

AppleTalk Remote Access Commands

This chapter describes the commands used to configure your access server to act as an AppleTalk Remote Access (ARA) server. Cisco's implementation of ARA gives Macintosh users direct access to information and resources in remote locations. Macintosh users can connect to another Macintosh computer or AppleTalk network over standard telephone lines. For example, if you have a PowerBook at home and need to get a file from your Macintosh at the office, ARA software can make the connection between your home computer and office computer.

This chapter does not describe how to configure or use the client Macintosh. Refer to Apple Computer's *Apple Remote Access Client User's Guide* and the *Apple Remote Access Personal Server User's Guide* for information about how to use ARA software on your Macintosh. For AppleTalk Remote Access configuration tasks and examples, refer to the "Configuring an AppleTalk Remote Access Server" chapter in the *Access and Communication Servers Configuration Guide*.

access-list additional-zones

To define the action 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

<i>access-list-number</i>	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

Access is denied.

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 access.

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 zone**

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 cable-range
no access-list access-list-number {deny | permit} cable-range cable-range
```

Syntax Description

<i>access-list-number</i>	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.
<i>cable-range</i>	Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number.

Default

No AppleTalk access lists are defined for a cable range.

Command Mode

Global configuration

Usage Guidelines

The **access-list cable-range** command affects matching on extended networks only. The conditions defined by this access list are used only when the packet's cable range exactly matches the cable range specified in the **access-list network** command. The conditions are never used to match a network number (for a nonextended network) even if the cable range has the same starting and ending number as the nonextended network number.

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

```
no access-list access-list-number
```

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

```
no access-list access-list-number {deny | permit} cable-range cable-range
```

Example

The access list created by the following commands allows all packets to be forwarded 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

access-list additional-zones

access-list includes

access-list network

access-list other-access

access-list within

access-list zone

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 cable-range
no access-list access-list-number {deny | permit} includes cable-range
```

Syntax Description

<i>access-list-number</i>	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.
<i>cable-range</i>	Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number. To specify a network number, set the starting and ending network numbers to the same value.

Default

No AppleTalk access list that overlaps any part of a range of network numbers or cable ranges is defined.

Command Mode

Global configuration

Usage Guidelines

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

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

```
no access-list access-list-number
```

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

```
no access-list access-list-number {deny | permit} includes cable-range
```

Example

The following example defines an access list that permits access to packets destined to any nonextended or extended network whose network number or cable range overlaps any part of the range 10 to 20. This means, for example, that packets whose cable ranges are 13 to 16 and 17 to 25 will be forwarded. This access list also allows all other packets to be forwarded.

access-list includes

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

Related Commands

access-list additional-zones

access-list cable-range

access-list network

access-list other-access

access-list within

access-list zone

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

<i>access-list-number</i>	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.
<i>network</i>	AppleTalk network number.

Default

No AppleTalk access list for a single network number is defined.

Command Mode

Global configuration

Usage Guidelines

The **access-list network** command affects matching on nonextended networks only. The conditions defined by this access list are used only when the packet's network number 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.

To delete an access list, specify the minimum number of keywords and arguments needed to delete the desired access list. For example, to delete an 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

access-list additional-zones
access-list cable-range
access-list includes
access-list other-access
access-list within
access-list zone

access-list other-access

To define the 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

<i>access-list-number</i>	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

Other access is denied.

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.

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

access-list additional-zones
access-list cable-range
access-list includes
access-list network
access-list within
access-list zone

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

Syntax Description

<i>access-list-number</i>	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.
<i>cable-range</i>	Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. 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

No AppleTalk access list is defined for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.

Command Mode

Global configuration

Usage Guidelines

The **access-list within** command affects matching on extended and nonextended AppleTalk networks. The conditions defined by this access list are used when the packet's cable range or network number is completely included in one (or more) of those specified in the **access-list network** command.

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

no access-list *access-list-number*

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

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

Example

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

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

Related Commands

access-list additional-zones

access-list cable-range

access-list includes

access-list network

access-list other-access

access-list zone

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

<i>access-list-number</i>	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.
<i>zone-name</i>	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 numbers. The zone name cannot have leading or trailing space characters.

Default

No AppleTalk access list is applied to a zone.

Command Mode

Global configuration

Usage Guidelines

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 address

To enable nonextended AppleTalk on an interface, use the **appletalk address** interface configuration command. To disable nonextended AppleTalk, 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 65280. 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 AppleTalk on the interface before assigning zone names.

