CHAPTER 12

AppleTalk Commands

AppleTalk is a local-area network system that was designed and developed by Apple Computer, Inc. It can run over Ethernet, Token Ring, and FDDI networks, and over Apple's proprietary twisted-pair media access system (LocalTalk). 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 Fiber Distributed Data Interface).

Use the commands in this chapter to configure and monitor AppleTalk networks. For AppleTalk configuration information and examples, refer to the "AppleTalk Commands" chapter of the *Router Products 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** global configuration command.

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

Default

To deny other access

Command Mode

Global configuration

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 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).

Example

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

access-list cable-range
access-list includes
access-list network
access-list other-access
access-list within
access-list zones
appletalk access-group
appletalk distribute-list in

appletalk distribute-list out
appletalk getzonelist-filter
appletalk permit-partial-zones

access-list cable-range

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

access-list *access-list-number* {**deny** | **permit**} **cable-range** *start-end*
no access-list *access-list-number* {**deny** | **permit**} **cable-range** *start-end*

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.
start-end	Cable range value. The *start* argument specifies the beginning of the cable range, and the *end* argument specifies the end of the range. These arguments are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number.

Default

None

Command Mode

Global configuration

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**). 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** *start-end*

Example

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

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

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

access-list additional-zones
access-list network
access-list includes
access-list other-access
access-list within
access-list zone
appletalk access-group
appletalk distribute-list in
appletalk distribute-list out
appletalk getzonelist-filter
priority-list protocol †

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** global configuration command. To remove an access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **includes** *start-end*
no access-list *access-list-number* {**deny** | **permit**} **includes** *start-end*

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.
start-end	Cable range or network number. The *start* argument specifies the beginning of the cable range, and the *end* argument specifies the end of the range. These arguments 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.

Default

None

Command Mode

Global configuration

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**). 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** *start-end*

Example

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

A dagger (†) indicates that the command is documented in another chapter.

access-list additional-zones
access-list cable-range
access-list network
access-list other-access
access-list within
access-list zone
appletalk access-group
appletalk distribute-list in
appletalk distribute-list out
appletalk getzonelist-filter
priority-list protocol †

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** global configuration command. To remove an access list, use the **no** form of this command.

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

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.

Default

None

Command Mode

Global configuration

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 a 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**). 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**} *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 *list* number 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*

Example

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

A dagger (†) indicates that the command is documented in another chapter.

access-list additional-zones
access-list cable-range
access-list includes
access-list other-access
access-list within
access-list zone
appletalk access-group
appletalk distribute-list in
appletalk distribute-list out
appletalk getzonelist-filter
priority-list protocol †

access-list other-access

To define the default action to take for access checks that apply to networks or cable ranges, use the **access-list other-access** global configuration command.

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

Default

To deny other access

Command Mode

Global configuration

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**). 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.

Example

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

A dagger (†) indicates that the command is documented in another chapter.

access-list additional-zones
access-list cable-range
access-list includes
access-list network
access-list within
access-list zone
appletalk access-group
appletalk distribute-list in
appletalk distribute-list out
priority-list protocol †

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** global configuration command. To remove this access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **within** *start-end*
no access-list *access-list-number* {**deny** | **permit**} **within** *start-end*

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.
start-end	Cable range or network number. The *start* argument specifies the beginning of the cable range, and the *end* argument specifies the end of the range. These arguments 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.

Default

None

Command Mode

Global configuration

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** *start-end*

Example

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

A dagger (†) indicates that the command is documented in another chapter.

access-list additional-zones
access-list cable-range
access-list includes
access-list network
access-list other-access
access-list zone
appletalk access-group
appletalk distribute-list in
appletalk distribute-list out
appletalk getzonelist-filter
priority-list protocol †

access-list zone

To define an AppleTalk access list that applies to a zone, use the **access-list zone** global configuration command. 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.

Default

None

Command Mode

Global configuration

Usage Guidelines

You apply access lists defined with the **access-list zones** 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.

Example

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

access-list additional-zones
access-list cable-range
access-list includes
access-list network
access-list other-access
access-list within
appletalk access-group
appletalk distribute-list in
appletalk distribute-list out
appletalk getzonelist-filter
appletalk permit-partial-zones

appletalk access-group

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

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

Syntax Description

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

Default

None

Command Mode

Interface configuration

Usage Guidelines

The **appletalk access-group** command applies data-packets filter to an interface. These filters check data packets being sent out an interface. If the packets' source network has access denied, these packets are not transmitted but rather are discarded.

Data-packet filters use access lists that define conditions for networks and cable ranges only. They ignore any zone information that may be in the access list.

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.

Example

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

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

Related Commands

access-list cable-range
access-list includes
access-list network
access-list other-access
access-list within
appletalk distribute-list in
appletalk distribute-list out

appletalk address

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

appletalk address *network.node*
no appletalk address

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.

Default

Disabled

Command Mode

Interface configuration

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 router 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.

Example

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

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

Related Commands

appletalk cable-range
appletalk discovery
appletalk zone

appletalk alternate-addressing

To display network numbers in a two-octet format, use the **appletalk alternate-addressing** global configuration command. 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.

Default

Disabled

Command Mode

Global configuration

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.

Example

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 the retransmission of ARP packets, use the **appletalk arp interval** global configuration command. To restore both default intervals, use the **no** form of this command.

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

Syntax Description

probe	(Optional.) Indicates that the interval specified is to be used with AARP requests that are trying to determined the address of the local router when the router 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 AppleTalk ARP transmissions. The minimum value is 33 milliseconds.

Default

If you omit **probe** and **request**, **probe** is the default.

probe—200 milliseconds
request—1000 milliseconds

Command Mode

Global configuration

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 router 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** command restores both the **probe** and **request** intervals specified in the **appletalk arp interval** and **appletalk arp retransmit-count** commands to their default values.

Example

In the following example, the AppleTalk ARP retry interval is lengthened to 2000 milliseconds:

```
appletalk arp request interval 2000
```

Related Commands

appletalk arp retransmit-count
appletalk arp-timeout
appletalk glean-packets
show appletalk global

appletalk arp retransmit-count

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

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

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 router 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. With the **probe** keyword, the default value is 10 retransmissions. With the **request** keyword, the default value is 5 retransmissions. Specifying 0 selects the default value.

Default

If you omit **probe** and **request**, **probe** is the default.

probe—10
request—5

Command Mode

Global configuration

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 router 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** command restores both the **probe** and **request** intervals specified in the **appletalk arp interval** and **appletalk arp retransmit-count** commands to their default values.

