalent Enhanced IGRP hop on a 9.6-kbps link. This allows Enhanced IGRP to be preferred over RTMP except in the most extreme of circumstances. Typically, you will see this only when using tunnels. If you want an Enhanced IGRP path in a tunnel to be preferred over an alternate RTMP path, you should set the interface delay and bandwidth parameters on the tunnel to bring the metric of the tunnel down to being better than a 9.6-kbps link.

Examples   In the following example, RTMP routing information is not redistributed:

```
appletalk routing eigrp 23
no appletalk route-redistribution
```

appletalk routing

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

appletalk routing

no appletalk routing

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.
10.3	The **eigrp** keyword was added.
12.2(13)T	The **eigrp** keyword and *router-number* argument were removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines If you do not specify the optional keyword and argument, this command enables AppleTalk routing using the RTMP routing protocol.

Examples The following example enables AppleTalk protocol processing:

```
appletalk routing
```

Related Commands

Command	Description
appletalk address	Enables nonextended AppleTalk routing on an interface.
appletalk cable-range	Enables an extended AppleTalk network.
appletalk protocol	Specifies the routing protocol to use on an interface.
appletalk zone	Sets the zone name for the connected AppleTalk network.

appletalk rtmp jitter

To set the interval timer on a router between subsequent AppleTalk Routing Table Maintenance Protocol (RTMP) routing updates, use the **appletalk rtmp jitter** command in global configuration mode. To disable this mode, use the **no** form of the command.

appletalk rtmp jitter *percent*

no appletalk rtmp jitter *percent*

Syntax Description	*percent*	Ranges from 0 to 100.

Defaults

0 percent

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The interval between subsequent routing updates is randomized to reduce the probability of synchronization with the routing updates from other routers on the same link. This is done by maintaining a separate transmission interval timer for each advertising interface.

The **appletalk rtmp jitter** command allows the user to stagger the routing updates and to avoid sending the updates every 10 seconds.

Examples

The following example sets AppleTalk RTMP updates to fluctuate 20 percent of the update interval time:

```
appletalk rtmp jitter 20
```

Related Commands

Command	Description
show appletalk globals	Displays information and settings about the AppleTalk internetwork and other parameters.

appletalk rtmp-stub

To enable AppleTalk Routing Table Maintenance Protocol (RTMP) stub mode, use the **appletalk rtmp-stub** command in interface configuration mode. To disable this mode, use the **no** form of the command.

appletalk rtmp-stub

no appletalk rtmp-stub

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled

Command Modes   Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   This command enables routers running RTMP to reduce the amount of CPU processing that RTMP modules use. RTMP modules send "stub" packets instead of full RTMP packets when you enable stub mode.

A stub packet is only the first tuple of an RTMP packet. The first tuple indicates the network number range assigned to that network. End nodes use stub packets to determine if their node number is in the right network range.

Upon startup, an end node on an extended network uses stub packets to verify that its previous node number is still within the segment's network number range. If it is, the end node reuses the previous node number and stores the network number range information. If an end node learns upon startup that its previous node number does not fall within the segment's new network number range, the end node picks a new node number based on the new network number range and stores the new network number range information.

After startup, end nodes use subsequent stub packets to verify that the network number range sent in the stub packets precisely matches its stored network number range. In this way, stub packets keep end nodes alive.

When routers that have stub mode enabled receive full RTMP packets, they discard these packets. Discarding full RTMP packets when stub mode is enabled saves the overhead processing of RTMP routes.

You can also use stub mode on "end" networks. End networks are those to which no other routers attach. Because no other routers are listening for routes on these end segments, there is no need for the end router to send full RTMP packets to these end segments. The end router can send stub packets to keep end nodes alive.

Examples

The following example turns on AppleTalk RTMP stub mode:

```
appletalk rtmp-stub
```

Related Commands

Command	Description
show appletalk interface	Displays the status of the AppleTalk interfaces configured in the Cisco IOS software and the parameters configured on each interface.

appletalk send-rtmps

To allow the Cisco IOS software to send routing updates to its neighbors, use the **appletalk send-rtmps** command in interface configuration mode. To block updates from being sent, use the **no** form of this command.

appletalk send-rtmps

no appletalk send-rtmps

Syntax Description   This command has no arguments or keywords.

Defaults   Routing updates are sent.

Command Modes   Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   If you block the sending of routing updates, an interface on the network that has AppleTalk enabled is not "visible" to other routers on the network.

Examples   The following example prevents a router from sending routing updates to its neighbors:

```
no appletalk send-rtmps
```

Related Commands

Command	Description
appletalk require-route-zones	Prevents the advertisement of routes (network numbers or cable ranges) that have no assigned zone.
appletalk strict-rtmp-checking	Performs maximum checking of routing updates to ensure their validity.
appletalk timers	Changes the routing update timers.

appletalk static cable-range

To define a static route or a floating static route on an extended network, use the **appletalk static cable-range** command in global configuration mode. To remove a static route, use the **no** form of this command.

appletalk static cable-range *cable-range* **to** *network.node* [**floating**] **zone** *zone-name*

no appletalk static cable-range *cable-range* **to** *network.node* [**floating**] [**zone** *zone-name*]

Syntax Description		
	cable-range	Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal number from 0 to 65,279. The starting network number must be less than or equal to the ending network number.
	to *network.node*	AppleTalk network address of the remote router. The argument *network* is the 16-bit network number in the range 0 to 65,279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.
	floating	(Optional) Specifies that this route is a floating static route, which is a static route that can be overridden by a dynamically learned route.
	zone *zone-name*	Name of the zone on the remote network. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

Defaults No static routes are defined.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines You cannot delete a particular zone from the zone list without first deleting the static route.

When links associated with static routes are lost, traffic may stop being forwarded even though alternative paths might be available. For this reason, you should be careful when assigning static routes.

Floating static routes are a kind of static route that can be overridden by dynamically learned routes. Floating static routes allow you to switch to another path whenever routing information for a destination is lost. One application of floating static routes is to provide back-up routes in topologies where dial-on-demand routing is used.

If you configure a floating static route, the Cisco IOS software checks to see if an entry for the route already exists in its routing table. If a dynamic route already exists, the floating static route is placed in reserve as part of a floating static route table. When the software detects that the dynamic route is no longer available, it replaces the dynamic route with the floating static route for that destination. If the route is later relearned dynamically, the dynamic route replaces the floating static route and the floating static route is again placed in reserve.

To avoid the possibility of a routing loop occurring, by default floating static routes are not redistributed into other dynamic protocols.

Examples

The following example creates a static route to the remote router whose address is 1.2 on the remote network 100-110 that is in the remote zone *Remote*:

```
appletalk static cable-range 100-110 to 1.2 zone Remote
```

The following example creates a floating static route to the remote router whose address is 1.3 on the remote network 100-110 that is in the remote zone *Remote*:

```
appletalk static cable-range 100-110 to 1.3 floating zone Remote
```

Related Commands

Command	Description
appletalk static network	Defines a static route or a floating static route on a nonextended network.
show appletalk route	Displays all entries or specified entries in the AppleTalk routing table.
show appletalk static	Displays information about the statically defined routes.

appletalk static network

To define a static route or a floating static route on a nonextended network, use the **appletalk static network** command in global configuration mode. To remove a static route, use the **no** form of this command.

appletalk static network *network-number* **to** *network.node* [**floating**] **zone** *zone-name*

no appletalk static network *network-number* **to** *network.node* [**floating**] [**zone** *zone-name*]

Syntax Description		
	network-number	AppleTalk network number assigned to the interface. It is a 16-bit decimal number and must be unique on the network. This is the network number that will be advertised by the Cisco IOS software as if it were a real network number.
	to *network.node*	AppleTalk network address of the remote router. The argument *network* is the 16-bit network number in the range 0 to 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.
	floating	(Optional) Specifies that this route is a floating static route, which is a static route that can be overridden by a dynamically learned route.
	zone *zone-name*	Name of the zone on the remote network. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

Defaults   No static routes are defined.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   You cannot delete a particular zone from the zone list without first deleting the static route.

When links associated with static routes are lost, traffic may stop being forwarded even though alternative paths might be available. For this reason, you should be careful when assigning static routes.

Floating static routes are a kind of static route that can be overridden by dynamically learned routes. Floating static routes allow you to switch to another path whenever routing information for a destination is lost. One application of floating static routes is to provide back-up routes in topologies where dial-on-demand routing is used.

If you configure a floating static route, the Cisco IOS software checks to see if an entry for the route already exists in its routing table. If a dynamic route already exists, the floating static route is placed in reserve as part of a floating static route table. When the Cisco IOS software detects that the dynamic route is no longer available, it replaces the dynamic route with the floating static route for that destination. If the route is later relearned dynamically, the dynamic route replaces the floating static route and the floating static route is again placed in reserve.

To avoid the possibility of a routing loop occurring, by default floating static routes are not redistributed into other dynamic protocols.

Examples

The following example creates a static route to the remote router whose address is 1.2 on the remote network 200 that is in the remote zone *Remote*:

```
appletalk static network 200 to 1.2 zone Remote
```

The following example creates a floating static route to the remote router whose address is 1.3 on the remote network 200 that is in the remote zone *Remote*:

```
appletalk static network 200 to 1.3 floating zone Remote
```

Related Commands

Command	Description
appletalk static cable-range	Defines a static route or a floating static route on an extended network.
show appletalk route	Displays all entries or specified entries in the AppleTalk routing table.
show appletalk static	Displays information about the statically defined routes.

appletalk strict-rtmp-checking

To perform maximum checking of routing updates to ensure their validity, use the **appletalk strict-rtmp-checking** command in global configuration mode. To disable the maximum checking, use the **no** form of this command.

appletalk strict-rtmp-checking

no appletalk strict-rtmp-checking

Syntax Description   This command has no arguments or keywords.

Defaults   Maximum checking is provided.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Strict Routing Table Maintenance Protocol (RTMP) checking discards any RTMP packets arriving from routers that are not directly connected to the local router. This means that the local router does not accept any routed RTMP packets. Note that RTMP packets that need to be forwarded are not discarded.

Examples   The following example disables strict checking of RTMP routing updates:

```
no appletalk strict-rtmp-checking
```

Related Commands

Command	Description
appletalk require-route-zones	Prevents the advertisement of routes (network numbers or cable ranges) that have no assigned zone.
appletalk send-rtmps	Allows the Cisco IOS software to send routing updates to its neighbors.
appletalk timers	Changes the routing update timers.

appletalk timers

To change the routing update timers, use the **appletalk timers** command in global configuration mode. To return to the default routing update timers, use the **no** form of this command.

appletalk timers *update-interval valid-interval invalid-interval*

no appletalk timers [*update-interval valid-interval invalid-interval*]

Syntax Description		
update-interval	Time, in seconds, between routing updates sent to other routers on the network. The default is 10 seconds.
valid-interval	Time, in seconds, that the Cisco IOS software will consider a route valid without having heard a routing update for that route. The default is 20 seconds (two times the update interval).
invalid-interval	Time, in seconds, that the route is retained after the last update. The default is 60 seconds (three times the valid interval).

Defaults

update-interval argument: 10 seconds
valid-interval argument: 20 seconds
invalid-interval argument: 60 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Routes older than the time specified by the *update-interval* argument are considered suspect. Once the period of time specified by the *valid-interval* argument has elapsed without having heard a routing update for a route, the route becomes bad and is eligible for replacement by a path with a higher (less favorable) metric. During the period for the *invalid-interval* argument, routing updates include this route with a special "notify neighbor" metric. If this timer expires, the route is deleted from the routing table.

Note that you should not attempt to modify the routing timers without fully understanding the ramifications of doing so. Many other AppleTalk router vendors provide no facility for modifying their routing timers; should you adjust the Cisco IOS software AppleTalk timers such that routing updates do not arrive at these other routers within the normal interval, it is possible to degrade or destroy AppleTalk network connectivity.

If you change the routing update interval, be sure to do so for *all* routers on the network.

In rare instances, you might want to change this interval, such as when a device is busy and cannot send routing updates every 10 seconds or when slower routers are incapable of processing received routing updates in a large network.

Examples

The following example increases the update interval to 20 seconds and the route-valid interval to 40 seconds:

```
appletalk timers 20 40 60
```

appletalk virtual-net

To add AppleTalk users who are logging in on an asynchronous line and using PPP encapsulation to an internal network, use the **appletalk virtual-net** command in global configuration mode. To remove an internal network, use the **no** form of this command.

appletalk virtual-net *network-number zone-name*

no appletalk virtual-net *network-number zone-name*

Syntax Description

network-number	AppleTalk network address assigned to the interface. This is a 16-bit decimal network number in the range 0 to 65279. The network address must be unique across your AppleTalk internetwork.
zone-name	Name of a new or existing zone to which the AppleTalk user will belong.

Defaults

No virtual networks are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A virtual network is a logical network that exists only within the Cisco IOS software. It enables you—and by extension anyone who dials into the router—to add an asynchronous interface to either a new or an existing AppleTalk zone.

Virtual networks work with both extended and nonextended AppleTalk networks. On Cisco routers, you can only set a virtual network on an asynchronous line on the auxiliary port.

If you issue the **appletalk virtual-net** command and specify a new AppleTalk zone name, the network number you specify is the only one associated with this zone. If you issue this command and specify an existing AppleTalk zone, the network number you specify is added to the existing zone.

The selected AppleTalk zone (either new or existing) is highlighted when you open the Macintosh Chooser window. From this window, you can access all available zones.

Examples

The following example adds a user to the virtual network number 3 and specifies the zone name renegade:

```
apple virtual-net 3 renegade
```

Related Commands	Command	Description
	appletalk address	Enables nonextended AppleTalk routing on an interface.
	appletalk cable-range	Enables an extended AppleTalk network.
	appletalk client-mode	Allows users to access an AppleTalk zone when dialing into an asynchronous line (on Cisco routers, only via the auxiliary port).
	appletalk zone	Sets the zone name for the connected AppleTalk network.
	show appletalk zone	Displays all entries or specified entries in the zone information table.

appletalk zip-query-interval

To specify the interval at which the Cisco IOS software sends ZIP queries, use the **appletalk zip-query-interval** command in global configuration mode. To return to the default interval, use the **no** form of this command.

appletalk zip-query-interval *interval*

no zip-query-interval

Syntax Description

interval	Interval, in seconds, at which the software sends ZIP queries. It can be any positive integer. The default is 10 seconds.

Defaults

10 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The software uses the information received in response to its ZIP queries to update its zone table.

Examples

The following example changes the ZIP query interval to 40 seconds:

```
appletalk zip-query-interval 40
```

appletalk zip-reply-filter

To configure a ZIP reply filter, use the **appletalk zip-reply-filter** command in interface configuration mode. To remove a filter, use the **no** form of this command.

> **appletalk zip-reply-filter** *access-list-number*

> **no appletalk zip-reply-filter** [*access-list-number*]

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 600 to 699.

Defaults

No access lists are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

ZIP reply filters limit the visibility of zones from routers in unprivileged regions throughout the internetwork. These filters filter the zone list for each network provided by a router to neighboring routers to remove restricted zones.

ZIP reply filters apply to downstream routers, not to end stations on networks attached to the local router. With ZIP reply filters, when downstream routers request the names of zones in a network, the local router replies with the names of visible zones only. It does not reply with the names of zones that have been hidden with a ZIP reply filter. To filter zones from end stations, use GZL filters.

ZIP reply filters determine which networks and cable ranges the Cisco IOS software sends out in routing updates. Before sending out routing updates, the software excludes the networks and cable ranges whose zones have been completely denied access by ZIP reply filters. Excluding this information ensures that routers receiving these routing updates do not send unnecessary ZIP requests.

Examples

The following example assigns a ZIP reply filter to Ethernet interface 0:

```
interface ethernet 0
 appletalk zip-reply-filter 600
```

Related Commands	Command	Description
	access-list additional-zones	Defines the default action to take for access checks that apply to zones.
	access-list zone	Defines an AppleTalk access list that applies to a zone.
	show appletalk interface	Displays the status of the AppleTalk interfaces configured in the Cisco IOS software and the parameters configured on each interface.

appletalk zone

To set the zone name for the connected AppleTalk network, use the **appletalk zone** command in interface configuration mode. To delete a zone, use the **no** form of this command.

appletalk zone *zone-name*

no appletalk zone [*zone-name*]

Syntax Description

zone-name	Name of the zone. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

Defaults

No zone name is set.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If discovery mode is not enabled, you can specify the **appletalk zone** command only after an **appletalk address** or **appletalk cable-range** command. You can issue it multiple times if it follows the **appletalk cable-range** command.

On interfaces that have discovery mode disabled, you must assign a zone name in order for AppleTalk routing to begin.

If an interface is using extended AppleTalk, the first zone specified in the list is the default zone. The Cisco IOS software always uses the default zone when registering NBP names for interfaces. Nodes in the network will select the zone in which they will operate from the list of zone names valid on the cable to which they are connected.

If an interface is using nonextended AppleTalk, repeated execution of the **appletalk zone** command will replace the interface's zone name with the newly specified zone name.

The **no** form of the command deletes a zone name from a zone list or deletes the entire zone list if you do not specify a zone name. For nonextended AppleTalk interfaces, the zone name argument is ignored. You should delete any existing zone-name list using the **no appletalk zone** interface subcommand before configuring a new zone list.