Specifying an address of 0.0, 0.*node*, or *network*.0 puts the interface into discovery mode. When in this mode, the access server attempts to determine network address information from another access server or router on the network. You can also enable discovery mode with the **appletalk discovery** command. Note that discovery mode does not run over synchronous serial lines.

Example

The following example enables nonextended AppleTalk on Ethernet interface 0:

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

Related Commands

appletalk cable-range
appletalk discovery
appletalk zone

appletalk cable-range

To assign a range of networks to a cable, use the **appletalk cable-range** interface configuration command. Use the **no** form of this command to disable a cable-range setting.

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

Syntax Description

<i>cable-range</i>	Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. These arguments are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number.
<i>network.node</i>	(Optional) Suggested AppleTalk address for the interface. The argument <i>network</i> is the 16-bit network number, and the argument <i>node</i> 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

The access server needs both a valid cable range and a zone list to use AppleTalk. This command must be entered before the **appletalk zone** command.

Whenever you change the cable range, the access server clears the internal zone list and you must enter a new zone list.

Configure the access server for discovery mode if you want to find out what the current cable range is. To configure the access server for discovery mode, use the **appletalk cable-range 0-0 0.0** command. This causes the access server to learn about the AppleTalk network. After saving the command in your configuration file, log back in and enable configuration mode. When you display the configuration, you will see the AppleTalk cable range and the AppleTalk zone variables. Then, add those two entries to the configuration and save the configuration file.

Examples

The following example shows how to use discovery mode:

```
appletalk routing  
interface ether 0  
  appletalk cable-range 0-0 0.0  
line 5 6  
  modem inout  
  speed 38400  
  arap enabled  
  autoselect
```

After you learn the cable range values, add them to the configuration file. For example:

```
appletalk cable-range 105-105 105.222
appletalk zone Marketing
username araiser password arapasswd
```

The following example assigns a cable range of 2-2 to the interface:

```
interface async 1
  appletalk cable-range 2-2
```

Related Commands

appletalk address

appletalk routing

appletalk zone

appletalk checksum

To enable the generation and verification of checksums for all AppleTalk 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 access server discards incoming DDP packets when the checksum is nonzero and is incorrect and when the access server is the final destination for the packet.

You might want to disable checksum generation and verification if you have older LaserWriter printers or other devices that cannot receive packets that contain checksums.

Example

The following example disables the generation and verification of checksums:

```
no appletalk checksum
```

appletalk discovery

To put 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 access server or 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 access server or router and then uses this information to configure itself.

If you enable discovery mode on an interface, that interface must configure itself by acquiring information from another operational access server or router on the attached network when the access server is starting up that interface. If no operational access server or router is present on the connected network, the interface will not start up.

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

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

If you enable **appletalk discovery** and the interface is restarted, you must have another operational access server or router on the directly connected network or the interface will not start up.

It is not advisable to have all access servers and routers on a network configured with discovery mode enabled. If all access servers were to restart simultaneously (for instance, after a power failure), the network would become inaccessible until at least one access server or 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 an access server to an existing network.

Discovery mode does not run over synchronous serial lines.

Use the **no appletalk discovery** command to disable discovery mode and allow the interface to be a seed port. If the interface is not operational when you issue this command, you must configure the zone name before the interface will be operational. If you are reconfiguring an operational interface by issuing the **no appletalk discovery** command, the command will have no effect because the network configuration is already established.

Example

The following example enables discovery mode on Ethernet interface 0:

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

Related Commands

appletalk address
appletalk cable-range
appletalk zone
show appletalk interface

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

<i>ip-address</i>	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 <i>server-zone</i>	Zone in which the MacIP server resides. The argument <i>server-zone</i> can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal numbers. For a list of Macintosh characters, refer to the Apple Computer, Inc. specification <i>Inside AppleTalk</i> . Zone names cannot have leading or trailing space characters.

Default

No IP addresses are allocated to dynamic MacIP clients.

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 172.16.1.28 to 172.16.1.44.

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

<i>ip-address</i>	IP address, in four-part dotted decimal notation. It is suggested that this address match the address of an existing IP interface.
zone <i>server-zone</i>	Zone in which the MacIP server resides. The argument <i>server-zone</i> can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal numbers. For a list of Macintosh characters, refer to the Apple Computer, Inc. specification <i>Inside AppleTalk</i> . Zone names cannot have leading or trailing space characters.