Example

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

appletalk arp interval
appletalk arp-timeout
appletalk glean-packets
show appletalk global

appletalk arp-timeout

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

appletalk arp-timeout *interval*
no appletalk arp-timeout

Syntax Description

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

Default

240 minutes (4 hours)

Command Mode

Interface configuration

Example

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

appletalk arp interval
appletalk arp retransmit-count
appletalk glean-packets

appletalk cable-range

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

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

Syntax Description

start-end	Cable range value. The *start* argument specifies the beginning of the cable range, and the *end* argument specifies the end of the range. These arguments are decimal number 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. The suggested network number must fall within the specified range of network numbers.

Default

Disabled

Command Mode

Interface configuration

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 router attempts to determine cable range 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.

Example

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

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

Related Commands

appletalk address
appletalk discovery
appletalk zone

appletalk checksum

To enable the generation and verification of checksums for all AppleTalk packets (except routed packets), use the **appletalk checksum** global configuration command. 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.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

When the **appletalk checksum** command is enabled, the router discards incoming DDP packets when the checksum is nonzero 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.

Our routers do not check checksums on routed packets, thereby eliminating the need to disable checksum to allow operation of some networking applications.

Example

The following example disables the generation and verification of checksums:

```
no appletalk checksum
```

Related Command

show appletalk global

appletalk discovery

To place an interface into discovery mode, use the **appletalk discovery** interface configuration command. 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.

Default

Disabled

Command Mode

Interface configuration

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, then when the router is starting 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 up.

If you do not enable discovery mode, then when the router is starting up, the interface must acquire its configuration from memory. If the stored configuration is not complete, the interface will not start up. 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 up. If there are no neighboring operational routers, the router will assume the interface's stored configuration is correct and will start up.

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 up.

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 also can 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 **appletalk 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 **write memory** EXEC command.

Example

The following example enables discovery mode on Ethernet interface 0:

```
interface ethernet 0
appletalk discovery
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

appletalk address
appletalk cable-range
appletalk zone
show appletalk interface
write memory †

appletalk distribute-list in

To filter routing updates received from other routers over a specified interface, use the **appletalk distribute-list in** interface configuration command. 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.
in	Indicates that the filter applies to updates received by the router.

Default

None

Command Mode

Interface configuration

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 router's AppleTalk routing table.

Example

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

access-list cable-range
access-list includes
access-list network

access-list other-access
access-list within
appletalk distribute-list out

appletalk distribute-list out

To filter routing updates transmitted to other routers, use the **appletalk distribute-list out** interface configuration command. 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.
out	Indicates that the filter applies to updates transmitted by the router.

Default

None

Command Mode

Interface configuration

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 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 ZIP GetZoneList 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.

Example

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

access-list additional-zones
access-list zones
appletalk distribute-list in
appletalk getzonelist-filter
appletalk permit-partial zones

appletalk event-logging

To log significant network events, use the **appletalk event-logging** global configuration command. 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.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

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

Example

The following example shows the use of the **appletalk event-logging** command:

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

Related Command

show appletalk global

appletalk free-trade-zone

To establish a free-trade zone, use the **appletalk free-trade-zone** interface configuration command. 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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

A free-trade zone is a part of an AppleTalk internet that is accessible by two other parts of the internet, 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 internets 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.

Example

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** interface configuration command. To remove this filter, use the **no** form of this command.

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

Syntax Description

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

Default

None

Command Mode

Interface configuration

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 internetwork filter GZL reply identically. Otherwise, the Chooser will list different zone 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 other vendors' routers 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 need to 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.

Example

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

access-list additional-zones
access-list zone
appletalk distribute-list out
appletalk permit-partial-zones

appletalk glean-packets

To derive AARP table entries from incoming packets, use the **appletalk glean-packets** interface configuration command. 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.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

The router automatically derives AARP table entries from incoming packets. This process is referred to as "gleaning." Gleaning speeds up the process of populating the AARP table.

Example

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 a router to start functioning even if the network is misconfigured, use the **appletalk ignore-verify-errors** global configuration command. 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.

Default

Disabled

Command Mode

Global configuration

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.

appletalk iptalk

To enable IPTalk encapsulation on an interface that already has a configured IP address, use the **appletalk iptalk** interface configuration command. To disable IPTalk encapsulation, use the **no** form of this command.

appletalk iptalk *network.node zone*
no appletalk iptalk

Syntax Description

network.node	AppleTalk network address assigned to 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.
zone	Name of the zone for the connected AppleTalk network.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Use the **appletalk iptalk** interface subcommand to enable IPTalk encapsulation on an interface that already has a configured IP address. This command encapsulates AppleTalk in IP packets in a manner compatible with the Columbia AppleTalk Package (CAP) IPTalk and the Kinetics IPTalk (KIP) implementations.

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 KIP (Kinetics IP) 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, because 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 router 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.

Example

The following example configuration illustrates how to configure IPTalk:

```
interface Ethernet 0
ip address 131.108.1.118 255.255.255.0
appletalk address 20.129
appletalk zone Native AppleTalk
appletalk iptalk 30.0 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 Command

appletalk iptalk-baseport

appletalk iptalk-baseport

To specify the UDP port number when configuring IPTalk, use the **appletalk iptalk-baseport** global configuration command. To return to the default UDP port number, use the **no** form of this command.

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

Syntax Description

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

Default

768

Command Mode

Global configuration

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 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.

Example

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 131.108.1.118 255.255.255.0
appletalk address 20.129
appletalk zone Native AppleTalk
appletalk iptalk 30.0 UDPZone
```

Related Command

appletalk iptalk

appletalk lookup-type

To specify which NBP service types are retained in the name cache, use the **appletalk lookup-type** global configuration command. 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 1-1 in the "Usage Guidelines" section.

Default

Retain ciscoRouter entries in name cache

Command Mode

Global configuration

Usage Guidelines

You can issue multiple **appletalk lookup-type** commands. The router 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 1-1 lists some AppleTalk service types.

Table 1-1 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
SNMP Agent	Active SNMP agents in Cisco routers
Services for Other Vendors' Routers	
AppleRouter	Apple internet 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 entries 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 routers 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 router or is running our software that is earlier than Release 9.0, it is possible the router 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 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.

Example

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

```
appletalk lookup GatorBox
appletalk lookup AppleRouter
appletalk lookup IPGATEWAY
appletalk lookup Workstation
```

Related Commands

appletalk name-lookup-interval
show appletalk name-cache
show appletalk nbp

appletalk macip dynamic

To allocate IP addresses to dynamic MacIP clients, use the **appletalk macip dynamic** global configuration command. 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 the Apple Computer, Inc. specification *Inside AppleTalk*.

Default

None

Command Mode

Global configuration

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*

Example

The following example illustrates MacIP support for dynamically addressed MacIP clients with IP addresses in the range 131.108.1.28 to 131.108.1.44.