The zone list is cleared automatically when you issue an **appletalk address** or **appletalk cable-range** command. The list also is cleared if you issue the **appletalk zone** command on an *existing* network; this can occur when adding zones to a set of routers until all routers are in agreement.

Examples

The following example assigns the zone name Twilight to an interface:

```
interface Ethernet 0
 appletalk cable-range 10-20
 appletalk zone Twilight
```

The following example uses AppleTalk special characters to set the zone name to *Cisco*:*A5Zone*:

```
appletalk zone Cisco:A5Zone
```

Related Commands

Command	Description
appletalk address	Enables nonextended AppleTalk routing on an interface.
appletalk cable-range	Enables an extended AppleTalk network.
show appletalk zone	Displays all entries or specified entries in the zone information table.

clear appletalk arp

To delete all entries or a specified entry from the AppleTalk Address Resolution Protocol (AARP) table, use the **clear appletalk arp** command in EXEC mode.

clear appletalk arp [*network*.*node*]

Syntax Description	*network*.*node*	(Optional) AppleTalk network address to be deleted from the AARP table. The argument *network* is the 16-bit network number in the range 0 to 65,279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example deletes all entries from the AARP table:

```
clear appletalk arp
```

Related Commands

Command	Description
show appletalk arp	Displays the entries in the ARP cache.

clear appletalk neighbor

To delete all entries or a specified entry from the neighbor table, use the **clear appletalk neighbor** command in EXEC mode.

clear appletalk neighbor [*neighbor-address*]

Syntax Description	*neighbor-address*	(Optional) Network address of the neighboring router to be deleted from the neighbor table. The address is in the format *network.node*. The argument *network* is the 16-bit network number in the range 1 to 65,279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines You cannot clear the entry for an active neighbor, that is, for a neighbor that still has RTMP connectivity.

Examples The following example deletes the neighboring router 1.129 from the neighbor table:

```
clear appletalk neighbor 1.129
```

Related Commands	Command	Description
	show appletalk neighbors	Displays information about the AppleTalk routers that are directly connected to any of the networks to which this router is directly connected.

clear appletalk route

To delete entries from the routing table, use the **clear appletalk route** command in EXEC mode.

clear appletalk route [*network*]

Syntax Description	*network*	(Optional) Number of the network to which the route provides access.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples   The following example deletes the route to network 1:

```
clear appletalk route 1
```

Related Commands

Command	Description
show appletalk route	Displays all entries or specified entries in the AppleTalk routing table.

clear appletalk traffic

To reset AppleTalk traffic counters, use the **clear appletalk traffic** command in EXEC mode.

clear appletalk traffic

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following is sample output after a **clear appletalk traffic** command was executed:

```
Router# clear appletalk traffic
Router# show appletalk traffic

AppleTalk statistics:
  Rcvd:  0 total, 0 checksum errors, 0 bad hop count
         0 local destination, 0 access denied
         0 for MacIP, 0 bad MacIP, 0 no client
         0 port disabled, 0 no listener
         0 ignored, 0 martians
  Bcast: 0 received, 0 sent
  Sent:  0 generated, 0 forwarded, 0 fast forwarded, 0 loopback
         0 forwarded from MacIP, 0 MacIP failures
         0 encapsulation failed, 0 no route, 0 no source
  DDP:   0 long, 0 short, 0 macip, 0 bad size
  NBP:   0 received, 0 invalid, 0 proxies
         0 replies sent, 0 forwards, 0 lookups, 0 failures
  RTMP:  0 received, 0 requests, 0 invalid, 0 ignored
         0 sent, 0 replies
  ATP:   0 received
  ZIP:   0 received, 0 sent, 0 netinfo
  Echo:  0 received, 0 discarded, 0 illegal
         0 generated, 0 replies sent
  Responder:  0 received, 0 illegal, 0 unknown
AppleTalk statistics:
         0 replies sent, 0 failures
  AARP:  0 requests, 0 replies, 0 probes
         0 martians, 0 bad encapsulation, 0 unknown
         0 sent, 0 failures, 0 delays, 0 drops
  Lost: 0 no buffers
  Unknown: 0 packets
  Discarded: 0 wrong encapsulation, 0 bad SNAP discriminator
```

For explanation of the fields shown in the preceding example, see the **show appletalk traffic** command later in this chapter.

	Command	Description
Related Commands	show appletalk macip-traffic	Displays statistics about MacIP traffic through the router.
	show appletalk traffic	Displays statistics about AppleTalk traffic.

clear smrp mcache

To remove all fast-switching entries in the Sample Multicast Routing Protocol (SMRP) fast-switching cache table, use the **clear smrp mcache** command in EXEC mode.

clear smrp mcache

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Use this command to clear the SMRP fast-switching cache table. The SMRP fast-switching cache table contains the information needed to fast switch SMRP data packets. It is usually unnecessary to clear the table; however, you can do so to repopulate it or to clear a corrupted entry.

Note   Using this command clears the table of all entries, not just a single entry.

Examples   The following example shows the fast-switching cache table before and after the **clear smrp mcache** command clears the table of entries:

```
Router# show smrp mcache


SMRP Multicast Fast Switching Cache
Group       In  Parent        Child         MAC Header (Top)
Address     Use Interface     Interface(s)  Network Header (Bottom)
-----------------------------------------------------------------

AT 11.121   Y   Ethernet0     Ethernet3     090007400b7900000c1740db
                                            001fed750000002aff020a0a0a
AT 11.122   Y   Ethernet0     Ethernet3     090007400b7a00000c1740db
                                            001f47750000002aff020a0a0a
AT 11.123   Y   Ethernet0     Ethernet1     090007400b7b00000c1740d9
                                            001fe77500000014ff020a0a0a
                              Ethernet3     090007400b7b00000c1740db
                                            001ffd750000002aff020a0a0a
AT 11.124   N   Ethernet0     Ethernet1     090007400b7c00000c1740d9
                                            001fef7500000014ff020a0a0a
```

```
Router# clear smrp mcache
Router# show smrp mcache

SMRP Multicast Fast Switching Cache
Group       In  Parent       Child        MAC Header (Top)
Address     Use Interface    Interface(s) Network Header (Bottom)
-----------------------------------------------------------------
```

Related Commands	Command	Description
	show smrp mcache	Displays the SMRP fast-switching cache table.

show appletalk access-lists

To display the AppleTalk access lists currently defined, use the **show appletalk access-lists** command in EXEC mode.

show appletalk access-lists

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following is sample output from the **show appletalk access-lists** command:

```
Router> show appletalk access-lists

AppleTalk access list 601:
        permit zone ZoneA
        permit zone ZoneB
        deny additional-zones
        permit network 55
        permit network 500
        permit cable-range 900-950
        deny includes 970-990
        permit within 991-995
        deny other-access
```

Table 9 describes fields shown in the display.

Table 9　　　*show appletalk access-lists Field Descriptions*

Field	Description
AppleTalk access list 601:	Number of the AppleTalk access lists.
permit zone deny zone	Indicates whether access to an AppleTalk zone has been explicitly permitted or denied with the **access-list zone** command.
permit additional-zones deny additional-zones	Indicates whether additional zones have been permitted or denied with the **access-list additional-zones** command.
permit network deny network	Indicates whether access to an AppleTalk network has been explicitly permitted or denied with the **access-list network** command.

Table 9   show appletalk access-lists Field Descriptions (continued)

Field	Description
permit cable-range deny cable-range	Indicates the cable ranges to which access has been permitted or denied with the **access-list cable-range** command.
permit includes deny includes	Indicates the cable ranges to which access has been permitted or denied with the **access-list includes** command.
permit within deny within	Indicates the additional cable ranges to which access has been permitted or denied with the **access-list within** command.
permit other-access deny other-access	Indicates whether additional networks or cable ranges have been permitted or denied with the **access-list other-access** command.

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list nbp	Defines an AppleTalk access list entry for a particular NBP named entity, class of NBP named entities, NBP packet type, or NBP named entities belonging to a specific zone.
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list other-nbps	Defines the default action to take for access checks that apply to NBP packets from named entities not otherwise explicitly denied or permitted.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
access-list zone	Defines an AppleTalk access list that applies to a zone.
appletalk access-group	Assigns an access list to an interface.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk getzonelist-filter	Filters GZL replies.

show appletalk adjacent-routes

To display routes to networks that are directly connected or that are one hop away, use the **show appletalk adjacent-routes** command in privileged EXEC mode.

show appletalk adjacent-routes

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The E - EIGRP field was removed from command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **show appletalk adjacent-routes** command provides a quick overview of the local environment that is especially useful when an AppleTalk internetwork consists of a large number of networks (typically, more then 600 networks).

You can use information provided by this command to determine if any local routes are missing or are misconfigured.

Examples   The following is sample output from the **show appletalk adjacent-routes** command:

```
Router# show appletalk adjacent-routes

Codes: R - RTMP derived, C - connected, S - static, P - proxy, 67 routes in internet

R Net 29-29 [1/G] via gatekeeper, 0 sec, Ethernet0, zone Engineering
C Net 2501-2501 directly connected, Ethernet1, no zone set
C Net 4160-4160 directly connected, Ethernet0, zone Low End SW Lab
C Net 4172-4172 directly connected, TokenRing0, zone Low End SW Lab
R Net 6160 [1/G] via urk, 0 sec, TokenRing0, zone Low End SW Lab
```

Table 10 describes the fields shown in the display.

Table 10   show appletalk adjacent-routes Field Descriptions

Field	Description
Codes:	Codes defining source of route.
R - RTMP derived	Route derived from an RTMP update.

Table 10   *show appletalk adjacent-routes Field Descriptions (continued)*

Field	Description
C - Connected	Directly connected network RTMP update.
S - Static	Static route.
P - Proxy	Proxy route.
67 routes in internet	Total number of known routes in the AppleTalk network.
Net 29-29	Cable range or network to which the route goes.
[1/G]	Hop count, followed by the state of the route. Possible values for state include the following: • G—Good (update has been received within the last 10 seconds) • S—Suspect (update has been received more than 10 seconds ago but less than 20 seconds ago) • B—Bad (update was received more than 20 seconds ago)
via	NBP registered name or address of the router that sent the routing information.
0 sec	Time, in seconds, since information about this network cable range was last received.
directly connected	Indicates that the network or cable range is directly connected to the router.
Ethernet0	Possible interface through which updates to this NBP registered name or address will be sent.
zone	Zone name assigned to the network or cable range sending this update.

show appletalk arp

To display the entries in the Address Resolution Protocol (ARP) cache, use the **show appletalk arp** command in privileged EXEC mode.

show appletalk arp

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   ARP establishes associates between network addresses and hardware (MAC) addresses. This information is maintained in the ARP cache.

Examples   The following is sample output from the **show appletalk arp** command:

```
Router# show appletalk arp

Address      Age (min)  Type      Hardware Addr   Encap     Interface
2000.1              -  Hardware  0000.0c04.1111  SNAP      Ethernet1
2000.2              0  Dynamic   0000.0c04.2222  SNAP      Ethernet1
2000.3              0  Dynamic   0000.0c04.3333  SNAP      Ethernet3
2000.4              -  Hardware  0000.0c04.4444  SNAP      Ethernet3
```

Table 11 describes the fields shown in the display.

Table 11   show appletalk arp Field Descriptions

Field	Description
Address	AppleTalk network address of the interface.
Age (min)	Time, in minutes, that this entry has been in the ARP table. Entries are purged after they have been in the table for 240 minutes (4 hours). A hyphen indicates that this is a new entry.

Table 11   show appletalk arp Field Descriptions (continued)

Field	Description
Type	Indicates how the ARP table entry was learned. It can be one of the following: • Dynamic—Entry was learned via AARP. • Hardware—Entry was learned from an adapter in the router. • Pending—Entry for a destination for which the router does not yet know the address. When a packet requests to be sent to an address for which the router does not yet have the MAC-level address, the Cisco IOS software creates an AARP entry for that AppleTalk address, then sends an AARP Resolve packet to get the MAC-level address for that node. When the software gets the response, the entry is marked "Dynamic." A pending AARP entry times out after 1 minute.
Hardware Addr	MAC address of this interface.
Encap	Encapsulation type. It can be one of the following: • ARPA—Ethernet-type encapsulation • Subnetwork Access Protocol (SNAP)—IEEE 802.3 encapsulation
Interface	Type and number of the interface.

show appletalk aurp events

To display the pending events in the AppleTalk Update-Based Routing Protocol (AURP) update-events queue, use the **show appletalk aurp events** command in privileged EXEC mode.

show appletalk aurp events

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples   The following is sample output from the **show appletalk aurp events** command:

```
Router# show appletalk aurp events

100-100, NDC EVENT pending
17043-17043, ND EVENT pending
```

Table 12 explains the fields shown in the display.

Table 12   show appletalk aurp events Field Descriptions

Field	Description
100-100	Network number or cable range.
NCD EVENT pending	Type of update event that is pending.

show appletalk aurp topology

To display entries in the AppleTalk Update-Based Routing Protocol (AURP) private path database, which consists of all paths learned from exterior routers, use the **show appletalk aurp topology** command in privileged EXEC mode.

show appletalk aurp topology

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples   The following is sample output from the **show appletalk aurp topology** command:

```
Router# show appletalk aurp topology

30
            via Tunnel0, 3 hops
80
            via Tunnel0, 3 hops
101-101
            via Tunnel0, 8 hops
102-102
            via Tunnel0, 8 hops
103-103
            via Tunnel0, 8 hops
104-104
            via Tunnel0, 8 hops
105-105
            via Tunnel0, 8 hops
108-108
            via Tunnel0, 8 hops
109-109
            via Tunnel0, 9 hops
120-120
            via Tunnel0, 10 hops
125-125
            via Tunnel0, 8 hops
169-169
            via Tunnel0, 7 hops
201-205
            via Tunnel0, 4 hops
```

Table 13 describes the fields shown in the display.

Table 13   *show appletalk aurp topology Field Descriptions*

Field	Description
30	AppleTalk network number or cable range.
via Tunnel0	Interface used to reach the network.
3 hops	Number of hops to the network.

show appletalk cache

To display the routes in the AppleTalk fast-switching table on an extended AppleTalk network, use the **show appletalk cache** command in EXEC mode.

> **show appletalk cache**

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **show appletalk cache** command displays information for all fast-switching route cache entries, regardless of whether they are valid.

Route entries are removed from the fast-switching cache if one of the following occurs:

- A route that was used has been deleted but has not yet been marked bad.
- A route that was used has gone bad.
- A route that was used has been replaced with a new route with a better metric.
- The state of route to a neighbor has changed from suspect to bad.
- The hardware address corresponding to a node address in the AARP cache has changed.
- The node address corresponding to a hardware address has changed.
- The ARP cache has been flushed.
- An ARP cache entry has been deleted.
- You have entered the **no appletalk routing** command, the **appletalk route-cache** command, or an **access-list** command.
- The encapsulation on the line has changed.
- An interface has become operational or nonoperational.

Examples   The following is sample output from the **show appletalk cache** command:

```
Router> show appletalk cache

AppleTalk Routing Cache, * = active entry, cache version is 227
Destination    Interface    MAC Header
```

```
*      29.0     Ethernet0     00000C00008200000C00D8DD
*   1544.000    Ethernet1     AA000400013400000C000E8C809B84BE02
*     33.000    Ethernet1     AA000400013400000C000E8C809B84BE02
```

The following is sample output from the **show appletalk cache** command when AppleTalk load balanced is enabled. The output displayed shows additional MAC headers for parallel paths (for example, 6099.52):

```
Router> show appletalk cache

Appletalk Routing cache, * = active entry, cache version is 11021
Destination    Interface     MAC Header
*     82.36     Ethernet1/4   00000CF366A600000C12C52D
   17043.208    Ethernet1/5   00000C367B4000000C12C52E
*  60099.52     Ethernet1/5   00000C367B4000000C12C52E
                Ethernet1/2   00000C367B3D00000C12C52B
                Ethernet1/3   00000C367B3E00000C12C52C
```

Table 14 describes the fields shown in the display.

Table 14   show appletalk cache Field Descriptions

Field	Description
*	Indicates the entry is valid.
cache version is	Version number of the AppleTalk fast-switching cache.
Destination	Destination network for this packet.
Interface	Router interface through which this packet is transmitted.
MAC Header	First bytes of this packet's MAC header.

Related Commands

Command	Description
appletalk maximum-paths	Defines the maximum number of equal-cost paths the router should use when balancing the traffic load.
appletalk route-cache	Enables fast switching on all supported interfaces.

show appletalk domain

To display all domain-related information, use the **show appletalk domain** command in EXEC mode.

show appletalk domain [*domain-number*]

Syntax Description

domain-number	(Optional) Number of an AppleTalk domain about which to display information. It can be a decimal integer from 1 to 1,000,000.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you omit the argument *domain-number*, the **show appletalk domain** command displays information about all domains.