Default

No MacIP servers are established for a zone.

Command Mode

Global configuration

Usage Guidelines

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

You can configure multiple MacIP servers for an access server, 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.

A MacIP server is not registered using NBP until at least one MacIP resource is configured.

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 on the access server and the Ethernet interface.

```
appletalk macip server 172.16.2.28 zone Engineering
ip address 172.16.1.27 255.255.255.0
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 numbers. For a list of Macintosh characters, refer to the Apple Computer, Inc. specification *Inside AppleTalk*. Zone names cannot have leading or trailing space characters.

Default

No IP addresses are allocated.

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 not 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 172.16.1.50 to 172.16.1.66. The three nodes that have the specific addresses are 172.16.1.81, 172.16.1.92, and 172.16.1.101.

```
! This global statement specifies the MacIP server address and zone:
appletalk macip server 172.16.1.27 zone Engineering
!
! These global statements identify the statically addressed clients:
appletalk macip static 172.16.1.50 172.16.1.66 zone Engineering
appletalk macip static 172.16.1.81 zone Engineering
appletalk macip static 172.16.1.92 zone Engineering
appletalk macip static 172.16.1.101 zone Engineering
!
! These statements assign the IP address and subnet mask for Ethernet
! interface 0:
interface ethernet 0
 ip address 172.16.1.27 255.255.255.0
!
! This global statement enables AppleTalk on the access server.
appletalk routing
!
! These statements enable AppleTalk 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 routing

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

Usage Guidelines

You must enable AppleTalk routing to permit your access server to be an AppleTalk Remote Access (ARA) server.

Example

The following example enables AppleTalk protocol processing on the access server:

```
appletalk routing
```

Related Commands

appletalk address
appletalk cable-range
appletalk zone
arap enable

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 numbers. For a list of Macintosh characters, refer to the Apple Computer, Inc. specification *Inside AppleTalk*. The zone name cannot have leading or trailing spaces.

Default

No zone name is defined.

If a zone list exists, the first zone in the list is the default zone.

Command Mode

Interface configuration

Usage Guidelines

The access server needs both a valid cable range and zone list to use AppleTalk.

The **appletalk cable-range** command must be entered before the **appletalk zone** command.

The first zone specified in the list is the default zone.

The **appletalk zone** command accepts spaces in zone names. Do not use quotation marks in the command entry. When you have completed the entry, use the **show startup-config** command to display the configuration file.

The **no** form of the command deletes a zone name from a zone list or, if you do not specify a zone name, it deletes the entire zone list. Before configuring a new zone list, delete any existing zone-name list using the **no appletalk zone** command.

The internal zone list is cleared automatically when you issue an **appletalk cable-range** command. The list is also cleared if you issue the **appletalk zone** command on an existing network.

Changing the Zone List

AppleTalk access servers maintain a complete list of zone names and associated network numbers. AppleTalk network protocols assume that the list of zones is stable as long as the associated networks remain reachable. The only way to make an old zone name disappear throughout your network is to cause the associated routes to disappear. If you change a zone name and keep the network numbers the same, you might need to wait for the next general power failure for parts of your network to acquire new zone lists and flush the old entry.

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 a colon and two hexadecimal numbers to specify a Macintosh special character in the zone name *Cisco•Zone*.

```
appletalk zone Cisco:A5Zone
```

Related Commands

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

appletalk cable-range
show appletalk zone
show startup-config †

arap authentication

To enable TACACS+ authentication for ARA on a line, use the **arap authentication** command. Use the **no** form of the command to disable authentication for an ARA line.

```
arap authentication { default | list-name }
no arap authentication { default | list-name }
```

Syntax Description

default	Use the default list created with the aaa authentication arap command.
<i>list-name</i>	Use the indicated list created with the aaa authentication arap command.

Default

ARAP authentication uses the default set with the **aaa authentication arap** command. If no default is set, the local user database is checked.

Command Mode

Line configuration

Usage Guideline

This command is a per-line command used with TACACS+, and specifies the name of a list of AAA authentication processes to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). Defaults and lists are created with the **aaa authentication arap** command. Entering the **no** version of **arap authentication** has the same effect as entering the command with the **default** argument.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication arap** command.



Caution If you use a *list-name* that is not configured using the **aaa authentication arap** command, you will disable ARAP on this line.