```
!This global statement specifies the MacIP server address and zone:
appletalk macip server 131.108.1.27 zone Engineering
!
!This global statement identifies the dynamically addressed clients:
appletalk macip dynamic 131.108.1.28 131.108.1.44 zone Engineering
!
!These statements assign the IP address and subnet mask for Ethernet interface 0:
interface ethernet 0
ip address 131.108.1.27 255.255.255.0
!
!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

A dagger (†) indicates that the command is documented in another chapter.

appletalk macip server
appletalk macip static
ip address †
show appletalk macip-servers

appletalk macip server

To establish a MacIP server for a zone, use the **appletalk macip server** global configuration command. 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 the Apple Computer, Inc. specification *Inside AppleTalk*.

Default

None

Command Mode

Global configuration

Usage Guidelines

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

You can configure only one MacIP server per AppleTalk 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*

Example

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 the router and the Ethernet interface.

```
appletalk macip server 131.108.1.27 zone Engineering
ip address 131.108.1.27 255.255.255.0
appletalk routing
interface ethernet 0
appletalk cable-range 69-69 69.128
appletalk zone Engineering
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

appletalk macip dynamic
appletalk macip static
ip address †
show appletalk macip-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** global configuration command. 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, Inc. specification *Inside AppleTalk*.

Default

None

Command Mode

Global configuration

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*

Example

The following example illustrates MacIP support for MacIP clients with statically allocated IP addresses. The IP addresses range is from 131.108.1.50 to 131.108.1.66. The three nodes that have the specific addresses are 131.108.1.81, 131.108.1.92, and 131.108.1.101.

```
!This global statement specifies the MacIP server address and zone:
appletalk macip server 131.108.1.27 zone Engineering
!
!These global statements identify the statically addressed clients:
appletalk macip static 131.108.1.50 131.108.1.66 zone Engineering
appletalk macip static 131.108.1.81 zone Engineering
appletalk macip static 131.108.1.92 zone Engineering
appletalk macip static 131.108.1.101 zone Engineering
!
!These statements assign the IP address and subnet mask for Ethernet interface 0:
interface ethernet 0
ip address 131.108.1.27 255.255.255.0
!
!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

A dagger (†) indicates that the command is documented in another chapter.

appletalk macip dynamic
appletalk macip server
ip address †
show appletalk macip-servers

appletalk name-lookup-interval

To set the interval between service pollings by the router on its AppleTalk interfaces, use the **appletalk name-lookup-interval** global configuration command. 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

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.

Default

0

Command Mode

Global configuration

Usage Guidelines

The router 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 re-enter a nonzero value, the configuration specified by the **appletalk lookup-type** command is reinstated. You cannot disable the lookup of ciscoRouter.

Example

The following example sets the lookup interval to 20 minutes:

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

Related Commands

appletalk lookup-type
show appletalk name-cache

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** global command. To return to the default behavior, which is 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.

Default

Disabled

Command Mode

Global configuration

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 software Release 8.3.

Example

The following example allows partial zones:

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

Related Commands

access-list additional zones
access-list zone
appletalk distribute-list out
appletalk getzonelist-filter

appletalk pre-fdditalk

To enable the recognition of pre-FDDITalk packets, use the **appletalk pre-fdditalk** interface configuration command. 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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

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

Example

The following example enables the recognition of pre-FDDITalk packets:

```
appletalk pre-fdditalk
```

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** global configuration command. To delete the proxy, use the **no** form of this command.

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

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 router as if it were a real network number.
zone-name	Name of the zone that contains the routers 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.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

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

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 need to 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.

Example

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

```
appletalk proxy 60 Twilight
```

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** global configuration command. To disable this option and allow the router 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.

Default

Enabled

Command Mode

Global configuration

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 router behavior compatible with software 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 router 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.

Example

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** interface configuration command. 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.

Default

Enabled on all interfaces that support fast switching

Command Mode

Interface configuration

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.

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.

For serial lines, fast switching is supported on extended serial lines with HDLC encapsulation only. It is not supported on nonextended serial lines.

Example

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 Command

show appletalk cache

appletalk routing

To enable AppleTalk routing, use the **appletalk routing** global configuration command. 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.

Default

Disabled

Command Mode

Global configuration

Example

The following example enables AppleTalk protocol processing on the router:

```
appletalk routing
```

Related Commands

appletalk address
appletalk cable-range
appletalk zone

appletalk send-rtmps

To allow a router to send routing updates to its neighbors, use the **appletalk send-rtmps** interface configuration command. 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.

Default

Send routing updates

Command Mode

Interface configuration

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.

Example

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

```
no appletalk send-rtmps
```

Related Commands

appletalk require-route-zones
appletalk strict-rtmp-checking
appletalk timers

appletalk strict-rtmp-checking

To perform maximum checking of routing updates to ensure their validity, use the **appletalk strict-rtmp-checking** global configuration command. 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.

Default

Provide maximum checking

Command Mode

Global configuration

Usage Guidelines

Strict 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 by the router are not discarded.

Example

The following example disables strict checking of RTMP routing updates:

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

Related Commands

appletalk require-route-zones
appletalk send-rtmps
appletalk timers

appletalk timers

To change the routing update timers, use the **appletalk timers** global configuration command. 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 router 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).

Default

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

Command Mode

Global configuration

Usage Guidelines

Routes older than the time specified by *update-interval* are considered suspect. Once the period of time specified by *valid-interval* 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 *invalid-interval* period, 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 our router’s 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 router 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.

Example

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

```
appletalk timers 20 40 60
```

appletalk zip-query-interval

To specify the interval at which the router sends ZIP queries, use the **appletalk zip-query-interval** global configuration command. 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 router sends ZIP queries. It can be any positive integer. The default is 10 seconds.

Default

10 seconds

Command Mode

Global configuration

Usage Guidelines

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

Example

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

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

appletalk zone

To set the zone name for the connected AppleTalk network, use the **appletalk zone** interface configuration command. 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.

Default

None

Command Mode

Interface configuration

Usage Guidelines

If discovery mode is not enabled, you can specify this 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 router 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•Zone*.

```
appletalk zone Cisco:A5Zone
```

Related Commands

appletalk address
appletalk cable-range
show appletalk zone

clear appletalk arp

To delete all the entries from the AppleTalk ARP (AARP) table, use the **clear appletalk arp** EXEC command.

clear appletalk arp [*network.node*]

Syntax Description

no argument	Deletes all entries from the router's AARP table.
network.node	AppleTalk network address to be deleted from the router's AARP table. 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.

Command Mode

EXEC

Example

The following example deletes all entries from the router's AARP table:

```
clear appletalk arp
```

Related Command

show appletalk arp

clear appletalk neighbor

To delete entries from the neighbor table, use the clear appletalk neighbor EXEC command.

clear appletalk neighbor [*neighbor-address*]

Syntax Description

no argument	Deletes all entries from the neighbor table.
neighbor-address	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 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

Command Mode

EXEC

Usage Guidelines

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

Example

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

```
clear appletalk neighbor 1.129
```

Related Command

show appletalk neighbors

clear appletalk route

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

clear appletalk route [*network*]

Syntax Description

no argument	Deletes all routes from the routing table.
network	Number of the network the route is to.