Examples

The following is sample output from the **show appletalk domain** command:

```
Router# show appletalk domain

    AppleTalk   Domain   Information:

    Domain 1        Name : Xerxes
--------------------------------------
    State             : Active
    Inbound remap range  : 100-199
    Outbound remap range : 200-299
    Hop reduction      : OFF
    Interfaces in domain :
          Ethernet1    : Enabled

    Domain 2        Name : Desdemona
------------------------------------
    State             : Active
    Inbound remap range  : 300-399
    Outbound remap range : 400-499
    Hop reduction      : OFF
    Interfaces in domain :
          Ethernet3    : Enabled
```

The following is sample output from the **show appletalk domain** command when you specify a domain number:

```
Router# show appletalk domain 1

      AppleTalk   Domain   Information:

      Domain 1        Name : Xerxes
      -------------------------------------
      State             : Active
      Inbound remap range  : 100-199
      Outbound remap range : 200-299
      Hop reduction     : OFF
      Interfaces in domain :
            Ethernet1     : Enabled
```

Table 15 describes the fields shown in the displays.

Table 15   show appletalk domain Field Descriptions

Field	Description
Domain	Number of the domain as specified with the **appletalk domain name** global configuration command.
Name	Name of the domain as specified with the **appletalk domain name** global configuration command.
State	Status of the domain. It can be either Active or Nonactive.
Inbound remap range	Inbound mapping range as specified with the **appletalk domain remap-range in** global configuration command.
Outbound remap range	Outbound mapping range as specified with the **appletalk domain remap-range out** global configuration command.
Hop reduction	Indicates whether hop reduction has been enabled with the **appletalk domain hop-reduction** global configuration command. It can be either OFF or ON.
Interfaces in domain	Indicates which interfaces are in the domain as specified with the **appletalk domain-group** interface configuration command and whether they are enabled.

Related Commands

Command	Description
appletalk domain-group	Assigns a predefined domain number to an interface.
appletalk domain hop-reduction	Reduces the hop-count value in packets traveling between segments of a domain.
appletalk domain name	Creates a domain and assigns it a name and number.
appletalk domain remap-range	Remaps ranges of AppleTalk network numbers or cable ranges between two segments of a domain.

show appletalk eigrp interfaces

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show appletalk eigrp interfaces** command in EXEC mode.

show appletalk eigrp interfaces [*type number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.

Command Modes   EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Use the **show appletalk 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.

Examples   The following is sample output from the **show appletalk eigrp interfaces** command:

```
Router> show appletalk eigrp interfaces

AT/EIGRP interfaces for process 1, router id 24096

                   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 16 describes the fields shown in the display.

Table 16   show appletalk eigrp interfaces Field Descriptions

Field	Description
process 1	Autonomous system number of the process.
router id	Identification number of the router, as configured in the **appletalk routing eigrp** command.
Interface	Interface name.
Peers	Number of neighbors on the interface.
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 appletalk eigrp neighbors	Displays the neighbors discovered by Enhanced IGRP.

show appletalk eigrp neighbors

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show appletalk eigrp neighbors** command in EXEC mode.

show appletalk eigrp neighbors [*interface*]

Syntax Description

interface	(Optional) Displays information about the specified neighbor router.

Command Modes   EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **show appletalk eigrp neighbors** command lists only the neighbors running AppleTalk Enhanced IGRP. To list all neighboring AppleTalk routers, use the **show appletalk neighbors** command.

Examples   The following is sample output from the **show appletalk eigrp neighbors** command:

```
Router# show appletalk eigrp neighbors

AT/EIGRP Neighbors for process 1, router id 83
Address              Interface    Holdtime Uptime  Q     Seq SRTT RTO
                                  (secs)   (h:m:s) Count Num (ms) (ms)
warp.Ethernet1       Ethernet2    41       0:02:48 0     282 4    20
master.Ethernet2     Ethernet2    40       1:16:46 0     333 4    20
```

Table 17 describes the fields shown in the display.

Table 17   show appletalk eigrp neighbors Field Descriptions

Field	Description
process 1	Number of the Enhanced IGRP routing process.
router id 83	Autonomous system number specified in the **appletalk routing** global configuration command.
Address	AppleTalk address of the AppleTalk Enhanced IGRP peer.

Table 17   *show appletalk eigrp neighbors Field Descriptions (continued)*

Field	Description
Interface	Interface on which the router is receiving hello packets from the peer.
Holdtime	Length of time, in seconds, that the 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 Count	Number of AppleTalk Enhanced IGRP packets (update, query, and reply) that the 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 AppleTalk 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 the Cisco IOS software waits before retransmitting a packet from the retransmission queue to a neighbor.

Related Commands

Command	Description
appletalk routing	Enables AppleTalk routing.
show appletalk neighbors	Displays information about the AppleTalk routers that are directly connected to any of the networks to which this router is directly connected.

show appletalk eigrp topology

To display the AppleTalk Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show appletalk eigrp topology** command in EXEC mode.

show appletalk eigrp topology [*network-number* | **active** | **zero-successors**]

Syntax Description

network-number	(Optional) Number of the AppleTalk network whose topology table entry you want to display.
active	(Optional) Displays the entries for all active routes.
zero-successors	(Optional) Displays the entries for destinations for which no successors exist. These entries are destinations that the Cisco IOS software currently does not know how to reach via Enhanced IGRP. This option is useful for debugging network problems.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All Enhanced IGRP routes that are received for a destination, regardless of metric, are placed in the topology table. The route to a destination that is currently in use is the first route listed. Routes that are listed as "connected" take precedence over any routes learned from any other source.

Examples

The following is sample output from the **show appletalk eigrp topology** command:

```
Router# show appletalk eigrp topology

IPX EIGRP Topology Table for process 1, router id 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 3165-0, 1 successors, FD is 0
        via Redistributed (25601/0),
        via 100.1 (2198016/2195456), Fddi0
        via 4080.67 (2198016/53760), Serial4
P 3161-0, 1 successors, FD is 307200
        via Redistributed (1025850/0),
```

```
        via 100.1 (2198016/2195456), Fddi0
        via 4080.67 (2198016/1028410), Serial4
P 100-100, 1 successors, FD is 0
        via Connected, Fddi0
        via 4080.67 (2198016/28160), Serial4
P 4080-4080, 1 successors, FD is 0
        via Connected, Serial4
        via 100.1 (2172416/2169856), Fddi0
```

Table 18 describes the fields that may be displayed in the output.

Table 18   show appletalk 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; and 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 the Cisco IOS software has sent a query and is waiting for a reply.
3165, 3161, and so on	Destination AppleTalk network number.
successors	Number of successors. This number corresponds to the number of next hops in the AppleTalk 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 software 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 the 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	AppleTalk address of the peer who told the 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 to us.
Ethernet0	Interface from which this information was learned.

The following is sample output from the **show appletalk eigrp topology** command when you specify an AppleTalk network number:

```
Router# show appletalk eigrp topology 3165

AT-EIGRP topology entry for 3165-0
State is Passive, Query origin flag is 1, 1 Successor(s)
Routing Descriptor Blocks:
0.0, from 0.0
  Composite metric is (25601/0), Send flag is 0x0, Route is Internal
  Vector metric:
    Minimum bandwidth is 2560000000 Kbit
    Total delay is 1000000 nanoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 0
100.1 (Fddi0), from 100.1
  Composite metric is (2198016/2195456), Send flag is 0x0, Route is External
  Vector metric:
    Minimum bandwidth is 1544 Kbit
    Total delay is 21100000 nanoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 2
4080.83 (Serial4), from 4080.83
    Composite metric is (2198016/53760), Send flag is 0x0, Route is Internal
    Vector metric:
    Minimum bandwidth is 1544 Kbit
    Total delay is 21100000 nanoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 2
```

Table 19 describes the fields that may appear in the output.

Table 19   *show appletalk eigrp topology Field Descriptions—Specified Network*

Field	Description
3165	AppleTalk 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.
Successors	Number of successors. This number corresponds to the number of next hops in the IPX routing table.

Table 19 **show appletalk eigrp topology Field Descriptions—Specified Network (continued)**

Field	Description
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 RTMP or another routing protocol. • AppleTalk host address—The destination was learned from that peer via this Enhanced IGRP process.
Ethernet0	Interface from which this information was learned.
from	Peer from whom the information was learned. For connected and redistributed routers, this is 0.0. For information learned via Enhanced IGRP, this is the peer's address. Currently, for information learned via Enhanced IGRP, the peer's AppleTalk 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. 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 routes are those that did not. Routes learned via RTMP are always external.
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	Smallest Maximum Transmission Unit (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 AppleTalk 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 appletalk route** command for this destination. The delay is the external delay.
Administrator tag	Currently not used.
Flag	Currently not used.

Related Commands	Command	Description
	show appletalk route	Displays all entries or specified entries in the AppleTalk routing table.

show appletalk globals

To display information and settings about the AppleTalk internetwork and other parameters, use the **show appletalk globals** command in EXEC mode.

show appletalk globals

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples   The following is sample output from the **show appletalk globals** command:

```
Router# show appletalk globals

AppleTalk global information:
    The router is a domain router.
    Internet is compatible with older, AT Phase1, routers.
    There are 67 routes in the internet.
    There are 25 zones defined.
    All significant events will be logged.
    ZIP resends queries every 10 seconds.
    RTMP updates are sent every 10 seconds with a jitter.
    RTMP entries are considered BAD after 20 seconds.
    RTMP entries are discarded after 60 seconds.
    AARP probe retransmit count: 10, interval: 200.
    AARP request retransmit count: 5, interval: 1000.
    DDP datagrams will be checksummed.
    RTMP datagrams will be strictly checked.
    RTMP routes may not be propagated without zones.
    Alternate node address format will not be displayed.
```

Table 20 describes the fields shown in the display.

Table 20   show appletalk globals Field Descriptions

Field	Description
AppleTalk global information:	Heading for the command output.
The router is a domain router.	Indicates whether this router is a domain router.
Internet is compatible with older, AT Phase1, routers.	Indicates whether the AppleTalk internetwork meets the criteria for interoperation with Phase 1 routers.

Table 20 **show appletalk globals Field Descriptions (continued)**

Field	Description
There are 67 routes in the internet.	Total number of routes in the AppleTalk internetwork from which this router has heard in routing updates.
There are 25 zones defined.	Total number of valid zones in the current AppleTalk internetwork configuration.
All significant events will be logged.	Indicates whether the router has been configured with the **appletalk event-logging** command.
ZIP resends queries every 10 seconds.	Interval, in seconds, at which zone name queries are retried.
RTMP updates are sent every 10 seconds.	Interval, in seconds, at which the Cisco IOS software sends routing updates.
RTMP entries are considered BAD after 20 seconds.	Time after which routes for which the software has not received an update will be marked as candidates for being deleted from the routing table.
RTMP entries are discarded after 60 seconds.	Time after which routes for which the software has not received an update will be deleted from the routing table.
AARP probe retransmit count: 10, interval: 200.	Number of AARP probe retransmissions that will be done before abandoning address negotiations and instead using the selected AppleTalk address, followed by the time, in milliseconds, between retransmission of ARP probe packets. You set these values with the **appletalk arp retransmit-count** and **appletalk arp interval** commands, respectively.
AARP request retransmit count: 5, interval: 1000.	Number of AARP request retransmissions that will be done before abandoning address negotiations and using the selected AppleTalk address, followed by the time, in milliseconds, between retransmission of ARP request packets. You set these values with the **appletalk arp retransmit-count** and **appletalk arp interval** commands, respectively.
DDP datagrams will be checksummed.	Indicates whether the **appletalk checksum** configuration command is enabled. When enabled, the software discards DDP packets when the checksum is incorrect and when the router is the final destination for the packet.
RTMP datagrams will be strictly checked.	Indicates whether the **appletalk strict-rtmp-checking** configuration command is enabled. When enabled, RTMP packets arriving from routers that are not directly connected to the router performing the check are discarded.

Table 20   show appletalk globals Field Descriptions (continued)

Field	Description
RTMP routes may not be propagated without zones.	Indicates whether the **appletalk require-route-zones** configuration command is enabled. When enabled, the Cisco IOS software does not advertise a route to its neighboring routers until it has obtained a network/zone association for that route.
Alternate node address format will not be displayed.	Indicates whether AppleTalk addresses will be printed in numeric or name form. You configure this with the **appletalk lookup-type** and **appletalk name-lookup-interval** commands.

Related Commands

Command	Description
appletalk arp interval	Specifies the time interval between retransmissions of ARP packets.
appletalk arp retransmit-count	Specifies the number of ARP probe or request transmissions.
appletalk checksum	Enables the generation and verification of checksums for all AppleTalk packets (except routed packets).
appletalk event-logging	Logs significant network events.
appletalk lookup-type	Specifies which NBP service types are retained in the name cache.
appletalk name-lookup-interval	Sets the interval between service pollings by the router on its AppleTalk interfaces.
appletalk require-route-zones	Prevents the advertisement of routes (network numbers or cable ranges) that have no assigned zone.
appletalk strict-rtmp-checking	Performs maximum checking of routing updates to ensure their validity.

show appletalk interface

To display the status of the AppleTalk interfaces configured in the Cisco IOS software and the parameters configured on each interface, use the **show appletalk interface** command in privileged EXEC mode.

> **show appletalk interface** [**brief**] [*type number*]

Syntax Description

brief	(Optional) Displays a brief summary of the status of the AppleTalk interfaces.
type	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), FDDI, High-Speed Serial Interface (HSSI), Virtual Interface, ISDN Basic Rate Interface (BRI), ATM interface, loopback, null, or serial.
number	(Optional) Interface number.

Command Modes   Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **show appletalk interface** is particularly useful when you first enable AppleTalk on a router interface.

Examples   The following is sample output from the **show appletalk interface** command for an extended AppleTalk network:

```
Router# show appletalk interface fddi 0

Fddi0 is up, line protocol is up
    AppleTalk cable range is 4199-4199
    AppleTalk address is 4199.82, Valid
    AppleTalk zone is "Low End SW Lab"
    AppleTalk address gleaning is disabled
    AppleTalk route cache is enabled
    Interface will not perform pre-FDDITalk compatibility
```

Table 21 describes the fields shown in the display as well as some fields not shown but that also may be displayed. Note that this command can show a node name in addition to the address, depending on how the software has been configured with the **appletalk lookup-type** and **appletalk name-lookup-interval** commands.

Table 21   show appletalk interface Field Descriptions—Extended Network

Field	Description
FDDI is ...	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
line protocol	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether *keepalives* are successful).
AppleTalk node	Indicates whether the node is up or down in the network.
AppleTalk cable range	Cable range of the interface.
AppleTalk address is ..., Valid	Address of the interface, and whether the address conflicts with any other address on the network ("Valid" means it does not).
AppleTalk zone	Name of the zone that this interface is in.
AppleTalk port configuration verified ...	When our access server implementation comes up on an interface, if there are other routers detected and the interface we are bringing up is not in discovery mode, our access server "confirms" our configuration with the routers that are already on the cable. The address printed in this field is that of the router with which the local router has verified that the interface configuration matches that on the running network.
AppleTalk discarded...packets due to input errors	Number of packets the interface discarded because of input errors. These errors are usually incorrect encapsulations (that is, the packet has a malformed header format).
AppleTalk address gleaning	Indicates whether the interface is automatically deriving ARP table entries from incoming packets (referred to as *gleaning*).
AppleTalk route cache	Indicates whether fast switching is enabled on the interface.
Interface will ...	Indicates that the AppleTalk interface will check to see if AppleTalk packets sent on the FDDI ring from routers running Cisco software releases prior to Release 9.0(3) or 9.1(2) are recognized.
AppleTalk domain	AppleTalk domain of which this interface is a member.

The following is sample output from the **show appletalk interface** command for a nonextended AppleTalk network:

```
Router# show appletalk interface ethernet 1

Ethernet 1 is up, line protocol is up
    AppleTalk address is 666.128, Valid
    AppleTalk zone is Underworld
    AppleTalk routing protocols enabled are RTMP
    AppleTalk address gleaning is enabled
    AppleTalk route cache is not initialized
```

Table 22 describes the fields shown in the display.

Table 22   show appletalk interface Field Descriptions—Nonextended Network

Field	Description
Ethernet 1	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
line protocol	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether *keepalives* are successful).
AppleTalk address is ..., Valid	Address of the interface, and whether the address conflicts with any other address on the network ("Valid" means it does not).
AppleTalk zone	Name of the zone that this interface is in.
AppleTalk routing protocols enabled	AppleTalk routing protocols that are enabled on the interface.
AppleTalk address gleaning	Indicates whether the interface is automatically deriving ARP table entries from incoming packets (referred to as *gleaning*).
AppleTalk route cache	Indicates whether fast switching is enabled on the interface.

The following is sample output from the **show appletalk interface brief** command:

```
Router# show appletalk interface brief

Interface   Address     Config       Status/Line Protocol    Atalk Protocol
TokenRing0  108.36      Extended     up                      down
TokenRing1  unassigned  not config'd administratively down   n/a
Ethernet0   10.82       Extended     up                      up
Serial0     unassigned  not config'd administratively down   n/a
Ethernet1   30.83       Extended     up                      up
Serial1     unassigned  not config'd administratively down   n/a
Serial2     unassigned  not config'd administratively down   n/a
Serial3     unassigned  not config'd administratively down   n/a
Serial4     unassigned  not config'd administratively down   n/a
Serial5     unassigned  not config'd administratively down   n/a
Fddi0       50001.82    Extended     administratively down   down
Ethernet2   unassigned  not config'd up                      n/a
Ethernet3   9993.137    Extended     up                      up
Ethernet4   40.82       Non-Extended up                      up
Ethernet5   unassigned  not config'd administratively down   n/a
Ethernet6   unassigned  not config'd administratively down   n/a
Ethernet7   unassigned  not config'd administratively down   n/a
```

Table 23 describes the fields shown in the display.

Table 23   show appletalk interface brief Field Descriptions

Field	Description
Interface	Interface type and number.
Address	Address assigned to the interface.
Config	How the interface is configured. Possible values are extended, nonextended, and not configured.

Table 23   show appletalk interface brief Field Descriptions (continued)

Field	Description
Status/Line Protocol	Whether the software processes that handle the line protocol believe the interface is usable (that is, whether *keepalives* are successful).
Atalk Protocol	Whether AppleTalk routing is up and running on the interface.

The following sample output displays the **show appletalk interface** command when AppleTalk RTMP stub mode is enabled. The last line of the output notes that this mode is turned on.