Example

The following example specifies that the TACACS+ authentication list called MIS-access is to be used on ARA line 7:

```
line 7
  arap authentication MIS-access
```

Related Command

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

aaa authentication arap †

arap callback

To enable an ARA client to request a callback, use the **arap callback** global configuration command.

arap callback

Syntax Description

This command has no arguments or keywords.

Default

Callback requests are not accepted on lines configured for ARA.

Command Mode

Global configuration

Usage Guidelines

This command enables the access server to accept callback requests from ARA clients. You have to first enable AppleTalk routing on the access server and enable automatic ARA startup on the line. You can then use this command with either local username authentication or TACACS+ authentication.

Example

The following example accepts a callback request from an ARA client:

```
arap callback
```

Related Commands

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

arap authentication
autoselect ara
callback forced-wait†
ppp authentication†
ppp callback†
service exec-callback†
username†

arap dedicated

To configure a line to be used only as an ARA connection, use the **arap dedicated** line configuration command. Use the **no** form of the command to return the line to interactive mode.

arap dedicated
no arap dedicated

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Line configuration

Example

The following example configures line 3 to be used only for ARA connections:

```
line 3
  arap dedicated
```

arap enable

To enable ARA for a line, use the **arap enable** line configuration command. Use the **no** form of this command to disable ARA.

arap enable
no arap enable

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Line configuration

Example

The following example enables ARA on a line:

```
line 3
  arap enable
```

Related Commands

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

appletalk routing
autoselect †

arap network

To create a new network/zone and cause it to be advertised, use the **arap network** global configuration command. Use the **no** form of this command to prevent a new network/zone from being advertised.

```
arap network [network-number] [zone-name]  
no arap network
```

Syntax Description

<i>network-number</i>	(Optional) The AppleTalk network number. The network number must be unique on your AppleTalk network. This network is where all ARAP users appear when they dial in to the network.
<i>zone-name</i>	(Optional) The AppleTalk zone name.

Default

A new network or zone is not created.

Command Mode

Global configuration

Usage Guidelines

This is a required command. ARAP does not run without it in Cisco IOS Release 10.2 and above.

Example

The following example creates a new network/zone:

```
arap network 400 test zone
```

arap net-access-list

To control Macintosh access to networks, use the **arap net-access-list** line configuration command. Use the **no** form of this command to return to the default setting.

arap net-access-list *net-access-list-number*
no arap net-access-list *net-access-list-number*

Syntax Description

net-access-list-number One of the *list* values configured using the AppleTalk **access-list cable-range**, **access-list includes**, **access-list network**, **access-list other-access**, and **access-list within** commands.

Default

Disabled. The Macintosh has access to all networks.

Command Mode

Line configuration

Usage Guidelines

You can use the **arap net-access-list** command to apply access lists defined by the **access-list cable-range**, **access-list includes**, **access-list network**, **access-list other-access**, and **access-list within** commands.

You cannot use the **arap net-access-list** command to apply access lists defined by the **access-list zone** and **access-list additional-zones** commands.

Example

In the following example, ARA is enabled on line 3 and the Macintosh will have access to the AppleTalk access list numbered 650.

```
line 3
 arap enable
 arap net-access-list 650
```

Related Commands

appletalk cable-range
access-list includes
access-list network
access-list other-access
access-list within
arap zonelist

arap noguest

To prevent Macintosh guests from logging in to the access server, use the **arap noguest** line configuration command. Use the **no** form of this command to remove this restriction.

arap noguest [if-needed]
no arap noguest

Syntax Description

if-needed (Optional) Does not authenticate if the user already provided authentication. This allows users to log in as guests if they have already been authenticated through a username and/or password.

Default
Disabled

Command Mode
Line configuration

Usage Guidelines

A guest is a person who connects to the network without having to give a name or a password.



Caution You should not use the **arap noguest** command if you are using modified (CCL) scripts and the **login tacacs** command.

Example

The following example prohibits guests from logging in to the access server:

```
line 3
  arap enable
  arap noguest
```

arap require-manual-password

To require users to enter their password manually at the time they log in, use the **arap require-manual-password** line configuration command.

arap require-manual-password

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Line configuration

Usage Guidelines

This command only works for ARAP 2.0 connections.