Command Mode

EXEC

Example

The following example deletes the route to network 1:

```
clear appletalk route 1
```

Related Command

show appletalk route

clear appletalk zone

To delete entries from the zone name table, use the **clear appletalk zone** EXEC command.

clear appletalk zone [*zone-name*]

Syntax Description

no argument	Deletes all entries from the zone table.
zone-name	Name of the zone to be deleted from the zone table.

Command Mode

EXEC

Example

The following example deletes the zone name Boojum from the zone table:

```
clear appletalk zone Boojum
```

Related Commands

appletalk zone
show appletalk zone

ping (user)

To check host reachability and network connectivity, use the **ping** EXEC command.

ping appletalk *network.node*

Syntax Description

appletalk	Specifies the AppleTalk protocol.
network.node	AppleTalk address of the system to ping.

Command Mode

EXEC

Usage Guidelines

The user **ping** (packet internet groper function) command provides a basic ping facility for users who do not have system privileges. This command is equivalent to the nonverbose form of the privileged **ping** command. It sends five 100-byte ping packets. The **ping** command sends Apple Echo Protocol (AEP) datagrams to other AppleTalk nodes to verify connectivity and measure round-trip times.

Only an interface that supports *HearSelf* can respond to packets generated at a local console and directed to an interface on the same router. Our routers support only *HearSelf* on Ethernet.

If the system cannot map an address for a host name, it will return an "%Unrecognized host or address" error message.

To abort a **ping** session, type the escape sequence. By default, this is Ctrl-^ X. You enter this by simultaneously pressing the Ctrl, Shift, and 6 keys, letting go, and then pressing the X key.

Table 1-2 describes the test characters displayed in **ping** responses.

Table 1-2 AppleTalk Ping Characters

Character	Meaning
!	Each exclamation point indicates the receipt of a reply from the target address.
.	Each period indicates the network server timed out while waiting for a reply from the target address.
B	A bad or malformed echo was received from the target address.
C	An echo with a bad DDP checksum was received.
E	Transmission of an echo packet to the target address failed.
R	Transmission of the echo packet to the target address failed due to lack of a route to the target address.

Sample Display

The following display shows input to and output from the user **ping** command.

```
router> ping appletalk 1024.128
Type escape sequence to abort.
Sending 5, 100-byte AppleTalk Echoes to 1024.128, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 4/4/8 ms
```

Related Command

ping (privileged)

ping (privileged)

To check host reachability and network connectivity, use the **ping** privileged EXEC command.

ping [**appletalk**] [*network.node*]

Syntax Description

appletalk	Specifies the AppleTalk protocol.
network.node	AppleTalk address of the system to ping.

Type

Privileged EXEC

Usage Guidelines

The privileged **ping** (packet internet groper function) command provides a complete **ping** facility for users who have system privileges. The **ping** command sends Apple Echo Protocol (AEP) datagrams to other AppleTalk nodes to verify connectivity and measure round-trip times.

Only an interface that supports *HearSelf* can respond to packets generated at a local console and directed to an interface on the same router. Our routers only support *HearSelf* on Ethernet.

If the system cannot map an address for a host name, it will return an "%Unrecognized host or address" error message.

To abort a **ping** session, type the escape sequence. By default, this is Ctrl-^ X. You enter this by simultaneously pressing the Ctrl, Shift, and 6 keys, letting go, and then pressing the X key.

Table 1-3 describes the test characters displayed in **ping** responses.

Table 1-3 AppleTalk Ping Characters

Character	Meaning
!	Each exclamation point indicates the receipt of a reply (echo) from the target address.
.	Each period indicates the network server timed out while waiting for a reply from the target address.
B	The echo received from the target address was bad or malformed.
C	An echo with a bad DDP checksum was received.
E	Transmission of an echo packet to the target address failed.
R	Transmission of the echo packet to the target address failed due to lack of a route to the target address.

Sample Display of a Standard Ping

The following display shows a sample standard **appletalk ping** session:

```
router# ping
Protocol [ip]: appletalk
Target Appletalk address: 1024.128
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Verbose [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte AppleTalk Echos to 1024.128, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 4/4/8 ms
```

Sample Display Using Ping in Verbose Mode

When you answer **y** in response to the prompt `Verbose [n]`, **ping** runs in verbose mode. The following display shows a sample **appletalk ping** session when verbose mode is enabled:

```
router# ping
Protocol [ip]: appletalk
Target AppleTalk address: 4.129
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Verbose [n]: y
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte AppleTalk Echos to 4.129, timeout is 2 seconds:
0 in 4 ms from 4.129 via 1 hop
1 in 8 ms from 4.129 via 1 hop
2 in 4 ms from 4.129 via 1 hop
3 in 8 ms from 4.129 via 1 hop
4 in 8 ms from 4.129 via 1 hop
Success rate is 100 percent, round-trip min/avg/max = 4/6/8 ms
```

Table 1-4 describes the fields in the verbose mode portion of the display.

Table 1-4 AppleTalk Ping Fields

Field	Meaning
0	Sequential number identifying the packet's relative position in the group of ping packets sent.
in 4 ms	Round-trip travel time of the ping packet, in milliseconds.
from 4.129	Source address of the ping packet.
via 1 hop	Number of hops the ping packet traveled to the destination.

Sample Display of NBP Ping and the Nbptest Facility

The AppleTalk **ping** command allows testing and informational lookup of NBP-registered entities. Use the NBP option when you find that AppleTalk zones are listed in the Chooser, but services in these zones are unavailable. When you enter **nbp** in response to the `Target AppleTalk address` prompt, **ping** starts the **nbptest** facility, which is an interactive, menu-driven facility. Type **help** or **?** to see the command list. Type **quit** to return to the EXEC prompt.

The following display shows how to initialize the AppleTalk **nbptest** utility:

```
router# ping
Protocol [ip]: appletalk
Target AppleTalk address: nbp
nbptest>
```

Type **help** to display the following list of available commands:

```
nbptest> help
Tests are:
lookup:     lookup an NVE. prompt for name, type and zone
parms:      display/change lookup parms (ntimes, ncecs, interval)
zones:      display zones
poll:       for every zone, lookup all devices, using default
help|?:     print command list
quit:       exit nbptest
```

The following paragraphs summarize the **nbptest** tests that you can perform:

- **lookup**—Searches for NBP entities in a specific zone.
- **parms**—Sets the parameters used in subsequent lookup and pool tests.
- **zones**—Displays the router's current zone list. It is equivalent to the **show appletalk zones** command.
- **poll**—Searches for all devices in all zones.
- **help** or **?**—Displays the list of **nbptest** tests.
- **quit**—exit from the **nbptest** facility.