```
Router# show appletalk interface ethernet 2

Ethernet2 is up, line protocol is up
  AppleTalk cable range is 30-30
  AppleTalk address is 30.1, Valid
  AppleTalk zone is "Zone30-30"
  AppleTalk address gleaning is disabled
  AppleTalk route cache is enabled
  AppleTalk RTMP stub mode is enabled
```

Related Commands

Command	Description
appletalk access-group	Assigns an access list to an interface.
appletalk address	Enables nonextended AppleTalk routing on an interface.
appletalk cable-range	Enables an extended AppleTalk network.
appletalk client-mode	Allows users to access an AppleTalk zone when dialing into an asynchronous line (on Cisco routers, only via the auxiliary port).
appletalk discovery	Places an interface into discovery mode.
appletalk distribute-list in	Filters routing updates received from other routers over a specified interface.
appletalk distribute-list out	Filters routing updates sent to other routers.
appletalk free-trade-zone	Establishes a free-trade zone.
appletalk getzonelist-filter	Filters GZL replies.
appletalk glean-packets	Derives ARP table entries from incoming packets.
appletalk pre-fdditalk	Enables the recognition of pre-FDDI Talk packets.
appletalk protocol	Specifies the routing protocol to use on an interface.
appletalk route-cache	Enables fast switching on all supported interfaces.
appletalk rtmp-stub	Enables AppleTalk RTMP stub mode.
appletalk send-rtmps	Allows the Cisco IOS software to send routing updates to its neighbors.
appletalk zip-reply-filter	Configures a ZIP reply filter.
appletalk zone	Sets the zone name for the connected AppleTalk network.

show appletalk macip-clients

To display status information about all known MacIP clients, use the **show appletalk macip-clients** command in EXEC mode.

show appletalk macip-clients

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show appletalk macip-clients** command:

```
Router# show appletalk macip-clients

172.31.199.1@[27001n,69a,72s] 45 secs    'S/W Test Lab'
```

Table 24 describes the fields shown in the display.

Table 24   show appletalk macip-clients Field Descriptions

Field	Description
172.31.199.1@	Client IP address.
[2700ln,69a,72s]	DDP address of the registered entity, showing the network number, node address, and socket number.
45 secs	Time (in seconds) since the last NBP confirmation was received.
'S/W Test Lab'	Name of the zone to which the MacIP client is attached.

Related Commands

Command	Description
show appletalk traffic	Displays statistics about AppleTalk traffic.

show appletalk macip-servers

To display status information about related servers, use the **show appletalk macip-servers** command in EXEC mode.

> **show appletalk macip-servers**

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The information in the **show appletalk macip-servers** display can help you quickly determine the status of your MacIP configuration. In particular, the STATE field can help identify problems in your AppleTalk environment.

Examples   The following is sample output from the **show appletalk macip-servers** command:

```
Router# show appletalk macip-servers

MACIP SERVER 1, IP 172.18.199.221,  ZONE 'S/W Test Lab' STATE is server_up
Resource #1 DYNAMIC 172.18.199.1-172.18.199.10, 1/10 IP in use
Resource #2 STATIC 172.18.199.11-172.18.199.20, 0/10 IP in use
```

Table 25 describes the fields shown in the display.

Table 25   show appletalk macip-servers Field Descriptions

Field	Description
MACIP SERVER 1	Number of the MacIP server. This number is assigned arbitrarily.
IP 172.18.199.221	IP address of the MacIP server.
ZONE 'S/W Test Lab'	AppleTalk server zone specified with the **appletalk macip server** command.

Table 25   show appletalk macip-servers Field Descriptions (continued)

Field	Description
STATE is server_up	State of the server. Table 27 lists the possible states. If the server remains in the "resource_wait" state, check that resources have been assigned to this server with either the **appletalk macip dynamic** or the **appletalk macip static** command.
Resource #1 DYNAMIC 172.18.199.1-172.18.199.10, 1/10 IP in use	Resource specifications defined in the **appletalk macip dynamic** and **appletalk macip static** commands. This list indicates whether the resource address was assigned dynamically or statically, identifies the IP address range associated with the resource specification, and indicates the number of active MacIP clients.

Use the **show appletalk macip-servers** command with **show appletalk interface** to identify AppleTalk network problems, as follows:

Step 1 Determine the state of the MacIP server using **show appletalk macip-servers**. If the STATE field continues to indicate an anomalous status (something other than "server_up," such as "resource_wait" or "zone_wait"), there is a problem.

Step 2 Determine the status of AppleTalk routing and the specific interface using the **show appletalk interface** command.

Step 3 If the protocol and interface are up, check the MacIP configuration commands for inconsistencies in the IP address and zone.

The STATE field of the **show appletalk macip-servers** command indicates the current state of each configured MacIP server. Each server operates according to the finite-state machine table described in Table 26. Table 27 describes the state functions listed in Table 26. These are the states that are displayed by the **show appletalk macip-servers** command.

Table 26   MacIP Finite-State Machine Table

State	Event	New State	Notes
initial	ADD_SERVER	resource_wait	Server configured
resource_wait	TIMEOUT	resource_wait	Wait for resources
resource_wait	ADD_RESOURCE	zone_wait	Wait for zone seeding
zone_wait	ZONE_SEEDED	server_start	Register server
zone_wait	TIMEOUT	zone_wait	Wait until seeded
server_start	START_OK	reg_wait	Wait for server register
server_start	START_FAIL	del_server	Could not start (possible configuration error)
reg_wait	REG_OK	server_up	Registration successful

Table 26   MacIP Finite-State Machine Table (continued)

State	Event	New State	Notes
reg_wait	REG_FAIL	del_server	Registration failed (possible duplicate IP address)
reg_wait	TIMEOUT	reg_wait	Wait until register
server_up	TIMEOUT	send_confirms	NBP confirm all clients
send_confirms	CONFIRM_OK	server_up	
send_confirms	ZONE_DOWN	zone_wait	Zone or IP interface down; restart
*	ADD_RESOURCE	*	Ignore, except resource_wait
*	DEL_SERVER	del_server	"No server" statement (HALT)
*	DEL_RESOURCE	ck_resource	Ignore
ck_resource	YES_RESOURCS	*	Return to previous state
ck_resource	NO_RESOURCES	resource_wait	Shut down and wait for resources

Table 27   Server States

State	Description
ck_resource	The server verifies that at least one client range is available. If not, it deregisters NBP names and returns to the resource_wait state.
del_server	State at which all servers end. In this state, the server deregisters all NBP names, purges all clients, and deallocates server resources.
initial	The state at which all servers start.
resource-wait	The server waits until a client range for the server has been configured.
send_confirms	The server tickles active clients every minute, deletes clients that have not responded within the last 5 minutes, and checks IP and AppleTalk interfaces used by MacIP server. If the interfaces are down or have been reconfigured, the server restarts.
server_start	The server registers configured IPADDRESS and registers as IPGATEWAY. It then opens an ATP socket to listen for IP address assignment requests, sends NBP lookup requests for existing IPADDRESSes, and automatically adds clients with addresses within one of the configured client ranges.
server_up	The server has registered. Being in this state enables routing to client ranges. The server now responds to IP address assignment requests.

Table 27   Server States (continued)

State	Description
zone_wait	The server waits until the configured AppleTalk zone name for the server is up. The server will remain in this state if no such zone has been configured or if AppleTalk routing is not enabled.
*	An asterisk in the first column represents any state. An asterisk in the second column represents a return to the previous state.

Related Commands

Command	Description
appletalk macip dynamic	Allocates IP addresses to dynamic MacIP clients.
appletalk macip server	Establishes a MacIP server for a zone.
appletalk macip static	Allocates an IP address to be used by a MacIP client that has reserved a static IP address.
show appletalk interface	Displays the status of the AppleTalk interfaces configured in the Cisco IOS software and the parameters configured on each interface.
show appletalk traffic	Displays statistics about AppleTalk traffic.

show appletalk macip-traffic

To display statistics about MacIP traffic through the router, use the **show appletalk macip-traffic** command in privileged EXEC mode.

show appletalk macip-traffic

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Use the **show appletalk macip-traffic** command to obtain a detailed breakdown of MacIP traffic that is sent through a router from an AppleTalk to an IP network. The output from this command differs from that of the **show appletalk traffic** command, which shows normal AppleTalk traffic generated, received, or routed by the router.

Examples   The following is sample output from the **show appletalk macip-traffic** command:

```
Router# show appletalk macip-traffic

 -- MACIP Statistics
               MACIP_DDP_IN:    11062
            MACIP_DDP_IP_OUT:    10984
 MACIP_DDP_NO_CLIENT_SERVICE:       78
                MACIP_IP_IN:     7619
           MACIP_IP_DDP_OUT:     7619
             MACIP_SERVER_IN:       62
            MACIP_SERVER_OUT:       52
        MACIP_SERVER_BAD_ATP:       10
     MACIP_SERVER_ASSIGN_IN:       26
    MACIP_SERVER_ASSIGN_OUT:       26
       MACIP_SERVER_INFO_IN:       26
      MACIP_SERVER_INFO_OUT:       26
```

Table 28 describes the fields shown in the display.

Table 28   show appletalk macip-traffic Field Descriptions

Field	Description
MACIP_DDP_IN	Number of DDP packets received.
MACIP_DDP_IP_OUT	Number of DDP packets received that were sent to the IP network.
MACIP_DDP_NO_CLIENT_ SERVICE	Number of DDP packets received for which there is no client.
MACIP_IP_IN	Number of IP packets received.
MACIP_IP_DDP_OUT	Number of IP packets received that were sent to the AppleTalk network.
MACIP_SERVER_IN	Number of packets destined for MacIP servers.
MACIP_SERVER_OUT	Number of packets sent by MacIP servers.
MACIP_SERVER_BAD_ATP	Number of MacIP allocation requests received with a bad request.
MACIP_SERVER_ASSIGN_IN	Number of MacIP allocation requests received asking for an IP address.
MACIP_SERVER_ASSIGN_ OUT	Number of IP addresses assigned.
MACIP_SERVER_INFO_IN	Number of MacIP packets received requesting server information.
MACIP_SERVER_INFO_OUT	Number of server information requests answered.

Related Commands

Command	Description
show appletalk traffic	Displays statistics about AppleTalk traffic.

show appletalk name-cache

To display a list of Name Binding Protocol (NBP) services offered by nearby routers and other devices that support NBP, use the **show appletalk name-cache** command in privileged EXEC mode.

show appletalk name-cache

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show appletalk name-cache** command displays the information currently in the NBP name cache.

Support for names allows you to easily identify and determine the status of any associated device. This can be important in AppleTalk internetworks where node numbers are dynamically generated.

You can authorize the **show appletalk name-cache** command to display any AppleTalk services of interest in local zones. This contrasts with the **show appletalk nbp** command, which you use to display services registered by routers.

Examples

The following is sample output from the **show appletalk name-cache** command:

```
Router# show appletalk name-cache

AppleTalk Name Cache:
Net    Adr  Skt  Name               Type           Zone
4160   19   8    gatekeeper         SNMP Agent     Underworld
4160   19   254  gatekeeper.Ether4  ciscoRouter    Underworld
4160   86   8    bones              SNMP Agent     Underworld
4160   86   72   131.108.160.78     IPADDRESS      Underworld
4160   86   254  bones.Ethernet0    IPGATEWAY      Underworld
```

Table 29 describes the fields shown in the display.

Table 29   show appletalk name-cache Field Descriptions

Field	Description
Net	AppleTalk network number or cable range.
Adr	Node address.

Table 29   show appletalk name-cache Field Descriptions (continued)

Field	Description
Skt	DDP socket number.
Name	Name of the service.
Type	Device type. The possible types vary, depending on the service. The following are the Cisco server types: • ciscoRouter—Server is a Cisco router. • SNMP Agent—Server is an SNMP agent. • IPGATEWAY—Active MacIP server names. • IPADDRESS—Active MacIP server addresses.
Zone	Name of the AppleTalk zone to which this address belongs.

Related Commands

Command	Description
show appletalk nbp	Displays the contents of the NBP name registration table.

show appletalk nbp

To display the contents of the Name Binding Protocol (NBP) name registration table, use the **show appletalk nbp** command in EXEC mode.

show appletalk nbp

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   The **show appletalk nbp** command lets you identify specific AppleTalk nodes. It displays services registered by the router. In contrast, use the **show appletalk name-cache** command to display any AppleTalk services of interest in local zones.

Routers with active AppleTalk interfaces register each interface separately. The Cisco IOS software generates a unique interface NBP name by appending the interface type name and unit number to the router name. For example, for the router named "router" that has AppleTalk enabled on Ethernet interface 0 in the zone Marketing, the NBP registered name is as follows:

```
router.Ethernet0:ciscoRouter@Marketing
```

Registering each interface on the router provides you with an indication that the device is configured and operating properly.

One name is registered for each interface. Other service types are registered once for each zone.

The Cisco IOS software deregisters the NBP name if AppleTalk is disabled on the interface for any reason.

Examples   The following is sample output from the **show appletalk nbp** command:

```
Router# show appletalk nbp

Net  Adr Skt Name                 Type          Zone
4160 211 254 pag.Ethernet0        ciscoRouter   Low End SW Lab
4160 211   8 pag                  SNMP Agent    Low End SW Lab
4172  84 254 pag.TokenRing0       ciscoRouter   LES Tokenring
4172  84   8 pag                  SNMP Agent    LES Tokenring
200   75 254 myrouter. Ethernet1  ciscoRouter   Marketing    *
```

Table 30 describes the fields shown in the display, as well as other fields that may also be displayed.

Table 30   ***show appletalk nbp Field Descriptions***

Field	Description
Net	AppleTalk network number.
Adr	Node address.
Skt	DDP socket number.
Name	Name of the service.
Type	Device type. The possible types vary, depending on the service. The following are the Cisco server types: • ciscoRouter—Cisco routers displayed by port. • SNMP Agent—SNMP agents displayed by zone if AppleTalk SNMP-over-DDP is enabled. • IPGATEWAY—Active MacIP server names. • IPADDRESS—Active MacIP server addresses.
Zone	Name of the AppleTalk zone to which this address belongs.
*	An asterisk in the right margin indicates that the name registration is pending confirmation.

	Command	Description
Related Commands	show appletalk name-cache	Displays a list of NBP services offered by nearby routers and other devices that support NBP.

show appletalk neighbors

To display information about the AppleTalk routers that are directly connected to any of the networks to which this router is directly connected, use the **show appletalk neighbors** command in EXEC mode.

show appletalk neighbors [*neighbor-address*]

Syntax Description

neighbor-address	(Optional) Displays information about the specified neighbor router.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If no neighbor address is specified, this command displays information about all AppleTalk routers.

The local router determines the AppleTalk network topology from its neighboring routers and learns from them most of the other information it needs to support the AppleTalk protocols.

Examples

The following is sample output from the **show appletalk neighbors** command:

```
Router# show appletalk neighbors

AppleTalk neighbors:
  17037.2      anger.Ethernet0/0        Ethernet0/0, uptime 8:33:27, 2 secs
          Neighbor is reachable as a RTMP peer
  17037.108     Ethernet0/0, uptime 8:33:21, 7 secs
          Neighbor is reachable as a RTMP peer
  17037.248     Ethernet0/0, uptime 8:33:30, 4 secs
          Neighbor is reachable as a RTMP peer
  17046.2      anger.Ethernet0/1        Ethernet0/1, uptime 8:33:27, 2 secs
          Neighbor is reachable as a RTMP peer
  17435.87     firewall.Ethernet0/0    Ethernet0/3, uptime 8:33:27, 6 secs
          Neighbor is reachable as a RTMP peer
  17435.186    the-wall.Ethernet0       Ethernet0/3, uptime 8:33:24, 5 secs
          Neighbor is reachable as a RTMP peer
  17435.233    teach-gw.Ethernet0       Ethernet0/3, uptime 8:33:24, 7 secs
          Neighbor is reachable as a RTMP peer
  17036.1      other-gw.Ethernet5 Ethernet0/5, uptime 8:33:29, 9 secs
          Neighbor is reachable as a RTMP peer
  4021.5       boojum.Hssi4/0   Hssi1/0, uptime 10:49:02, 0 secs
        Neighbor has restarted 1 time in 8:33:11.
          Neighbor is reachable as a static peer
```

Table 31 describes the fields shown in this display. Depending on the configuration of the **appletalk lookup-type** and **appletalk name-lookup-interval** commands, a node name as well as a node address also may be shown in this display.

Table 31   show appletalk neighbors Field Descriptions

Field	Description
31.86	AppleTalk address of the neighbor router.
Ethernet0/0	Router interface through which the neighbor router can be reached.
uptime 133:28:06	Amount of time (in hours, minutes, and seconds) that the Cisco IOS software has received this neighboring router's routing updates.
2 secs	Time (in seconds) since the software last received an update from the neighbor router.
Neighbor is reachable as a RTMP peer Neighbor is reachable as a static peer	Indicates how the route to this neighbor was learned.
Neighbor is down. Neighbor has restarted 1 time	Indicates whether neighbor is up or down, and number of times it has restarted in the specified time interval, displayed in the format hours:minutes:seconds.

The following is sample output from the **show appletalk neighbors** command when you specify the AppleTalk address of a particular neighbor:

```
Router# show appletalk neighbors 69.163

Neighbor 69.163, Ethernet0, uptime 268:00:52, last update 7 secs ago
  We have sent queries for 299 nets via 214 packets.
  Last query was sent 4061 secs ago.
  We received 152 replies and 0 extended replies.
  We have received queries for 14304 nets in 4835 packets.
  We sent 157 replies and 28 extended replies.
  We received 0 ZIP notifies.
  We received 0 obsolete ZIP commands.
  We received 4 miscellaneous ZIP commands.
  We received 0 unrecognized ZIP commands.
  We have received 92943 routing updates.
  Of the 92943 valid updates, 1320 entries were invalid.
  We received 1 routing update which were very late.
  Last update had 0 extended and 2 nonextended routes.
  Last update detail: 2 old
```

Table 32 describes the fields shown in this display. Depending on the configuration of the **appletalk lookup-type** and **appletalk name-lookup-interval** commands, a node name as well as a node address can be shown in this display.

Table 32   *show appletalk neighbors Field Descriptions—Specific Address*

Field	Description
Neighbor 69.163	AppleTalk address of the neighbor.
Ethernet0	Interface through which the router receives this neighbor's routing updates.
uptime 268:00:52	Amount of time (in hours, minutes, and seconds) that the Cisco IOS software has received this neighboring router's routing updates.
last update 7 secs ago	Time (in seconds) since the software last received an update from the neighbor router.
sent queries	Number of queries sent to neighbor networks and the number of query packets sent.
Last query was sent	Time (in seconds) since last query was sent.
received replies	Number of RTMP replies heard from this neighbor.
extended replies	Number of extended RTMP replies received from this neighbor.
ZIP notifies	Number of ZIP notify packets received from this neighbor.
obsolete ZIP commands	Number of nonextended-only (obsolete) ZIP commands received from this neighbor.
miscellaneous ZIP commands	Number of ZIP commands (for example, GNI, GZI, and GMZ) from end systems rather than from routers.
unrecognized ZIP commands	Number of bogus ZIP packets received from this neighbor.
routing updates	Number of RMTP updates received from this neighbor.
entries were invalid	Of the routing update packets received from this neighbor, the number of invalid entries discarded.
Last update detail	Of the routing update packets received from this neighbor, the number already known about.

Related Commands

Command	Description
appletalk lookup-type	Specifies which NBP service types are retained in the name cache.
appletalk name-lookup-interval	Sets the interval between service pollings by the router on its AppleTalk interfaces.

show appletalk remap

To display domain remapping information, use the **show appletalk remap** EXEC command.

show appletalk remap [**domain** *domain-number* [{**in** | **out**} [{**to** | **from**} *domain-network*]]]

Syntax Description

domain *domain-number*	(Optional) Number of an AppleTalk domain about which to display remapping information. It can be a decimal integer from 1 through 1,000,000.
in	(Optional) Displays remapping information about inbound packets, that is, on packets entering the local segment of the domain.
out	(Optional) Displays remapping information about outbound packets, that is on packets exiting from the local segment of the domain.
to	(Optional) Displays information about the network number or cable range to which an address has been remapped.
from	(Optional) Displays information about the original network number or cable range.
domain-network	(Optional) Number of an AppleTalk network.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you omit all options, keywords, and arguments, the **show appletalk remap** command displays all remapping information about all domains.

Examples

The following is sample output from the **show appletalk remap** command:

```
Router# show appletalk remap

      AppleTalk   Remapping  Table :
      ----------------------------

      Domain 1 : Domain 1   State : Active
      -----------------------------------------

      Direction : IN

      Domain Net(Cable)       Remapped to        Status
      3    - 3               100   - 100          Good
```

```
 Direction : OUT

Domain Net(Cable)        Remapped to          Status
1    - 1                 200   - 200          Good

Domain 2 : Domain 2   State : Active
-----------------------------------------

Direction : IN

Domain Net(Cable)        Remapped to          Status

Direction : OUT

Domain Net(Cable)        Remapped to          Status
2    - 2                 400   - 400          Good
100  - 100               401   - 401          Good
```

The following is sample output from the **show appletalk remap** command when you specify a domain number:

```
Router# show appletalk remap domain 1

     AppleTalk   Remapping  Table :
     -----------------------------

     Domain 1 : Domain 1   State : Active
     -----------------------------------------

     Direction : IN

     Domain Net(Cable)        Remapped to          Status
     3    - 3                 100   - 100          Good

     Direction : OUT

     Domain Net(Cable)        Remapped to          Status
     1    - 1                 201   - 201          Good
```

The following is sample output from the **show appletalk remap** command to display inbound remappings for AppleTalk network 100:

```
Router# show appletalk remap domain 1 in from 100

     AppleTalk   Remapping  Table :
          -----------------------------

For the Remap 100  the Domain  net is 3
```

Table 33 describes the fields shown in the display.

Table 33   show appletalk remap Field Descriptions

Field	Description
Domain	Number of the AppleTalk IP domain.
State	State of the domain. It can be either Active or Nonactive.
Direction	Indicates whether the mapping is an inbound one (for packets entering the local domain segment) or an outbound one (for packets leaving the local domain segment).

Table 33   show appletalk remap Field Descriptions (continued)

Field	Description
Domain Net (Cable)	Network number or cable range that is being remapped.
Remapped to	Number or range of numbers to which a network number or cable range has been remapped.
Status	It can be one of the following values: • Unassigned—The network number or cable range was just remapped. • Unzipped—The remapped network number or cable range is trying to acquire a zone list. This state is possible for inbound remapped network numbers only. • Suspect—The Cisco IOS software suspects that it already has this entry in the routing table, and it is performing loop detection for this entry. This state is possible for inbound remappings only. • Good—The remapped entry has a complete zone list and, for inbound remappings only, it is in the main routing table. • Bad—The remapping entry is about to be deleted from the remapping table.

Related Commands

Command	Description
appletalk domain remap-range	Remaps ranges of AppleTalk network numbers or cable ranges between two segments of a domain.

show appletalk route

To display all entries or specified entries in the AppleTalk routing table, use the **show appletalk route** EXEC command.

show appletalk route [*network | type number*]

Syntax Description

network	(Optional) Displays the routing table entry for the specified network.
type number	(Optional) Displays the routing table entries for networks that can be reached via the specified interface type and number.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The E - EIGRP field was removed from command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   If you omit the arguments, this command displays all entries in the routing table.

Examples   The following is sample output from the **show appletalk route** command for a nonextended AppleTalk network:

```
Router# show appletalk route

Codes: R - RTMP derived, C - connected, A - AURP
P - proxy, S - static
5 routes in internet
C Net 258 directly connected, 1431 uses, Ethernet0, zone Twilight
R Net 6 [1/G] via 258.179, 8 sec, 0 uses, Ethernet0, zone The O
C Net 11 directly connected, 472 uses, Ethernet1, zone No Parking
R Net 2154 [1/G] via 258.179, 8 sec, 6892 uses, Ethernet0, zone LocalTalk
S Net 1111 via 258.144, 0 uses, Ethernet0, no zone set
[hops/state] state can be one of G:Good, S:Suspect, B:Bad
```

The following is sample output from the **show appletalk route** command for an extended AppleTalk network:

```
Router# show appletalk route

Codes: R - RTMP derived, C - connected, A - AURP
P - proxy, S - static
5 routes in internet
E Net 10000 -10000 [1/G] via 300.199, 275 sec, Ethernet2, zone France
R Net 890 [2/G] via 4.129, 1 sec, Ethernet0, zone release lab
```

```
R Net 901 [2/G] via 4.129, 1 sec, Ethernet0, zone Dave's House
C Net 999-999 directly connected, Serial3, zone Magnolia Estates
R Net 2003 [4/G] via 80.129, 6 sec, Ethernet4, zone Bldg-13
```

The following is sample output from the **show appletalk route** command when AppleTalk load balancing is enabled. The output displayed shows additional equal-cost path entries.

```
Router# show appletalk route

Codes: R - RTMP derived, C - connected, A - AURP
       P - proxy, S - static
759 routes in internet. Up to 4 parallel paths allowed.

The first zone listed for each entry is its default (primary) zone.

R Net 20-20 [2/G] via 60.172, 1 sec, Ethernet1/2,
                  via 1010.68 1 sec, Ethernet1/3,
                  via 70.199, 2 sec, Ethernet1/5, zone zone20
R Net 32-32 [9/G] via 60172, 2 sec, Ethernet1/2
                  via 1010.68, 2 sec, Ethernet1/3,
                  via 70.199, 2 sec, Ethernet1/5,
                  Zone: "Executive Briefing Center"
R Net 43-43 [7/G] via 60.172, 2 sec, Ethernet1/2,
                  via 1010.68, 2 sec, Ethernet1/3,
                  via 70.199, 2 sec, Ethernet1/5, zone ISDN Tunnel
R Net 57-57 [6/G] via 60.172, 2 sec, Ethernet1/2,
                  via 1010.68, 2 sec, Ethernet1/3,
                  via 70.199, 2 sec, Ethernet1/5, zone zone-home-bumi
```

Table 34 describes the fields shown in the two displays, as well as some fields not shown but that may also be displayed. Depending on the configuration of the **appletalk lookup-type** and **appletalk name-lookup-interval** global configuration commands, a node name may appear in this display instead of a node address.

Table 34   *show appletalk route Field Descriptions*

Field	Description
Codes:	Codes defining how the route was learned.
R - RTMP derived	Route learned from an RTMP update.
C - Connected	Directly connected network.
A - AURP	Route learned from an AURP update.
S - Static	Statically defined route.
P - Proxy	Proxy route. Proxy routes are included in outgoing RTMP updates as if they were directly connected routes (although they are not really directly connected), since they are not associated with any interface. Whenever an NBQ BrRq for the zone in question is generated by anyone anywhere in the internetwork, an NBP FwdReq is directed to any router connected to the proxy route. The Phase 2 router (which is the only router directly connected) converts the FwdReq to LkUps, which are understood by Phase 1 routers, and sends them to every network in the zone.
routes	Number of routes in the table.
Net	Network to which the route goes.

Table 34   show appletalk route Field Descriptions (continued)

Field	Description
Net 999-999	Cable range to which the route goes.
directly connected	Indicates that the network is directly connected to the router.
uses	Fair estimate of the number of times a route gets used. It actually indicates the number of times the route has been selected for use prior to operations such as access list filtering.
Ethernet	Possible interface through which updates to the remote network will be sent.
zone	Name of zone of which the destination network is a member.
[1/G]	Number of hops to this network, followed by the state of the link to that network. The state can be one of the following letters: • G—Link is good. • S—Link is suspect. • B—Link is bad. The state is determined from the routing updates that occur at 10-second intervals. A separate and nonsynchronized event occurs at 20-second intervals, checking and flushing the ratings for particular routes that have not been updated. For each 20-second period that passes with no new routing information, a rating changes from G to S and then from S to B. After 1 minute with no updates, that route is flushed. Every time the Cisco IOS software receives a useful update, the status of the route in question is reset to G. Useful updates are those advertising a route that is as good or better than the one currently in the table. When an AppleTalk route is poisoned by another router, its metric gets changed to poisoned (that is, 31 hops). The software then will age this route normally during a holddown period, during which the route will still be visible in the routing table.
via 258.179	Address of a router that is the next hop to the remote network.
via gatekeeper	Node name of a router that is the next hop to the remote network.
sec	Number of seconds that have elapsed since an RMTP update about this network was last received.

The following is sample output from the **show appletalk route** command when you specify a network number:

```
Router# show appletalk route 69

Codes: R - RTMP derived, C - connected, A - AURP
P - proxy, S - static

The first zone listed for each entry is its default (primary) zone.
```

```
R Net 69-69 [2/G] via gatekeeper, 0 sec, Ethernet0, zone Empty Guf
Route installed 125:20:21, updated 0 secs ago
Next hop: gatekeeper, 2 hops away
Zone list provided by gatekeeper
Route has been updated since last RTMP was sent
Valid zones: "Empty Guf"
```

Table 35 describes the fields shown in the display.

Table 35   *show appletalk route Field Descriptions—Specified Network*

Field	Description
Codes:	Codes defining how the route was learned.
R - RTMP derived	Route learned from an RTMP update.
C - Connected	Directly connected network.
A - AURP derived	Route learned from an AURP update.
P - Proxy	Proxy route.
S - Static	Static route.
routes in internet	Number of routes in the Apple Talk internet.
Net	Cable range to which the route goes. This is the number of the network you specified on the **show appletalk route** command line.
[2/G]	Number of hops to this network, followed by the state of the link to that network. The state can be one of the following letters: • G—Link is good. • S—Link is suspect. • B—Link is bad. The state is determined from the routing updates that occur at 10-second intervals. A separate and nonsynchronized event occurs at 20-second intervals, checking and flushing the ratings for particular routes that have not been updated. For each 20-second period that passes with no new routing information, a rating changes from G to S and then from S to B. After 1 minute with no updates, that route is flushed. Every time the Cisco IOS software receives a useful update, the status of the route in question is reset to G. Useful updates are those advertising a route that is as good or better than the one currently in the table. When an AppleTalk route is poisoned by another router, its metric gets changed to poisoned (that is, 31 hops). The software then will age this route normally during a holddown period, during which the route will still be visible in the routing table.
via gatekeeper	Address or node name of a router that is the next hop to the remote network.

Table 35   show appletalk route Field Descriptions—Specified Network (continued)

Field	Description
0 sec	Number of seconds that have elapsed since an RMTP update about this network was last received.
Ethernet0	Possible interface through which updates to the remote network will be sent.
zone Empty Guf	Name of zone of which the destination network is a member.
Route installed 125:20:21	Length of time (in hours, minutes, and seconds) since this route was first learned about.
updated 0 secs ago	Time (in seconds) since the software received an update for this route.
Next hop: gatekeeper	Address or node name of the router that is one hop away.
2 hops away	Number of hops to the network specified in the **show appletalk route** command line.
Zone list provided by gatekeeper	Address or node name of the router that provided the zone list included with the RTMP update.
Route has been updated since last RTMP was sent	Indicates whether the software has received a routing update from a neighboring router since the last time the software sent an RTMP update for this route.
Valid zones: "Empty Guf"	Zone names that are valid for this network.

Related Commands

Command	Description
appletalk lookup-type	Specifies which NBP service types are retained in the name cache.
appletalk maximum-paths	Defines the maximum number of equal-cost paths the router should use when balancing the traffic load.
appletalk name-lookup-interval	Sets the interval between service pollings by the router on its AppleTalk interfaces.
appletalk proxy-nbp	Assigns a proxy network number for each zone in which there is a router that supports only nonextended AppleTalk.
clear appletalk route	Deletes entries from the routing table.

show appletalk sockets

To display all information or specified information about process-level operation in the sockets of an AppleTalk interface, use the **show appletalk sockets** privileged EXEC command.

show appletalk sockets [*socket-number*]

Syntax Description	*socket-number* (Optional) Displays information about the specified socket number.

Command Modes   Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   If no socket number is specified, this command displays information about all sockets.

Examples   The following is sample output from the **show appletalk sockets** command when you do not specify a socket number:

```
Router# show appletalk sockets

Socket    Name      Owner         Waiting/Processed
1         RTMP      AT RTMP          0     148766
2         NIS       AT NBP           0     15642
4         AEP       AT Maintenance   0     0
6         ZIP       AT ZIP           0     13619
8         SNMP      AT SNMP          0     0
253       PingServ  AT Maintenance   0     0
```

The following is sample output from the **show appletalk sockets** command when you do specify a socket number:

```
Router# show appletalk sockets 6

6         ZIP       AT ZIP           0     13619
```

Table 36 describes the fields shown in these displays.

Table 36   *show appletalk sockets Field Descriptions*

Field	Description
Socket	Socket number.
Name	Name of the socket.
Owner	Process that is managing communication with this socket.
Waiting/Processed	Number of packets waiting to be processed by the socket, and number of packets that have been processed by the socket since it was established.

show appletalk static

To display information about the statically defined routes, including floating static routes, use the **show appletalk static** EXEC command.

show appletalk static

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples   The following is sample output from the **show appletalk static** command:

```
Router# show appletalk static

    AppleTalk    Static    Entries
-------------------------------------
Network     NextIR     Zone      Status

100-109     1.10       Zone100   A
200         1.10       Zone200   A
300-309     1.10       Zone300   A(Floating)
```

Table 37 describes the fields shown in the display.

Table 37   *show appletalk static Field Descriptions*

Field	Description
Network	For an extended AppleTalk network, the network range. For a nonextended AppleTalk network, the network number.
NextIR	The next internetwork router.
Zone	The AppleTalk zone name.
Status	The status of the route, which can be one of the following: • A—The static route is active. • A(Floating)—The floating static route is active. • N/A—The static route is not active. • N/A(Floating)—The floating static route is not active.

Related Commands

Command	Description
appletalk static cable-range	Defines a static route or a floating static route on an extended network.
appletalk static network	Defines a static route or a floating static route on a nonextended network.
show appletalk neighbors	Displays information about the AppleTalk routers that are directly connected to any of the networks to which this router is directly connected.
show appletalk route	Displays all entries or specified entries in the AppleTalk routing table.

show appletalk traffic

To display statistics about AppleTalk traffic, including MacIP traffic, use the **show appletalk traffic** EXEC command.

show appletalk traffic

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The EIGRP section was removed from command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   For MacIP traffic, an IP alias is established for each MacIP client and for the IP address of the MacIP server if it does not match an existing IP interface address. To display the client aliases, use the **show ip aliases** command.

Examples   The following is sample output from the **show appletalk traffic** command:

```
Router# show appletalk traffic

AppleTalk statistics:
  Rcvd:  357471 total, 0 checksum errors, 264 bad hop count
         321006 local destination, 0 access denied
         0 for MacIP, 0 bad MacIP, 0 no client
         13510 port disabled, 2437 no listener
         0 ignored, 0 martians
  Bcast: 191881 received, 270406 sent
  Sent:  550293 generated, 66495 forwarded, 1840 fast forwarded, 0 loopback
         0 forwarded from MacIP, 0 MacIP failures
         436 encapsulation failed, 0 no route, 0 no source
  DDP:   387265 long, 0 short, 0 macip, 0 bad size
  NBP:   302779 received, 0 invalid, 0 proxies
         57875 replies sent, 59947 forwards, 418674 lookups, 432 failures
  RTMP:  108454 received, 0 requests, 0 invalid, 40189 ignored
         90170 sent, 0 replies
  AURP:  0 Open Requests, 0 Router Downs
         0 Routing Information sent, 0 Routing Information received
         0 Zone Information sent, 0 Zone Information received
         0 Get Zone Nets sent, 0 Get Zone Nets received
         0 Get Domain Zone List sent, 0 Get Domain Zone List received
AppleTalk statistics:
```

```
        0 bad sequence
ATP:   0 received
ZIP:   13619 received, 33633 sent, 32 netinfo
Echo:  0 received, 0 discarded, 0 illegal
       0 generated, 0 replies sent
Responder:  0 received, 0 illegal, 0 unknown
       0 replies sent, 0 failures
AARP:  85 requests, 149 replies, 100 probes
       84 martians, 0 bad encapsulation, 0 unknown
       278 sent, 0 failures, 29 delays, 315 drops
Lost: 0 no buffers
Unknown: 0 packets
Discarded: 130475 wrong encapsulation, 0 bad SNAP discriminator
```

Table 38 describes the fields shown in the display.

Table 38   show appletalk traffic Field Descriptions

Field	Description
Rcvd:	This section describes the packets received.
357741 total	Total number of packets received.
0 checksum errors	Number of packets that were discarded because their DDP checksum was incorrect. The DDP checksum is verified for packets that are directed to the router. It is not verified for forwarded packets.
264 bad hop count	Number of packets discarded because they had traveled too many hops.
321006 local destination	Number of packets addressed to the local router.
0 access denied	Number of packets discarded because they were denied by an access list.
0 for MacIP	Number of AppleTalk packets the Cisco IOS software received that were encapsulated within an IP packet.
0 bad MacIP	Number of bad MacIP packets the software received and discarded. These packets may have been malformed or may not have included a destination address.
0 no client	Number of packets discarded because they were directed to a nonexistent MacIP client.
13510 port disabled	Number of packets discarded because routing was disabled for that port (extended AppleTalk only). This is the result of a configuration error or a packet's being received while the software is in verification/discovery mode.
2437 no listener	Number of packets discarded because they were directed to a socket that had no services associated with it.
0 ignored	Number of routing update packets ignored because they were from a misconfigured neighbor or because routing was disabled.
0 martians	Number of packets discarded because they contained bogus information in the DDP header. What distinguishes this error from the others is that the data in the header is never valid as opposed to not being valid at a given point in time.

Table 38   *show appletalk traffic Field Descriptions (continued)*

Field	Description
Bcast:	Number of broadcast packets sent and received.
191881 received	Number of broadcast packets received.
270406 sent	Number of broadcast packets sent.
Sent:	Number of packets transmitted.
550293 generated	Number of packets generated.
66495 forwarded	Number of packets forwarded using routes derived from process switching.
1840 fast forwarded	Number of packets sent using routes from the fast-switching cache.
0 loopback	Number of packets that were broadcast out an interface on the router for which the device simulated reception of the packet because the interface does not support sending a broadcast packet to itself. The count is cumulative for all interfaces on the device.
0 forwarded from MacIP	Number of IP packets forwarded that were encapsulated within an AppleTalk DDP packet.
0 MacIP failures	Number of MacIP packets sent that were corrupted during the MacIP encapsulation process.
436 encapsulation failed	Number of packets the router could not send because encapsulation failed. This can happen because encapsulation of the DDP packet failed or because AARP address resolution failed.
0 no route	Number of packets the router could not send because it knew of no route to the destination.
0 no source	Number of packets the router sent when it did not know its own address. This should happen only if something is seriously wrong with the router or network configuration.
DDP:	This section describes DDP packets seen.
387265 long	Number of DDP long packets.
0 short	Number of DDP short packets.
0 macip	Number of IP packets encapsulated in an AppleTalk DDP packet that the router sent.
0 bad size	Number of packets whose physical packet length and claimed length differed.
NBP:	This section describes NBP packets.
302779 received	Total number of NBP packets received.
0 invalid	Number of invalid NBP packets received. Causes include invalid op code and invalid packet type.
0 proxies	Number of NBP proxy lookup requests received by the router when it was configured for NBP proxy transition usage.
57875 replies sent	Number of NBP replies sent.

Cisco IOS AppleTalk Command Reference ■

Table 38   show appletalk traffic Field Descriptions (continued)

Field	Description
59947 forwards	Number of NBP forward requests received or sent.
418674 lookups	Number of NBP lookups received.
432 failures	Generic counter that increments any time the NBP process experiences a problem.
RTMP:	This section describes RTMP packets.
108454 received	Total number of RTMP packets received.
0 requests	Number of RTMP requests received.
0 invalid	Number of invalid RTMP packets received. Causes include invalid op code and invalid packet type.
40189 ignored	Number of RTMP packets ignored. One reason for this is that the interface is still in discovery mode and is not yet initialized.
90170 sent	Number of RTMP packets sent.
0 replies	Number of RTMP replies sent.
ATP:	This section describes ATP packets.
0 received	Number of ATP packets the router received.
ZIP:	This section describes ZIP packets.
13619 received	Number of ZIP packets the router received.
33633 sent	Number of ZIP packets the router sent.
32 netinfo	Number of packets that requested port configuration via ZIP GetNetInfo requests. These are commonly used during node startup and are occasionally used by some AppleTalk network management software packages.
Echo:	This section describes AEP packets.
0 received	Number of AEP packets the router received.
0 discarded	Number of AEP packets the router discarded.
0 illegal	Number of illegal AEP packets the router received.
0 generated	Number of AEP packets the router generated.
0 replies sent	Number of AEP replies the router sent.
Responder:	This section describes Responder Request packets.
0 received	Number of Responder Request packets the router received.
0 illegal	Number of illegal Responder Request packets the router received.
0 unknown	Number of Responder Request packets the router received that it did not recognize.
0 replies sent	Number of Responder Request replies the router sent.
0 failures	Number of Responder Request replies the router could not send.
AARP:	This section describes AARP packets.

Table 38   show appletalk traffic Field Descriptions (continued)

Field	Description
85 requests	Number of AARP requests the router received.
149 replies	Number of AARP replies the router received.
100 probes	Number of AARP probe packets the router received.
84 martians	Number of AARP packets the router did not recognize. If you start seeing an inordinate number of martians on an interface, check whether a bridge has been inserted into the network. When a bridge is starting up, it floods the network with AARP packets.
0 bad encapsulation	Number of AARP packets received that had an unrecognizable encapsulation.
0 unknown	Number of AARP packets the router did not recognize.
278 sent	Number of AARP packets the router sent.
0 failures	Number of AARP packets the router could not send.
29 delays	Number of AppleTalk packets delayed while waiting for the results of an AARP request.
315 drops	Number of AppleTalk packets dropped because an AARP request failed.
Lost: 0 no buffers	Number of packets lost because of lack of buffer space.
Unknown: 0 packets	Number of packets whose protocol could not be determined.
Discarded:	This section describes the number of packets that were discarded.
130475 wrong encapsulation	Number of packets discarded because they had the wrong encapsulation.That is, nonextended AppleTalk packets were on an extended AppleTalk network, or vice versa.
0 bad SNAP discrimination	Number of packets discarded because they had the wrong SNAP discriminator. This occurs when another AppleTalk device has implemented an obsolete or incorrect packet format.
AURP:	This section describes AppleTalk Update Routing Protocol packets.
0 open requests	Total number of open requests.
0 router downs	Number of router down packets received.
0 routing information sent	Number of routing information packets sent.
0 routing information received	Number of routing information packets received.
0 zone information sent	Number of ZIP packets sent.
0 zone information received	Number of ZIP packets received.
0 get zone nets sent	Number of get zone network packets sent requesting zone information.
0 get zone nets received	Number of get zone network packets received requesting zone information.

Table 38   show appletalk traffic Field Descriptions (continued)

Field	Description
0 get domain zone list sent	Number of get domain zone list packets sent requesting domain zone list information.
0 get domain zone list received	Number of get domain zone list packets received requesting domain zone list information.
0 bad sequence	Number of AURP packets received out of sequence.

Related Commands

Command	Description
clear appletalk traffic	Resets AppleTalk traffic counters.
show appletalk macip-traffic	Displays statistics about MacIP traffic through the router.
show ip aliases	Displays the IP addresses mapped to TCP ports (aliases) and SLIP addresses, which are treated similarly to aliases.

show appletalk zone

To display all entries or specified entries in the zone information table, use the **show appletalk zone** EXEC command.

show appletalk zone [*zone-name*]

Syntax Description		
	zone-name	(Optional) Displays the entry for the specified zone.

Command Modes   EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   If no zone name is specified, the command displays all entries in the zone information table.

You can use this command on extended and nonextended networks.

A zone name can be associated with multiple network addresses or cable ranges, or both. There is not a one-to-one correspondence between a zone name and a LAN; a zone name may correspond to one or more networks (LANs or network interfaces). This means that a zone name will effectively replace multiple network addresses in zone filtering. This is reflected in the output of the **show appletalk zone** command. For example, the zone named *Mt. View 1* in the following example is associated with two network numbers and four cable ranges.

Examples   The following is sample output from the **show appletalk zone** command:

```
Router# show appletalk zone

Name                 Network(s)
Engineering          3 29-29 4042-4042
customer eng         19-19
CISCO IP             4140-4140
Dave's House         3876 3924 5007
Narrow Beam          4013-4013 4023-4023 4037-4037 4038-4038
Low End SW Lab       6160 4172-4172 9555-9555 4160-4160
Tir'n na'Og          199-199
Mt. View 1           7010-7010 7122 7142 7020-7020 7040-7040 7060-7060
Mt. View 2           7152 7050-7050
UDP                  1112-12
Empty Guf            69-69
Light                80
europe               2010 3010 3034 5004
Bldg-13              4032 5026 61669 3012 3025 3032 5025 5027
Bldg-17              3004 3024 5002 5006
```

The following is sample output from the **show appletalk zone** command when you specify a zone name:

```
Router# show appletalk zone CISCO IP

AppleTalk Zone Information for CISCO IP:
  Valid for nets: 4140-4140
  Not associated with any interface.
  Not associated with any access list.
```

Table 39 describes the fields shown in the display.

Table 39   show appletalk zone Field Descriptions—Specific Zone Name

Field	Description
AppleTalk Zone Information for CISCO IP:	Name of the zone.
Valid for nets: 4140-4140	Cable range(s) or network numbers assigned to this zone.
Not associated with any interface.	Interfaces that have been assigned to this zone.
Not associated with any access list.	Access lists that have been defined for this zone.

Related Commands

Command	Description
appletalk zone	Sets the zone name for the connected AppleTalk network.

show smrp forward

To display all entries or specific entries in the Simple Multicast Routing Protocol (SMRP) forwarding table, use the **show smrp forward** EXEC command.

show smrp forward [**appletalk** [*group-address*]]

Syntax Description

appletalk	(Optional) Displays SMRP forwarding table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk only.
group-address	(Optional) SMRP group address. All members of a group listen for multicast packets on this address.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The SMRP forwarding table describes the relationship between the SMRP router and the distribution tree for each SMRP group on the internetwork. An SMRP router has an entry in this table for every SMRP group for which the router is forwarding data. When data for an SMRP group arrives on the parent interface, it is forwarded to each child interface.

Looking at child and parent interfaces in relation to members of an SMRP group, a child interface is a neighbor that is farther away from the SMRP creator node and a parent interface is one that is closer to the creator node.

If no SMRP group address is specified, then the **show smrp forward** command displays information for all entries in the SMRP forwarding table. For all entries, the **show smrp forward** command displays the SMRP group address, the state of the SMRP group, the parent interface and address, and one or more child interfaces and addresses.

If an SMRP group address is specified, the command displays additional information for that group showing the child count, the time elapsed since the entry was updated, and the next poll time.

Note Because SMRP is currently supported over AppleTalk networks only, sample output resulting from the **show smrp forward** command is the same as output from the **show smrp forward appletalk** command.

Examples   The following is sample output from the **show smrp forward** command that shows all entries:

```
Router# show smrp forward

SMRP Forwarding Table

Group        State        Parent                     Child
Address              Interface    Address    Interface    Address
-----------------------------------------------------------------

AT 1.2     Fwd    Ethernet2    20.3       Ethernet3    30.2
AT 10.1    Fwd    Ethernet2    20.4       Ethernet4    40.2
AT 30.1    Fwd    Ethernet3    30.1       Ethernet2    20.2
```

The following is sample output from the **show smrp forward** command with the **appletalk** keyword and an SMRP group address specified:

```
Router# show smrp forward appletalk 10.1

Group        State        Parent                     Child
Address              Interface    Address    Interface    Address
-----------------------------------------------------------------

AT 10.1    Fwd    Ethernet2    20.4       Ethernet4    40.2

Child count: 1
Elapsed update time: 01:15:32
Next poll time (sec): 3
```

Table 40 describes the fields shown in the displays.

Table 40   show smrp forward Field Descriptions

Field	Description
Group Address	Address of the SMRP group.
State	State of the group. Possible states are as follows: • Join—Joining the group • Fwd—Forwarding data • Leave—Leaving the group
Parent Interface	Interface that receives data to be forwarded.
Parent Address	Address of the parent interface.
Child Interface	One or more interfaces to which data is forwarded.
Child Address	Address of the interface.
Child Count	For a specific SMRP group address, the number of children for the group.
Elapsed update time	Time elapsed since the last change was made to the forwarding entry.
Next poll time	Time remaining before polling all child members.

show smrp globals

To display global information about Simple Multicast Routing Protocol (SMRP)—such as whether SMRP is enabled and running and settings for timers, most of which are used internally—use the **show smrp globals** EXEC command.

show smrp globals

Syntax Description   This command has no arguments or keywords.

Command Modes   EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples   The following is sample output from the **show smrp globals** command:

```
Router# show smrp globals

SMRP global information:
  SMRP is running.
  Maximum number of retries for requests is 4 times.
  Request transactions are sent every 10 seconds.
  Response transactions are sent every 100 seconds.
  Creators are polled every 60 seconds.
  Members are polled every 30 seconds.
  Hellos are sent every 10 seconds.
  Neighbors are down after not being heard from for 30 seconds.
  Poisoned routes purged after 60 seconds.
  Primary requests sent every 1 second.
  Secondary requests sent every 1 second.
```

Table 41 describes the global information shown in the display.

Table 41   *show smrp globals Field Descriptions*

Field	Description
SMRP is running.	SMRP is enabled.
Maximum number of retries for requests is 4.	This value is used internally.

Cisco IOS AppleTalk Command Reference

Table 41   show smrp globals Field Descriptions (continued)

Field	Description
Request transactions are sent every 10 seconds.	This timer is used internally.
Response transactions are sent every 100 seconds.	This timer is used internally. This is a variable value that is determined by the following mathematical formula: $2 * request\text{-}interval * (maximum\text{-}retries + 1)$
Creators are polled every 60 seconds.	Identifies how often the Cisco IOS software polls the SMRP group creator. This timer is used internally.
Members are polled every 30 seconds.	Identifies how often the software polls the SMRP group members. This timer is used internally.
Hellos are sent every 10 seconds.	Identifies how often the software sends hello packets to its neighbors.
Neighbors are down after not being heard from for 30 seconds.	Identifies the time in seconds that elapses after which neighbors that are not heard from are assumed to be down.
Poisoned routes are purged after 60 seconds.	Poisoned routes are bad route having a distance of 255 hops.
Primary requests sent every 1 second.	Primary requests are requests from a secondary router requesting to become the primary router. Only a secondary router can become a primary router.
Secondary requests sent every 1 second.	Secondary requests are requests from a router in normal operation mode requesting to become a secondary router. Only a router in normal mode can become a secondary router.

show smrp group

To display all entries or specific entries in the SMRP group table, use the **show smrp group** EXEC command.

show smrp group [**appletalk** [*group-address*]]

Syntax Description		
appletalk	(Optional) Displays SMRP group table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk networks only.
group-address	(Optional) SMRP group address.

Command Modes EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines If no SMRP group address is specified, the command displays the group address, the state, and the parent and child information for all entries in the SMRP group table. If a group address is specified, the command displays the standard information plus additional information for that group showing the child count, the elapsed update time, and the next poll time.

> **Note** Because SMRP is currently supported over AppleTalk networks only, sample output resulting from the **show smrp group** command is the same as output from **show smrp group appletalk** command.

An SMRP group address is an address that is based on the local network address of the network to which the creator of the SMRP group belongs.

Examples The following is sample output from the **show smrp group** command that shows all group table entries:

```
Router# show smrp group

SMRP Group Table
Group         Creation  Next       Creator
Address       Time      Poll  Interface    Address
------------------------------------------------------------

AT 30.1       0:04:37   22    Ethernet3    30.1
```

```
AT 40.2        0:04:35   24     Ethernet4      40.1
AT 40.1        0:04:36   23     Ethernet4      40.1
```

The following is sample output from the **show smrp group** command with the **appletalk** keyword and an SMRP group address specified:

```
Router# show smrp group appletalk 40.2

SMRP Group Table
Group       Creation  Next            Creator
Address     Time      Poll  Interface     Address
---------------------------------------------------------------

AT 40.2    0:05:58   1     Ethernet4      40.1
```

Table 42 describes the fields shown in the display.

Table 42   show smrp group Field Descriptions

Field	Description
Group Address	SMRP group address. AT signifies that this is an AppleTalk network group.
Creation Time	Elapsed time since the group was created in hours, minutes, and seconds (*hh*:*mm*:*ss*).
Next Poll	Time remaining until the next check is performed to determine if the creator is still active.
Creator Interface	Interface that the creator of the SMRP group is on.
Creator Address	Address of the creator.

show smrp mcache

To display the SMRP fast-switching cache table, use the **show smrp mcache** EXEC command.

show smrp mcache [**appletalk** [*group-address*]]

Syntax Description		
appletalk	(Optional) Displays the SMRP fast-switching cache table entries for all AppleTalk network groups. Currently, SMRP services are supported over AppleTalk only.	
group-address	(Optional) SMRP group address. Use this argument to display only this group's fast-switching cache table entry.	

Command Modes   EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   An SMRP router has an entry in its forwarding table for every SMRP group for which the router forwards data. For each group, the forwarding table lists the parent interface and address and one or more child interfaces and addresses. When data for an SMRP group arrives on the parent interface, the router forwards it to each child interface. The SMRP fast-switching cache table specifies whether or not to fast switch SMRP data packets out the interfaces specified by the forwarding table.

Use the **show smrp mcache** command to view the SMRP fast-switching cache table. The command displays which interfaces are fast-switch enabled. If a parent interface is not fast-switch enabled, then there is no entry (row) in the table. If a child interface is not fast-switch enabled, then it is not in the list of child interfaces for an entry in the table.

If you do not specify an SMRP group address, the **show smrp mcache** command displays information for all entries in the SMRP fast-switching cache table. If you specify an SMRP group address, the command displays cache entries for only that group.

SMRP fast-switching is enabled by default.

Examples   The following is sample output from the **show smrp mcache** command:

```
Router# show smrp mcache

SMRP Multicast Fast Switching Cache
```

```
Group         In  Parent        Child          MAC Header (Top)
Address       Use Interface     Interface(s)   Network Header (Bottom)
------------------------------------------------------------------

AT 11.121     Y   Ethernet0     Ethernet3      090007400b7900000c1740db
                                               001fed750000002aff020a0a0a
AT 11.122     Y   Ethernet0     Ethernet3      090007400b7a00000c1740db
                                               001f47750000002aff020a0a0a
AT 11.123     Y   Ethernet0     Ethernet1      090007400b7b00000c1740d9
                                               001fe77500000014ff020a0a0a
                                Ethernet3      090007400b7b00000c1740db
                                               001ffd750000002aff020a0a0a
AT 11.124     N   Ethernet0     Ethernet1      090007400b7c00000c1740d9
                                               001fef7500000014ff020a0a0a
```

Table 43 describes the fields shown in the display.

Table 43   show smrp mcache Field Descriptions

Field	Description
Group Address	SMRP group address. AT signifies that this is an AppleTalk network group.
In Use	Y = Router can use the cache entry to fast-switch packets. N = Router cannot use cache entry to fast-switch packets. Router forwards packets via the process level.
Parent Interface	Interface that receives the SMRP data packet to send out. The interface must be fast-switch enabled.
Child Interface(s)	One or more interfaces to which the SMRP data packet is sent. At least one of the child interfaces must be fast-switch enabled.
MAC Header (Top) Network Header (Bottom)	MAC header and network header for only fast-switch enabled child interfaces.

Related Commands

Command	Description
clear smrp mcache	Removes all fast-switching entries in the SMRP fast-switching cache table.
show smrp forward	Displays all entries or specific entries in the SMRP forwarding table.

show smrp neighbor

To display all entries or specific entries in the SMRP neighbor table, use the **show smrp neighbor** EXEC command.

show smrp neighbor [**appletalk** [*network-address*]]

Syntax Description		
appletalk	(Optional) Displays SMRP neighbor table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk networks only.
network-address	(Optional) Network address of the neighbor router.

Command Modes EXEC

Command History	Release	Modification
	11.0	This command was introduced.
	12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines A neighbor is an adjacent router. Neighboring routers keep track of one another by sending and receiving hello packets periodically. Using this method, the Cisco IOS software can determine if it has heard from a neighbor router within a certain amount of time. The software creates an entry in its neighbor table when it finds a neighboring route. The software maintains the entry, indicating, among other information, the current state of the neighbor. The software updates the entry if the state of the neighbor router changes; for example, a secondary router became a primary router. The secondary router is the router that becomes the primary router when the primary router is no longer heard from.

For all neighboring routers, the **show smrp neighbor** command displays the address of the neighbor router, the state of the neighbor, its interface, the last time it was heard from, its route version number, and whether or not routes need to be sent to the neighbor. If the network address of a specific neighbor is given as a command parameter, this information is displayed for that neighbor router only.

Note Because SMRP is currently supported over AppleTalk networks only, sample output resulting from the **show smrp neighbor** command is the same as output from **show smrp neighbor appletalk** command.

Examples The following is sample output from the **show smrp neighbor** command that displays SMRP neighbor table entries for all neighbors:

```
Router# show smrp neighbor

SMRP Neighbor Table
                                    Last
Neighbor  State Interface    Heard
----------------------------------

20.3      (S)   Ethernet2    5
10.4      (N)   Ethernet1    3
11.5      (S)   Ethernet1    7
```

The following is sample output from the **show smrp neighbor** command with the **appletalk** keyword and the network address of a specific neighboring node:

```
Router# show smrp neighbor appletalk 20.3

SMRP Neighbor Table
                               Last
Neighbor  State Interface    Heard
----------------------------------

20.3      (S)   Ethernet2    5

Route version: 0x0000000E
Routes needed: False
```

Table 44 describes the fields shown in the display.

Table 44   show smrp neighbor Field Descriptions

Field	Description
Neighbor	Network address of the neighbor router.
State	State of the neighbor. Possible states are: • (P) —Primary operation • (S) —Secondary operation • (N) —Normal operation • PN.. —Primary negotiation • SN.. —Secondary negotiation • -D- —Down
Interface	Interface to the neighbor router.
Last Heard	Last time in seconds that the neighbor was heard from.
Route Version	Route version number of the neighbor. If the route version number is less than the neighbor's route version, then the route will be sent to that neighbor.
Routes Needed	True if routes need to be sent to the neighbor; False if not.

show smrp port

To display all entries or specific entries in the SMRP port table, use the **show smrp port** EXEC command.

show smrp port [**appletalk** [*type number*]]

Syntax Description

appletalk	(Optional) Displays SMRP port table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk networks only.
type	(Optional) Interface type.
number	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For all SMRP ports, the **show smrp port** command displays the interface of the SMRP port, the current state of the port, the network protocol type (currently only AppleTalk is supported) and its address, the address of the primary router on the local network, the address of the secondary router on the local network, the current groups on the port, and the last group on the port.

If the interface of a specific SMRP port is given, this information is displayed for that port only.

Note Because SMRP is currently supported over AppleTalk networks only, sample output resulting from the **show smrp port** command is the same as output from **show smrp port appletalk** command.

Examples

The following is sample output from the **show smrp port** command:

```
Router# show smrp port

SMRP Port Table
Interface     State Network       Type Address   Primary   Secondary
------------------------------------------------------------------

Ethernet2     (P)   20-22         AT   20.2      20.2      20.3
Ethernet3     (P)   30-33         AT   30.2      30.2      0.0
```

```
Ethernet4     (S)   40-44         AT   40.3    40.2     40.0
```

The following is sample output from the **show smrp port** command with the **appletalk** keyword and the interface of a specific port:

```
Router# show smrp port appletalk ethernet 2

SMRP Port Table
Interface      State Network        Type Address   Primary   Secondary
-----------------------------------------------------------------

Ethernet2     (P)   20-22          AT   20.2     20.2      20.3
Current groups:
Last group:
```

Table 45 describes the fields shown in the displays.

Table 45   show smrp port Field Descriptions

Field	Description
Interface	Interface of a specific SMRP port.
State	Current state of the port. Possible states are as follows: • (P) —Primary operation • (S) —Secondary operation • (N) —Normal operation • PN.. —Primary negotiation • SN.. —Secondary negotiation • -D- —Down
Network	Network range.
Type	Network protocol type. Currently only AppleTalk (AT) is supported.
Address	Network layer address.
Primary	Address of the primary SMRP router on the local network.
Secondary	Address of the secondary SMRP router on the local network.

Related Commands

Command	Description
test appletalk	Makes SMRP multicast services available over AppleTalk for a specific interface.

show smrp route

To display all entries or specific entries in the Simple Multicast Routing Protocol (SMRP) routing table, use the **show smrp route** EXEC command.

show smrp route [**appletalk** [*network*] | *type number*]

Syntax Description

appletalk	(Optional) Displays SMRP route table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk networks only.
network	(Optional) SMRP network range.
type	(Optional) Interface type.
number	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For all SMRP routes, the **show smrp route** command displays the number of SMRP routes in the internetwork. For each route, it shows the SMRP network range of the route, the version of the route, the elapsed time since the route was updated, the number of hops away the route is from the route's origin, the number of hops away the route is from the tunnel origin, the interface from which the route was received, and the router that sent the route.

If a specific network range is given, this information is displayed for that network range only.

If the interface is specified, the routes that came from this interface are displayed.

If the **appletalk** keyword is specified with or without an SMRP network range, the number of SMRP routes in the internetwork is not specified. Connected routes have a hop value of 0 and no address value.

Note Because SMRP is currently supported over AppleTalk networks only, sample output resulting from the **show smrp port** command is the same as output from **show smrp port appletalk** command.

Examples

The following is sample output from the **show smrp route** command:

```
Router# show smrp route
```

```
SMRP Route Table

5 routes in internet

Network        Hop Tunnel        Parent
                              Interface     Address
--------------------------------------------------------------

AT 1-1          1    0       Ethernet2    20.3
AT 10-11        1    0       Ethernet2    20.3
AT 20-22        0    0       Ethernet2
AT 40-44        0    0       Ethernet4
```

The following is sample output from the **show smrp route** command with the **appletalk** keyword and a specific SMRP network number within an SMRP network range:

```
Router# show smrp route appletalk 21

Network      Hop   Tunnel        Parent
                               Interface    Address
--------------------------------------------------------------

AT 20-22    0    0     Ethernet2    20.3

Route version: 0x0000000E
Elapsed update time: 00:23:55
```

The following is sample output from the **show smrp route** command for a specific interface:

```
Router# show smrp route appletalk ethernet 2

Network      Hop   Tunnel        Parent
                               Interface    Address
--------------------------------------------------------------

AT 1-1      1    0     Ethernet2    20.3
AT 10-11    1    0     Ethernet2    20.3
AT 20-22    0    0     Ethernet2
```

Table 46 describes the fields shown in the displays.

Table 46   show smrp route Field Descriptions

Field	Description
Network	SMRP network range (the route). "AT" indicates that this is an AppleTalk network.
Hop	Number of hops away from origin.
Tunnel	Number of hops away from the origin of this tunnel.
Parent Interface	Interface from which the route was received.
Parent Address	Address of the router that sent this route.
Route version	Version number of a route. If the route version is greater than the neighbor's route version, then the route will be sent to that neighbor.
Elapsed update time	Time elapsed since the route was last updated.

show smrp traffic

To display all entries or specific entries in the Simple Multicast Routing Protocol (SMRP) traffic table, use the **show smrp traffic** EXEC command.

show smrp traffic [**all** | **group** | **neighbor** | **port** | **route** | **transaction**]

Syntax Description

all	(Optional) Displays SMRP traffic for SMRP groups, neighbors, ports, routes, and transactions.
group	(Optional) Displays SMRP traffic for SMRP groups.
neighbor	(Optional) Displays SMRP traffic for neighbors.
port	(Optional) Displays SMRP traffic for ports.
route	(Optional) Displays SMRP traffic for routes.
transaction	(Optional) Displays SMRP traffic for transactions.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To display general SMRP statistics, use the **show smrp traffic** command without keywords. To display traffic for all of the categories defined by the keywords, use the **show smrp traffic all** command. To display traffic for a specific category, specify the command and the keyword for the category.

Examples

The following is sample output from the **show smrp traffic all** command:

```
Router# show smrp traffic all

SMRP statistics:
 Rcvd:  350 total, 99 hellos, 0 mc data, 0 fast handled
        78 requests, 127 confirms, 1 reject
        3 primaries, 6 secondaries
        7 notifies, 2 distance vectors
        3 create groups, 0 delete groups
        4 join groups, 0 leave groups
        54 members
        0 add group entries, 0 remove group entries
        0 locates, 0 tunnels
```

```
        Sent:  547 total, 307 hellos
               0 duplicate mc data, 0 mc data, 0 fast forwarded
               176 requests, 62 confirms, 2 rejects
               3 primaries, 3 secondaries
               6 notifies, 1 distance vector
               0 joins, 0 leaves
               42 creators, 81 members
               0 add group entries, 0 remove group entries
        Misc:  0 no buffers, 0 no forwards
               0 bad portids, 0 port downs
               0 bad versions, 0 runts
               0 bad packet types, 0 input errors

SMRP group statistics:
        Groups:  3 added, 0 removed,
        Forwards:  3 new, 1 recycled, 0 deleted
        Child Ports:  4 added, 1 freed,
        Misc: 0 range fulls, 0 not primary drops
                0 no routes

SMRP port statistics:
  Ports:  3 new, 0 recycled, 0 deleted

SMRP route statistics:
  Routes:  5 new, 0 recycled, 0 deleted
  Neighbor AT 20.3:
        1 received updates, 1 send updates
        3 received routes, 0 sent routes
        0 poisoned, 0 improved
        0 better parent interfaces, 0 worst parent interfaces
        0 better parent addresses, 0 worst parent addresses
        0 bad ranges, 0 overlaps