Example

The following example forces users to enter their passwords manually at the time they log in, rather than use a saved password:

```
arap require-manual-password
```

Related Commands

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

enable password †

login (line configuration) †

password †

arap timelimit

To set the maximum length of an ARA session for a line, use the **arap timelimit** line configuration command. Use the **no** form of this command to return to the default of unlimited session length.

arap timelimit [*minutes*]
no arap timelimit

Syntax Description

minutes (Optional) Maximum length of time (in minutes) for a session

Default

Unlimited session length

Command Mode

Line configuration

Usage Guidelines

After the specified length of time, the session will be terminated.

Example

The following example specifies a maximum length of 20 minutes for ARA sessions:

```
line 3
  arap enable
  arap timelimit 20
```

Related Command

arap warningtime

arap use-tacacs

To enable TACACS for ARAP authentication, use the **arap use-tacacs** line configuration command. Use the **no** form of this command to disable TACACS for ARAP authentication.

arap use-tacacs [single-line]
no arap use-tacacs

Syntax Description

single-line (Optional) Accepts the username and password in the username field. If you are using an older version of TACACS, (before Extended TACACS) you must use this keyword.

Default

Disabled

Command Mode

Line configuration

Usage Guidelines

This is a per line command. Use this command only when you have set up an extended TACACS server. This command requires the new Cisco extended TACACS server.

Note This command cannot be used with AAA/TACACS+. Use the **arap authentication** command instead.

The command specifies that if a username and password are specified in the username, separated by an asterisk (*), then a standard TACACS login query is performed using that username and password. If the username does not contain an asterisk, then normal ARAP authentication is performed using TACACS.

This feature is useful when integrating TACACS with other authentication systems that require a clear text version of the user's password. Such systems include one-time password systems, token card systems, and others.



Caution Normal ARAP authentications prevent the clear-text password from being transmitted over the link. When you use the **single-line** keyword, passwords cross the link in the clear, exposing them to anyone looking for such information.

Due to the two-way nature of the ARAP authentication, the ARA application requires that a password value be entered in the Password field in the ARA dialog box. This secondary password must be "arap." First enter the username and password in the form *username*password* in the Name field of the dialog box, then enter **arap** in the Password field.

Example

The following example enables TACACS for ARAP authentication:

```
line 3
 arap use-tacacs
```

Related Commands

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

arap enable

arap noquest

autoselect †

tacacs-server extended †

tacacs-server host †

arap warningtime

To set when a disconnect warning message is displayed, use the **arap warningtime** line configuration command. Use the **no** form of this command to disable this function.

arap warningtime [*minutes*]
no arap warningtime

Syntax Description

minutes (Optional) Amount of time, in minutes, before the configured session time limit. At the configured amount of time before a session is to be disconnected, the access server sends a message to the Macintosh client, which causes a warning message to appear on the user's screen.

Default

Disabled

Command Mode

Line configuration

Usage Guidelines

This command can only be used if a session time limit has been configured on the line.

Example

The following example shows a line configured for 20-minute ARA sessions, with a warning 17 minutes after the session is started:

```
line 3
  arap enable
  arap dedicated
  arap timelimit 20
  arap warningtime 3
```

Related Command

arap timelimit

arap zonelist

To control what zones the Macintosh client sees, use the **arap zonelist** line configuration command. Use the **no** form of this command to disable the default setting.

```
arap zonelist zone-access-list-number  
no arap zonelist zone-access-list-number
```

Syntax Description

zone-access-list-number One of the *list* values configured using the AppleTalk **access-list zone** or **access-list additional-zones** commands.

Default

Disabled. The Macintosh will see all defined zones.

Command Mode

Line configuration

Usage Guidelines

You can use the **arap zonelist** command to apply access lists defined by the **access-list zone** and **access-list additional-zones** command.

You cannot use the **arap zonelist** command to apply access lists defined by the **access-list network** command.

Example

In the following example, ARA is enabled on line 3 and the Macintosh will see only zones permitted by access list 650.

```
line 3  
  arap enable  
  arap zonelist 650
```

Related Commands

access-list additional-zones
access-list zone
arap net-access-list

debug arap

To debug ARA sessions, use the **debug arap** privileged EXEC command. Use the **no** form of this command to turn off the debugging function.

```
debug arap { internal | memory | mnp4 | v42bis }  
no debug arap
```

Syntax Description

internal	Debug internal ARA packets
memory	Debug memory allocation for ARA
mnp4	Debug low-level asynchronous serial protocol
v42bis	Debug compression

Default

Disabled

Command Mode

Privileged EXEC

Example

The following example activates debugging internal ARA packets on line 3:

```
debug arap internal
```

login authentication

To enable TACACS+ authentication for logins, use the **login authentication** command. Use the **no** form of the command to return to the default.

```
login authentication { default | list-name }
no login authentication { default | list-name }
```

Syntax Description

default	Uses the default list created with the aaa authentication login command.
<i>list-name</i>	Uses the indicated list created with the aaa authentication login command.