The remainder of this section shows and explains the output of the various **nbptest** commands.

When running any of the **nbptest** 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 NBP truncation wildcard.

The following display shows sample output of the **nbptest lookup** command:

```
nbptest> lookup
Entity name [=]:
Type of Service [ipgateway]: macintosh:c5
Zone [bldg-17]: 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’
NBP lookup request timed out
Processed 6 replies, 7 events
```

Table 1-5 describes the fields shown in the display.

Table 1-5 AppleTalk Ping Nbptest Lookup Field Descriptions

Field	Description
Entity name [=]:	Name of NBP entity to display. The default is to display entries for all NBP entities. This is the same as typing =.
Type of Service	NBP service. The default is ipgateway. An = indicates any type of service.
Zone	Zone to search. The default is the zone of the current interface.

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.
NBP lookup request timed out	Indicates whether replies were heard within the timeout interval.
Processed 6 replies, 7 events	Number of NBP replies the router has received.

The following display shows sample output of the **nbptest parms** command:

```
nbptest> parms
maxrequests [5]:1
maxreplies [1]:100
interval [5]:10
```

Table 1-6 describes the fields shown in the display.

Table 1-6 AppleTalk Ping Nbptest Parms Field Descriptions

Field	Description
maxrequests	Maximum number of lookup retries. This is a number in the range 1 to 5. The default value is 5.
maxreplies	Maximum number of replies to accept for each lookup. This is a number in the range 1 to 500. The default is 1.
interval	Interval, in seconds, between each retry. This is in the range 1 to 60. The default is 5.

The following display shows sample output from the **nbptest zones** command:

```
nbptest> zones
Name                    Network(s)
UDP                     17 11
Heavenly                1161 6
Hostipal                55
Bldg-17                 82 81 14 13
CSL EtherTalk           22
Twilight                1554 254 36 33 4
EtherTalk               22
LocalTalk               80
Total of 9 zones
```

Table 1-7 describes the fields shown in the display.

Table 1-7 AppleTalk Ping Nbptest Zones Field Descriptions

Field	Description
Name	Zone name.
Network(s)	Number or numbers of the AppleTalk networks assigned to the zone.

The following display shows sample output from the **nbptest poll** command:

```
nbptest> poll
poll: sent 2 lookups
(100n,82a,252s)[1]: ‘userA:Macintosh IIci@Zone one’
(200n,75a,254s)[1]: ‘userB:Macintosh IIcx@Zone two’
NBP polling completed.
Processed 2 replies, 2 events
```

Table 1-8 describes the fields shown in the display.

Table 1-8 AppleTalk Ping Nbptest 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.
NBP polling completed.	Indicates that the polling completed successfully.
Processed 2 replies, 2 events	Number of NBP replies the router has received.

Related Commands

ping (user)
show appletalk zones

show appletalk access-lists

To display the AppleTalk access lists currently defined, use the **show appletalk access-lists** EXEC command.

show appletalk access-lists

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

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 1-9 describes fields shown in the display.

Table 1-9 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.
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

access-list additional-zones
access-list cable-range
access-list includes
access-list network
access-list other-access
access-list within
access-list zone
appletalk access-group
appletalk distribute-list in
appletalk distribute-list out
appletalk getzonelist-filter

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** EXEC command.

show appletalk adjacent-routes

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

The **show appletalk adjacent-routes** command provides a quick overview of the local environment that is especially useful when an AppleTalk internet 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.

Sample Display

The following is sample output from the **show appletalk adjacent-routes** command:

```
router# show appletalk adjacent-routes

Codes: R - RTMP derived, C - connected, 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 1-10 describes the fields shown in the display.

Table 1-10 Show AppleTalk Adjacent-Routes Field Descriptions

Field	Description
Codes:	Codes defining source of route.
R	Route learned from an RTMP update.
C	Directly connected network.
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)

Field	Description
via	NBP registered name or address of the router that sent the routing information.
directly connected	Indicates that the network or cable range is directly connected to the router.
0 sec	Time, in seconds, since information about this network cable range was last received.
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 AppleTalk ARP (AARP) cache, use the **show appletalk arp** EXEC command.

show appletalk arp

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

ARP establishes associates between network addresses and hardware (MAC) addresses. This information is maintained in the router's ARP cache.

Sample Display

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 1-11 describes the fields shown in the display.

Table 1-11 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.
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 router 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 router gets the response, the entry is marked "Dynamic." A pending AARP entry times out after 1 minute.

Field	Description
Hardware Addr	MAC address of this interface.
Encap	Encapsulation type. It can be one of the following: • ARPA—Ethernet-type encapsulation • SNAP—IEEE 802.3 encapsulation.
Interface	Type and number of the interface.

show appletalk cache

To display the routes in the AppleTalk fast-switching table on an extended AppleTalk network, use the **show appletalk cache** EXEC command.

show appletalk cache

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

The **show appletalk cache** command displays information for all fast-switching route cache entries, whether or not 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 a **no appletalk routing**, an **appletalk route-cache**, or an **access-list** command.
- The encapsulation on the line has changed.
- An interface has become operational or nonoperational.

Sample Display

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     AA0004000134000000C000E8C809B84BE02
*    33.000     Ethernet1     AA0004000134000000C000E8C809B84BE02
```

Table 1-12 describes the fields shown in the display.

Table 1-12 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 Command

appletalk route-cache

show appletalk globals

To display information and settings about the router's AppleTalk internetwork and other parameters, use the **show appletalk globals** EXEC command.

show appletalk globals

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show appletalk globals** command:

```
router# show appletalk globals
AppleTalk global information:
      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.
      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 1-13 describes the fields shown in the display.

Table 1-13 Show AppleTalk Globals Field Descriptions

Field	Description
AppleTalk global information:	Heading for the command output.
Internet is compatible with older, AT Phase1, routers.	Indicates whether the AppleTalk internetwork meets the criteria for interoperation with Phase 1 routers.
There are 67 routes in the internet.	Total number of routes in the AppleTalk internet from which this router has heard in routing updates.
There are 25 zones defined.	Total number of valid zones in the current AppleTalk internet 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 router sends routing updates.
RTMP entries are considered BAD after 20 seconds.	Time after which routes for which the router has not received an update will be marked as candidates for being deleted from the routing table.

Field	Description
RTMP entries are discarded after 60 seconds.	Time after which routes for which the router 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 probe retransmit-count** and **appletalk arp probe 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 request retransmit-count** and **appletalk arp request interval** commands, respectively.
DDP datagrams will be checksummed.	Indicates whether the **appletalk checksum** configuration command is enabled. When enabled, the router 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** configuration command is enabled. When enabled, RTMP packets arriving from routers that are not directly connected to the router performing the check are discarded.
RTMP routes may not be propagated without zones.	Indicates whether the **appletalk require-route-zones** configuration command is enabled. When enabled, the router 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

appletalk arp probe interval
appletalk arp probe retransmit-count
appletalk checksum
appletalk event-logging
appletalk lookup-type
appletalk name-lookup-interval
appletalk require-route-zones
appletalk strict-rtmp

show appletalk interface

To display the status of the AppleTalk interfaces configured in the router and the parameters configured on each interface, use the **show appletalk interface** EXEC command.

show appletalk interface [**brief**] [*type unit*]

Syntax Description

brief	(Optional.) Displays a brief summary of the status of the AppleTalk interfaces.
type unit	(Optional.) Interface and unit identifiers. The argument *type* can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), loopback, null, serial, or tunnel. The variable *unit* is the number of the interface. For example, ethernet 0 specifies the first Ethernet interface.

Command Mode

EXEC

Usage Guidelines

The **show appletalk interface** is particularly useful when you first enable AppleTalk on a router interface.

Sample Displays

The following is sample output from the **show appletalk interface** command for an extended AppleTalk network:

```
router# show appletalk interface t0
TokenRing 0 is up, line protocol is up
    AppleTalk cable range is 4172-4172
    AppleTalk address is 4172.30, Valid
    AppleTalk zone is "Low End SW Lab"
    AppleTalk port configuration provided by 4172.224 (urk)
    AppleTalk discarded 117 packets due to output errors
    AppleTalk discovery mode is enabled
    AppleTalk address gleaning is disabled
    AppleTalk route cache is not supported by hardware
```

Table 1-14 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 router has been configured with the **appletalk lookup-type** and **appletalk name-lookup-interval** commands.

Table 1-14 Show AppleTalk Interface Field Descriptions for an Extended Network

Field	Description
TokenRing is ...	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
line protocol is ...	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether keepalives are successful).
AppleTalk cable range is ...	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 is ...	Name of the zone that this interface is in.
AppleTalk port configuration provided by ...	Indicates whether the interface was configured in discovery mode. If it was, this line shows the address and name of the router that provided the configuration information.
AppleTalk discarded 117 packets due to output errors	Number of packets discarded due to output errors. These errors can occur for the following reasons: • There is no AARP entry for the destination address. • There was a controller error. • Lower-level software returned the "send AppleTalk packet" error message.
AppleTalk discovery mode is ...	Indicates whether AppleTalk discovery mode has been enabled on the interface via the **appletalk discovery** command. When enabled, the configuration for this interface (cable range and the zone list) is obtained from another router on the same cable.
AppleTalk gleaning is ...	Indicates whether the interface is automatically deriving ARP table entries from incoming packets (referred to as "gleaning").
AppleTalk route cache is ...	Indicates whether fast switching is enabled on the interface.
Port configuration mismatch	Indicates that the router is misconfigured.
Interface violates Internet compatibility	Usually indicates that extended and nonextended AppleTalk nodes are incorrectly sharing the same network.

The following is sample output from the **show appletalk interface** command for a nonextended AppleTalk network:

```
router# show appletalk interface e1
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 1-15 describes the fields shown in the display.

Table 1-15 Show AppleTalk Interface Field Descriptions for a Nonextended Network

Field	Description
Ethernet 1 is ...	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
line protocol is ...	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 is ...	Name of the zone that this interface is in.
AppleTalk routing protocols enabled are ...	AppleTalk routing protocols that are enabled on the interface.
AppleTalk address gleaning is ...	Indicates whether the interface is automatically deriving ARP table entries from incoming packets (referred to as "gleaning").
AppleTalk route cache is ...	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 1-16 describes the fields shown in the display.

Table 1-16 Show AppleTalk Interface Brief Field Descriptions

Field	Description
Interface	Interface and unit identifiers.
Address	Address assigned to the interface.
Config	How the interface is configured. Possible values are extended, nonextended, and not configured.
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.

Related Commands

appletalk discovery
appletalk lookup-type
appletalk name-lookup-interval

show appletalk macip-clients

To display status information about all known MacIP clients, use the **show appletalk macip-clients** EXEC command.

show appletalk macip-clients

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show appletalk macip-clients** command:

```
router# show appletalk macip-clients

131.108.199.1@[27001n,69a,72s] 45 secs    'S/W Test Lab'
```

Table 1-17 describes the fields shown in the display.

Table 1-17 Show AppleTalk MacIP Clients Field Descriptions

Field	Description
131.108.199.1@	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 Command

show appletalk traffic

show appletalk macip-servers

To display status information about a router's servers, use the **show appletalk macip-servers** EXEC command.

show appletalk macip-servers

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

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.

Sample Display

The following is sample output from the **show appletalk macip-servers** command:

```
router# show appletalk macip-servers
MACIP SERVER 1, IP 131.108.199.221,  ZONE 'S/W Test Lab' STATE is server_up
Resource #1 DYNAMIC 131.108.199.1-131.108.199.10, 1/10 IP in use
Resource #2 STATIC 131.108.199.11-131.108.199.20, 0/10 IP in use
```

Table 1-18 describes the fields shown in the display.

Table 1-18 Show AppleTalk MacIP Servers Field Descriptions

Field	Description
MACIP SERVER 1	Number of the MacIP server. This number is assigned arbitrarily.
IP 131.108.199.221	IP address of the MacIP server.
ZONE 'S/W Test Lab'	AppleTalk server zone specified with the **appletalk macip server** command.
STATE is server_up	State of the server. Table 1-20 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 131.108.199.1-131.108.199.10, 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 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 1-19. Table 1-20 describes the state functions listed in Table 1-19. These are the states that are displayed by the **show appletalk macip-servers** command.

Table 1-19 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
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_RESOURCES	*	Return to previous state
ck_resource	NO_RESOURCES	resource_wait	Shut down and wait for resources

Table 1-20 Server States

State	Description
ck_resource	The server makes sure 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.

State	Description
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.
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

appletalk macip dynamic
appletalk macip server
appletalk macip static
show appletalk interface
show appletalk traffic

show appletalk macip-traffic

To display statistics about MacIP traffic through the router, use the **show appletalk macip-traffic** EXEC command.

show appletalk macip-traffic

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

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.

Sample Display

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 1-21 describes the fields shown in the display.

Table 1-21 Show AppleTalk MacIP Traffic Field Descriptions

Field	Description
MACIP_DDP_IN	Number of DDP packets received by the router.
MACIP_DDP_IP_OUT	Number of DDP packets received by the router that were sent to the IP network.
MACIP_DDP_NO_CLIENT_ SERVICE	Number of DDP packets received by the router for which there is no client.
MACIP_IP_IN	Number of IP packets received by the router.
MACIP_IP_DDP_OUT	Number of IP packets received by the router 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.