SMRP transaction statistics:
  Requests:  5 new, 135 recycled
        0 deleted, 0 freed
        9 timeouts, 36 resends
        0 duplicates, 0 incomplete duplicates
  Responses:  16 new, 62 recycled, 0 freed
        0 deleted, 0 freed
        0 unexpected, 0 bad
```

Table 47 describes the fields shown in the display.

Table 47   *show smrp traffic Field Descriptions*

Field	Description
SMRP Statistics:	
Rcvd:	
total	Total number of SMRP packets received.
hellos	Number of hello packets received from neighbors.
mc data	Number of packets of multicast data received.
fast handled	Number of input packets handled by the SMRP fast-switching function.
requests	Number of request transactions received from neighbors.
confirms	Number of confirm response transactions received.

Table 47　　　*show smrp traffic Field Descriptions (continued)*

Field	Description
reject	Number of reject response transactions received.
primaries	Number of primary request packets received.
secondaries	Number of secondary request packets received.
notifies	Number of notify packets received. A router sends a notify packet when it becomes an SMRP primary, secondary, or normal router. A router in normal operation mode can become a secondary router and a router in secondary operation mode can become a primary router.
distance vectors	Number of route update packets received.
create groups	Number of create group packets received from the creator endpoint when it requests to create a group.
delete groups	Number of delete group packets received. These packets are sent when a group is deleted.
join groups	Number of join-group packets received. These packets are sent when members join a group.
leave groups	Number of leave-group packets received. These packets are sent when members leave a group.
members	Number of member-request packets for polling group members received.
add group entries	Number of packets received to add group entries.
remove group entries	Number of packets received to remove group entries.
locates	Number of locate packets received. Endpoints send locate packets to find the SMRP router on the local network.
tunnels	Number of SMRP tunnel packets received.
Sent:	
total	Total number of SMRP packets sent.
hellos	Number of hello packets sent to neighbors.
duplicate mc data	Number of packets of multicast data duplicated and forwarded.
mc data	Number of packets of multicast data forwarded.
fast forwarded	Number of packets that were fast-switched out of the fast-switch enabled interface.
requests	Number of request transaction packets sent to neighbors.
confirms	Number of confirm responses sent.
rejects	Number of reject responses sent.
primaries	Number of primary request packets sent.
secondaries	Number of secondary request packets sent. These are sent in attempt to become the secondary router.

Table 47   show smrp traffic Field Descriptions (continued)

Field	Description
notifies	The number of notify packets sent. A router sends a notify packet when it becomes an SMRP primary, secondary, or normal router. A router in normal operation mode can become a secondary router and a router in secondary operation mode can become a primary router.
distance vectors	Number of route-update packets sent.
joins	Number of join-group packets sent. These packets are sent when members join a group.
leaves	Number of leave-group packets sent. These packets are sent when members leave a group.
creators	Number of creator-request packets sent to poll the creator endpoint to verify that it is still active.
members	Number of member request packets sent for polling group members.
add group entries	Number of packets sent to the secondary router to add group entries.
remove group entries	Number of packets sent to the secondary router to remove group entries.
Misc:	
no buffers	Number of times no system buffers available condition occurred. Memory allocation failure.
no forwards	Number of packets for which there was no entry in the forwarding table for the packet's destination.
bad portids	Number of packets with invalid port IDs.
port downs	Number of packets for ports that were down.
bad versions	Number of packets with the wrong SMRP protocol version number.
runts	Number of truncated packet.
bad packet types	Number of packets with invalid type field values.
input errors	Number of packets received that failed network layer packet validation.
SMRP group statistics:	
Groups:	
added	Number of groups added.
removed	Number of groups removed.
Forwards:	
new	Number of new entries created in the forwarding table.
recycled	Number of forwarding table entries that were recycled.
deleted	Number of forwarding table entries that were deleted.
Child Ports:	

Table 47   *show smrp traffic Field Descriptions (continued)*

Field	Description
added	Number of child ports added to the forwarding table entries.
freed	Number of child ports removed from the forwarding table entries.
Misc:	
range fulls	Number of times attempts were made to create SMRP groups after the range of available SMRP addresses was exhausted. The number of SMRP group addresses available equals the SMRP network range times 254.
not primary drops	Number of packets received and dropped because this router is not the SMRP primary router and, therefore, not responsible for the packets.
no routes	Number of times a route to the creator endpoint was not found in the routing table.
SMRP port statistics:	
Ports:	SMRP port traffic information
new	Number of new port entries added to the SMRP port table.
recycled	Number of recycled port entries added to the SMRP port table.
deleted	Number of port entries deleted from the SMRP port table.
SMRP route statistics:	
Routes:	Neighbor route statistics.
new	Number of new entries added to the SMRP routing table.
recycled	Number of recycled entries added to the SMRP routing table.
deleted	Number of entries deleted from the SMRP routing table.
Neighbor AT	AppleTalk neighbor information.
received updates	For each SMRP neighbor, the number of distance vector (routing update) packets received.
sent updates	For each SMRP neighbor, the number of distance vector (routing update) packets sent.
received routes	For each SMRP neighbor, the number of routes received.
sent routes	For each SMRP neighbor, the number of routes sent.
poisoned	Number of bad routes (with 255 hops) received in distance vector packets.
improved	Number of routes improved through updates received in distance vector packets.
better parent interfaces	Number of times the Cisco IOS software switches to a better parent interface when a tie condition exists. A tie exists when both routes have equal hop counts. A ties is broken by choosing the neighbor with the higher network address.

Table 47   show smrp traffic Field Descriptions (continued)

Field	Description
worst parent interfaces	Number of times the software does not switch interfaces in a tie condition. The software assesses a tie between two interfaces to choose the interface for the route when the hop count of both routes is equal. A tie is broken by choosing the neighbor with the higher network address.
better parent addresses	Number of times this software wins a tie to forward a packet when a tie condition exists. A tie condition occurs when two routers on the same local net have routes to the packet's destination with the same hop count. Whichever router has the highest network address wins and forwards the packet.
worst parent addresses	Number of times this software loses a tie to forward a packet when a tie condition exists. A tie condition occurs when two routers on the same local net have routes to the packet's destination with the same hop count. Whichever router has the highest network address wins and forwards the packet.
bad ranges	Number of times an invalid SMRP network range was received.
overlaps	Number of times an incoming SMRP network range overlapped with an existing SMRP routing entry.
SMRP transaction statistics:	
Requests:	
new	Number of new requests created.
recycled	Number of recycled requests.
deleted	Number of times data was allocated for requests.
freed	Number of times deleted requests are freed.
timeouts	Number of times requests timed out.
resends	Number of times requests were resent.
duplicates	Number of times a processed request arrived.
incomplete duplicates	Number of times requests were received while in incomplete state.
Responses:	
new	Number of new responses created.
recycled	Number of recycled responses.
freed	Number of freed responses.
deleted	Number of times data was allocated for responses.
freed	Number of times deleted responses are freed.
unexpected	Number of unexpected responses.
bad	Number of bad responses.

smrp mroute-cache protocol appletalk

To enable Simple Multicast Routing Protocol (SMRP) fast-switching on a port, use the **smrp mroute-cache protocol appletalk** interface configuration command. To disable SMRP fast-switching, use the **no** form of this command.

> **smrp mroute-cache protocol appletalk**

> **no smrp mroute-cache protocol appletalk**

Syntax Description   This command has no arguments or keywords.

Defaults   Enabled

Command Modes   Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   By default, fast-switching is enabled on all SMRP ports. A network protocol and interface comprise an SMRP port. Fast switching improves the throughput rate by processing incoming packets more quickly than process switching.

SMRP uses the forwarding table to forward packets for a particular SMRP group. For each group, the forwarding table lists the parent interface and address and one or more child interfaces and addresses. When data for an SMRP group arrives on the parent interface, the router forwards it to each child interface. The SMRP fast-switching cache table specifies whether to fast switch SMRP data packets out the interfaces specified by the forwarding table.

SMRP fast switching requires that:

- A parent port is fast-switch enabled.

- One or more child ports are fast-switch enabled.

When the parent port is fast-switch enabled, the system populates and validates a fast-switching cache table when forwarding packets out child ports.

To populate the fast-switching cache table with fast-switching information, the first packets are process switched. Thus, the fast-switching cache table is populated with information about fast-switch enabled child ports. When succeeding packets arrive, the system uses the SMRP fast-switching cache table to fast switch the packets out those child ports.

If there are non-fast-switching ports in the forwarding table, then the system process switches the packet out those ports.

To validate the fast-switching cache table, the system validates each cache entry when it forwards the first packet out all child ports. If a cache entry is validated, the router can use the entry to fast switch succeeding packets out the child ports.

If a cache entry is invalidated, the router cannot use the entry to fast switch packets. The entry is removed from the fast-switching cache table and the router process switches packets out the child ports. A cache entry is invalidated when one of these conditions is met:

- A child endpoint leaves the SMRP group.

- A new child endpoint joins the SMRP group.

- A port's fast-switching configuration is enabled or disabled.

- A port is restarted.

Examples   The following example disables SMRP fast-switching:

```
no smrp mroute-cache protocol appletalk
```

smrp protocol appletalk

To make Simple Multicast Routing Protocol (SMRP) multicast services available over AppleTalk for a specific interface, use the **smrp protocol appletalk** interface configuration command. To disable SMRP over AppleTalk for a specific interface, use the **no** form of this command.

smrp protocol appletalk [**network-range** *beginning-end*]

no smrp protocol appletalk [**network-range** *beginning-end*]

Syntax Description

network-range	(Optional) SMRP network range for the interface. We recommend that you do not specify an SMRP network range. When you omit the range, the Cisco IOS software uses the AppleTalk cable range configured for the interface as the SMRP network range. If you specify a range, it must fall within the SMRP network range 1 to 65,535.
beginning-end	(Optional) The beginning and end of the SMRP network range for this AppleTalk network. If you specify a range, it must fall within the SMRP network range 1 to 65,535.

Defaults

SMRP is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SMRP supports point-to-multipoint multicasting of packets for AppleTalk networks. This support provides the capability of sending data from a single source to multiple stations without having to send duplicate copies of the data.

The **smrp protocol appletalk** command configures SMRP support over an AppleTalk network on an interface basis. Before you use this command, you must issue the **smrp routing** command to enable SMRP. After you enable SMRP, you can use this command to make SMRP services available over AppleTalk for any number of individual interfaces.

We recommend that you do not specify an SMRP network range for the AppleTalk network. Because the upper limit of the AppleTalk network range is 65,535, AppleTalk network numbers always fit within the SMRP network range; SMRP network numbers are 3 bytes long, whereas AppleTalk network numbers

are 2 bytes long. If the AppleTalk network is a nonextended network, which is defined by a single network number, the AppleTalk network is mapped to the SMRP network range using the single number to define both ends of the range (for example, 65,520-65,520).

To disable SMRP services for a specific AppleTalk network, use the **no** form of this command. To disable SMRP services globally (that is, for all AppleTalk networks whose interfaces you have configured for SMRP support) issue the **no smrp routing** command.

Examples

The following example enables SMRP globally and turns on SMRP support over AppleTalk for the current interface:

```
smrp routing
interface ethernet 0
 smrp protocol appletalk
```

The following example disables SMRP over AppleTalk for the current interface:

```
interface ethernet 0
 no smrp protocol appletalk
```

Related Commands

Command	Description
show smrp port	Displays all entries or specific entries in the SMRP port table.
test appletalk	Enables the use of the multicast transport services provided by the SMRP.

smrp routing

To enable the use of the multicast transport services provided by the Simple Multicast Routing Protocol (SMRP), use the **smrp routing** global configuration command. To disable SMRP services for all interfaces, use the **no** form of this command.

smrp routing

no smrp routing

Syntax Description   This command has no arguments or keywords.

Defaults   SMRP is disabled.

Command Modes   Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Currently, SMRP services are supported over AppleTalk only. The **smrp routing** command enables the use of SMRP. To enable SMRP for an AppleTalk network over a specific interface, you must use the **smrp protocol appletalk** interface configuration command after you issue this command. The **smrp routing** command has no effect until you enable SMRP at the interface level.

Examples   The following example enables SMRP:

```
smrp routing
```

The following example disables SMRP:

```
no smrp routing
```

Related Commands

Command	Description
test appletalk	Makes SMRP multicast services available over AppleTalk for a specific interface.

test appletalk

To enter the test mode, use the **test appletalk** command in privileged EXEC mode.

> **test appletalk**

Syntax Description   This command has no arguments or keywords.

Command Modes   Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   Use the **test appletalk** command to enter test mode. From test mode you can test the Name Binding Protocol (NBP) protocol.

The following display shows how to enter Appletalk test mode:

```
Router# test appletalk
Router(atalk test)#
```

Type **?** to display the following list of test options:

```
Router(atalk test)# ?
end    Exit AppleTalk test mode
nbp    AppleTalk NBP test commands
```

Use the **test appletalk** command with the **nbp** options to test and to perform informational lookups of NBP-registered entities. Use the NBP options when you find that AppleTalk zones are listed in the Chooser, but services in these zones are unavailable.

Type **nbp ?** to learn what NBP test commands you can use:

```
Router(atalk test)# nbp ?
nbp confirm:       send out an NBP confirm packet to the specified entity
nbp lookup:        lookup an NVE. prompt for name, type and zone
nbp parameters:    display/change lookup parms (ntimes, ncecs, interval)
nbp poll:          for every zone, lookup all devices, using default
?:                  print command list
end:               exit nbptest
```

The following list summarizes the **nbp** test commands you can use:

- **nbp confirm**—Sends out an NBP confirm packet to the specified entity.

- **nbp lookup**—Searches for NBP entities in a specific zone.

- **nbp parameters**—Sets the parameters used in subsequent lookup and pool tests.

- **nbp poll**—Searches for all devices in all zones.
- **?**—Displays the list of **nbp** tests.
- **end**—Exit from the **nbp** test commands.

The remainder of this section shows and explains the syntax and output of the various NBP test commands.

When running any of the NBP tests, you specify a nonprinting character by entering a three-character string that is the hexadecimal equivalent of the character. For example, type **:c5** to specify the test appletalk truncation wildcard.

This is the syntax of the **nbp confirm** command:

nbp confirm *appletalk-address* [**:***skt*] *object***:***type***@***zone*

The syntax description is as follows:

appletalk-address	AppleTalk network address in the form *network.node*. The argument *network* is the 16-bit network number in the range 1 to 65,279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.
:*skt*	(Optional) Name of socket.
*object***:***type*	Name of device and the type of service. The colon (**:**) between *object* and *type* is required.
@*zone*	Name of the AppleTalk zone where the entity *object***:***type* resides.

Examples

The following is sample output from the **nbp confirm** command. In this example, the test sends a confirm packet to the entity *ciscoRouter* in zone *Engineering*.

```
Router(atalk test)# nbp confirm 24279.173 my-mac:AFPServer@Engineering

confirmed my-mac:AFPServer@Engineering at 24279n,173a,250s
```

This is the syntax of the **nbp lookup** command:

nbp lookup *object***:***type***@***zone*

The syntax description is as follows:

*object***:***type*	Name of device and the type of service. The colon (**:**) between *object* and *type* is required.
@*zone*	Name of the AppleTalk zone where the entity *object***:***type* resides.

The following is sample output from the **nbp lookup** command:

```
Router(atalk test)# nbp lookup =:macintosh:c5@engineering

(100n,50a,253s)[1]: 'userA:Macintosh IIcx@engineering'
(100n,16a,251s)[1]: 'userB:Macintosh II@engineering'
(200n,24a,253s)[1]: 'userC:Macintosh IIci@engineering'
(200n,36a,251s)[1]: 'userD:Macintosh II@engineering'
(300n,21a,252s)[1]: 'userE:Macintosh SE/30@engineering'
```

```
test appletalk lookup request timed out
Processed 6 replies, 7 events
```

Table 48 describes the fields shown in the display.

Table 48   nbp lookup Field Descriptions

Field	Description
(100n,50a,253s) [1]	AppleTalk DDP address of the registered entity, in the format network, node address, and socket number. The number in brackets is either the current value of the field (if this is the first time you have invoked **nbptest**) or the value the field had the last time you invoked **nbptest**.
'userA:Macintosh IIcx@engineering'	NBP enumerator:NBP entity string of the registered entity.
test appletalk lookup request timed out	Indicates whether replies were heard within the timeout interval.
Processed 6 replies, 7 events	Number of NBP replies received.

This is the syntax of the **nbp parameters** command:

> **nbp parameters** *retransmissions replies interval*

The syntax description is as follows:

retransmissions	Maximum number of lookup retransmissions. This is a number from 1 to 5. The default value is 5.
replies	Maximum number of replies to accept for each lookup. This is a number from 1 to 500. The default is 1.
interval	Interval, in seconds, between each retry. This value is from 1 to 60 seconds. The default is 5 seconds.

The following is sample output of the **nbp parameters** command. In this example, the maximum number of retransmission is 1, the maximum number of replies is 100, and there are 10 seconds between each retry.

```
Router(atalk test)# nbp parameters 1 100 10
```

The **nbp poll** command has no keywords or arguments. The following is sample output from the **nbp poll** command:

```
Router(atalk test)# nbp poll

poll: sent 2 lookups
(100n,82a,252s)[1]: 'userA:Macintosh IIci@Zone one'
(200n,75a,254s)[1]: 'userB:Macintosh IIcx@Zone two'
test appletalk polling completed.
Processed 2 replies, 2 events
```

Table 49 describes the fields shown in the display.

Table 49   nbp poll Field Descriptions

Field	Description
poll	Number of lookups the command sent.
(100n,82,252s) [1]	AppleTalk DDP address of the registered entity, in the format network, node address, and socket number. The number in brackets is either the current value of the field (if this is the first time you have invoked **nbptest**) or the value the field had the last time you invoked **nbptest**.
'userA:Macintosh IIci@Zone one'	NBP enumerator:NBP entity string of the registered entity.
test appletalk polling completed.	Indicates that the polling completed successfully.
Processed 2 replies, 2 events	Number of NBP replies received.

The following example enables the **appletalk nbp polling** command, which does not use any keywords or arguments:

```
Router (atalk test)# nbp poll
```

Related Commands

Command	Description
test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
test interfaces	Tests the system interfaces on the modular router.
test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

■ **test appletalk**