Field	Description
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 Command

show appletalk traffic

show appletalk name-cache

To display a list of NBP services offered by nearby routers and other devices that support NBP, use the **show appletalk name-cache** EXEC command.

show appletalk name-cache

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

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 the router.

Sample Display

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 1-22 describes the fields shown in the display.

Table 1-22 Show AppleTalk Name-Cache Field Descriptions

Field	Description
Net	AppleTalk network number or cable range.
Adr	Node address.
Skt	DDP socket number.

Field	Description
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 Command

show appletalk nbp

show appletalk nbp

To display the contents of the NBP name registration table, use the **show appletalk nbp** EXEC command.

show appletalk nbp

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

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 router 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 router is configured and operating properly.

One name is registered for each interface. Other service types are registered once for each zone.

The router deregisters the NBP name if AppleTalk is disabled on the interface for any reason.

Sample Display

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 1-23 describes the fields shown in the display as well as some fields not shown but that also may be displayed.

Table 1-23 Show AppleTalk NBP Field Descriptions

Field	Description
Net	AppleTalk network number.
Adr	Node address.
Skt	DDP socket number.
Name	Name of the service.

Field	Description
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.

Related Command

show appletalk name-cache

show appletalk neighbors

To display information about AppleTalk routers that are directly connected to any of the networks to which this router is directly connected, use the **show appletalk neighbors** EXEC command.

show appletalk neighbors [*neighbor-address*]

Syntax Description

no argument	Displays information about all neighbor AppleTalk routers.
neighbor-address	(Optional.) Displays information about the specified neighbor router.

Command Mode

EXEC

Usage Guidelines

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.

Sample Displays

The following is sample output from the **show appletalk neighbors** command:

```
router# show appletalk neighbors

AppleTalk neighbors:

31.86, Ethernet8, uptime 133:28:06, last update 1 sec ago
81.82, Fddi0, uptime 266:11:44, last update 7 secs ago
81.81, Fddi0, uptime 267:30:28, last update 958334 secs ago
  Neighbor is down.
29.200, Ethernet3, uptime 263:45:50, last update 948440 secs ago
Neighbor has restarted 2 times in 267:59:53.
  Neighbor is down.
81.80, Fddi0, uptime 268:00:08, last update 963617 secs ago
  Neighbor is down.
17.128, Ethernet2, uptime 133:26:43, last update 2 secs ago
  Neighbor has restarted 1 time in 268:00:21.
69.163, Ethernet0, uptime 268:00:25, last update 1 sec ago
```

Table 1-24 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 1-24 Show AppleTalk Neighbors Field Descriptions

Field	Description
31.86	AppleTalk address of the neighbor router.
Ethernet8	Router interface through which the neighbor router can be reached.
uptime 133:28:06	Amount of time, in hours, minutes, and seconds, that the router has received this neighboring router's routing updates.
last update 1 sec ago	Time, in seconds, since the router last received an update from the neighbor router.
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 neighbor** 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 1-25 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 1-25 Show AppleTalk Neighbor Field Descriptions for a 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 router has received this neighboring router's routing updates.
last update 7 secs ago	Time, in seconds, since the router last received an update from the neighbor router.
received queries	Number of RTMP queries that have been received from this neighbor.
Last query was sent	Time, in seconds, since last query was sent.
replies received	Number of RTMP replies the router has heard from this neighbor.
extended replies	Number of extended RTMP replies the router has received from this neighbor.
ZIP notifies	Number of ZIP notify packets the router has received from this neighbor.

Field	Description
obsolete ZIP commands	Number of nonextended-only (obsolete) ZIP commands the router has received from this neighbor.
miscellaneous ZIP commands	Number of ZIP commands (for example, GNI, GZI, and GMZ) the router received from end systems rather than from routers.
unrecognized ZIP commands	Number of bogus ZIP packets the router has received from this neighbor.
routing updates	Number of RMTP updates the router has received from this neighbor.
invalid entries	Of the routing update packets received from this neighbor, the number of invalid entries the router discarded.
Last update detail	Of the routing update packets received from this neighbor, the number the router already knew about.

Related Commands

appletalk lookup-type
appletalk name-lookup-interval

show appletalk route

To display the entries in the AppleTalk routing table, use the **show appletalk route** EXEC command.

show appletalk route [*network* | *unit type*]

Syntax Description

no argument	Displays all entries in the routing table.
network	(Optional.) Displays the routing table entry for the specified network.
unit type	(Optional.) Displays the routing table entries for networks that can be reached via the specified interface.

Command Mode

EXEC

Sample Displays

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, S - static, 3 routes
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, 29 routes in internet

C Net 254 directly connected, Ethernet1, zone Twilight
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
```

Table 1-26 describes the fields shown in the two displays as well as some fields not shown but that also may be displayed. Depending on the configuration of the global configuration commands **appletalk lookup-type** and **appletalk name-lookup-interval**, a node name may appear in this display instead of a node address.

Table 1-26 Show AppleTalk Route Field Descriptions

Field	Description
Codes:	Codes defining how the route was learned.
R	Route learned from an RTMP update.
C	Directly connected network.
S	Statically defined route. AppleTalk routes cannot be statically defined; therefore you should never see this code.
3 routes	Number of routes in the table.
Net 258	Network to which the route goes.
Net 999-999	Cable range to which the route goes.
directly connected	Indicates that the network is directly connected to the router.
1431 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.
Ethernet0	Possible interface through which updates to the remote network will be sent.
zone Twilight	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 router 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 router 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.
8 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, 67 routes in internet

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 1-27 describes significant fields shown in the display.

Table 1-27 Show AppleTalk Route Field Descriptions for a Specified Network

Field	Description
Codes:	Codes defining how the route was learned.
R	Route learned from an RTMP update.
C	Directly connected network.
67 routes in internet	Number of routes in the Apple Talk internet.
Net 69-69	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 router 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 router 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.
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 router received an update for this route.
Next hop: gatekeeper	Address or node name of the router that is one hop away.

Field	Description
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 router has received a routing update from a neighboring router since the last time the router sent an RTMP update for this route.
Valid zones: “Empty Guf”	Zone names that are valid for this network.

Related Commands

appletalk lookup-type
appletalk name-lookup-interval
clear apple route

show appletalk sockets

To display information about process-level operation in the sockets of an AppleTalk interface, use the **show appletalk sockets** EXEC command.

show appletalk sockets [*socket-number*]

Syntax Description

no argument	Displays information about all sockets.
socket-number	(Optional.) Displays information about the specified socket number.

Command Mode

EXEC

Sample Display

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 socket** command when you do specify a socket number:

```
router# show appletalk socket 6
6        ZIP       AT ZIP           0    13619
```

Table 1-28 describes the fields shown in these displays.

Table 1-28 Show AppleTalk Socket 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 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 Mode

EXEC

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.

Sample Display

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 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
  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 1-29 describes the fields shown in the display.

Table 1-29 Show Apple Traffic Field Descriptions

Field	Description
Rcvd:	This section describes the packets that the router has received.
357741 total	Total number of packets the router 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 router received that were encapsulated within an IP packet.
0 bad MacIP	Number of bad MacIP packets the router 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 router 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.
Bcast:	Number of broadcast packets sent and received by the router.
Sent:	This section describes the packets that the router has transmitted.
550293 generated	Number of packets sent that were generated by the router.
66495 forwarded	Number of packets sent that were forwarded by the router.
1840 fast forwarded	Number of packets sent using routes from the fast-switching cache.
0 forwarded from MacIP	Number of IP packets the router 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 by the router.
387265 long	Number of DDP long packets.

Field	Description
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 the router has sent.
59947 forwards	Number of NBP forward requests the router has received or sent.
418674 lookups	Number of NBP lookups the router has 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 the router has received.
0 requests	Number of RTMP requests the router has received.
0 invalid	Number of invalid RTMP packets received. Causes include invalid op code and invalid packet type.
40189 ignored	Number of RTMP packets the router 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 the router has sent.
0 replies	Number of RTMP replies the router has 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 has received.
33633 sent	Number of ZIP packets the router has 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.

Field	Description
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.
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 due to 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	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.

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

show appletalk macip-traffic
show ip aliases †

show appletalk zone

To display the entries in the zone information table, use the **show appletalk zone** EXEC command.

show appletalk zone [*zone-name*]

Syntax Description

no argument	Displays all entries in the zone information table.
zone-name	(Optional.) Displays the entry for the specified zone.

Command Mode

EXEC

Usage Guidelines

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 local-area network (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 sample display below is associated with two network numbers and four cable ranges.

Sample Display

The following is sample output from the **show appletalk zone** command:

```
router# show appletalk zone
Name                    Network(s)
Gates of Hell           666-666
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
```

Table 1-30 describes the fields shown in the display.

Table 1-30 Show AppleTalk Zone Field Descriptions

Field	Description
Name	Name of the zone.
Network	Cable ranges or network numbers assigned to this zone.

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 1-31 describes the fields shown in the display.

Table 1-31 Show AppleTalk Zone Field Descriptions for a 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 Command

appletalk zone

tunnel destination

To specify the destination for encapsulated packets, use the **tunnel destination** interface configuration command. To remove a destination, use the **no** form of this command.

tunnel destination *ip-address*
no tunnel destination *ip-address*

Syntax Description

ip-address	Internet address of the destination router. The address is expressed in decimal in four-part, dotted notation.

Default

None

Command Mode

Interface configuration

Usage Guidelines

Tunneling encapsulates an AppleTalk packet inside an IP packet, which is sent across the IP backbone to a destination router. The destination router then de-encapsulates the AppleTalk packet and, if necessary, routes the packet to an AppleTalk network. To enable tunneling, you must specify a source interface or router through which the encapsulated packets will be sent (using the **tunnel source** command) and the address of a destination router that will receive the encapsulated packets (using the **tunnel destination** command).

You can configure multiple tunnels that originate from the same router.

Tunnels are logically point-to-point links. This requires that you configure a separate tunnel for each link.

If two tunnels have the same source and destination addresses, they must use different encapsulations.

Examples

The following example enables Cayman tunneling:

```
interface tunnel0
tunnel source ethernet0
tunnel destination 131.108.164.19
tunnel mode cayman
```

The following example enables GRE tunneling:

```
interface tunnel0
appletalk cable-range 4160-4160 4160.19
appletalk zone Engineering
tunnel source ethernet0
tunnel destination 131.108.164.19
tunnel mode gre ip
```

Related Commands

appletalk cable-range
appletalk zone
tunnel mode
tunnel source

tunnel mode

To specify the tunneling method, use the **tunnel mode** interface configuration command. To disable a tunneling method, use the **no** form of this command.

tunnel mode {**cayman** | **gre ip**}
no tunnel mode {**cayman** | **gre ip**}

Syntax Description

cayman	Enables Cayman tunneling.
gre ip	Enables Generic Route Encapsulation (GRE) tunneling.

Default

gre ip

Command Mode

Interface configuration

Usage Guidelines

The **tunnel mode** lets you specify the AppleTalk tunneling method.

Cayman tunneling implements tunneling as designed by Cayman Systems. This enables our routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers as well as between our router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address. This means that there is no way to ping the other end of the tunnel.

Generic Route Encapsulation (GRE) tunneling can be done between our routers only. When using GRE tunneling, you configure the tunnel with an AppleTalk network address. This means that you can ping the other end of the tunnel.

If two tunnels have the same source and destination addresses, they must use different encapsulations.

Examples

The following example enables Cayman tunneling:

```
interface tunnel0
tunnel source ethernet0
tunnel destination 131.108.164.19
tunnel mode cayman
```

The following example enables GRE tunneling:

```
interface tunnel0
appletalk cable-range 4160-4160 4160.19
appletalk zone Engineering
tunnel source ethernet0
tunnel destination 131.108.164.19
tunnel mode gre ip
```

Related Commands

appletalk cable-range
appletalk zone
tunnel destination
tunnel source

tunnel source

To specify the interface out which encapsulated packets are sent, use the **tunnel source** interface configuration command. To remove a source interface, use the **no** form of this command.

tunnel source {*interface* | *ip-address*}
no tunnel source {*interface* | *ip-address*}

Syntax Description

interface	Name of a network interface, such as Ethernet0.
ip-address	Internet address of the source interface. The address is expressed in decimal in four-part, dotted notation.

Default

None

Command Mode

Interface configuration

Usage Guidelines

Tunneling encapsulates an AppleTalk packet inside an IP packet, which is sent across the IP backbone to a destination router. The destination router then de-encapsulates the AppleTalk packet and, if necessary, routes the packet to an AppleTalk network. To enable tunneling, you must specify a source interface or router through which the encapsulated packets will be sent (using the **tunnel source** command) and the address of a destination router that will receive the encapsulated packets (using the **tunnel destination** command).

You can configure multiple tunnels that originate from the same router.

Tunnels are logically point-to-point links. This requires that you configure a separate tunnel for each link.

If two tunnels have the same source and destination addresses, they must use different encapsulations.

Examples

The following example enables Cayman tunneling:

```
interface tunnel0
tunnel source ethernet0
tunnel destination 131.108.164.19
tunnel mode cayman
```

The following example enables GRE tunneling:

```
interface tunnel0
appletalk cable-range 4160-4160 4160.19
appletalk zone Engineering
tunnel source ethernet0
tunnel destination 131.108.164.19
tunnel mode gre ip
```

Related Commands

appletalk cable-range
appletalk zone
tunnel destination
tunnel mode