Default

Login authentication uses the default set with **aaa authentication** command. If no default is set, the local user database is checked. On the console, no authentication is performed.

Command Mode

Line configuration

Usage Guideline

This command is a per-line command used with AAA, and specifies the name of a list of TACACS+ authentication processes to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). Defaults and lists are created with the **aaa authentication login** command. Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** argument.

Before issuing this command, create a list of authentication processes by using the **aaa authentication login** global configuration command.



Caution If you use a *list-name* that is not configured using the **aaa authentication login** command, you will disable logins on this line.

Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
 login authentication default
```

The following example specifies that the AAA authentication list called MIS-access is to be used on line 7:

```
line 7
 login authentication MIS-access
```

Related Command

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

aaa authentication login[†]

login tacacs

To configure your access server to use TACACS user authentication, use the **login tacacs** line configuration command. The **no** form of this command disables TACACS user authentication for a line.

login tacacs
no login tacacs

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Line configuration

Usage Guidelines

You can use TACACS security if you have configured a TACACS server and you have a CCL script that allows you to use TACACS security. For information about using files provided by Cisco to modify CCL scripts to support TACACS user authentication, refer to the “Configuring an AppleTalk Remote Access Server” chapter in the *Access and Communication Servers Configuration Guide*.

Note This command cannot be used with AAA/TACACS+. Use the **login authentication** command instead.

Example

In the following example, lines 1 through 16 are configured for TACACS user authentication:

```
line 1 16
 login tacacs
```

show appletalk arp

To display the entries in the AppleTalk Address Resolution Protocol (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

AARP establishes associates between network addresses and hardware (MAC) addresses. This information is maintained in the access server's AARP 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
```

Table 14-1 describes the fields shown in the display.

Table 14-1 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 using AARP. Hardware—Entry was learned from an adapter in the access server. Pending—Entry for a destination for which the access server does not yet know the address. When a packet requests to be sent to an address for which the access server does not yet have the MAC-level address, the access server 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 access server gets the response, the entry is marked "Dynamic." A pending AARP entry times out after one minute.
Hardware Addr	MAC address of this interface.

Field	Description
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 interface

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

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

Syntax Description

- brief** (Optional) Displays a brief summary of the status of the AppleTalk interfaces.
- type* (Optional) Interface type identifier, which can be one of the following: **asynchronous, dialer, ethernet, loopback, null, serial, or tunnel**.
- number* (Optional) Interface number. For example, ethernet 0 specifies the first Ethernet interface.

Command Mode

EXEC

Usage Guidelines

The **show appletalk interface** command is particularly useful for discovering the status of the interface when you first enable AppleTalk.

Sample Displays

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

```
Router# show appletalk interface
Ethernet0 is up, line protocol is up
  AppleTalk cable range is 111-111
  AppleTalk address is 111.188, Valid
  AppleTalk zone is Cisco Interop Demo
  AppleTalk port configuration verified by 111.59
  AppleTalk route cache is not supported by hardware
```

Table 14-2 describes the fields shown in the display as well as some fields not shown but that might also be displayed.

Table 14-2 Show AppleTalk Interface Field Descriptions for an Extended Network

Field	Description
Ethernet0 is up	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
line protocol is up	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether the keepalives are successful).
AppleTalk cable range is <i>start-end</i>	Cable range of the interface.

Field	Description
AppleTalk address is <i>address</i> , 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 <i>zone</i>	Name of the zone that this interface is in.
AppleTalk port configuration verified by <i>address</i> (name)	Indicates whether the interface was configured in discovery mode. If it was, this line shows which access server provided the configuration information.
AppleTalk route cache is not supported by hardware	Indicates whether fast switching is enabled on the interface.
Port configuration mismatch	Indicates that the access server 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 ethernet 0
Ethernet0 is up, line protocol is up
  AppleTalk address is 666.128, Valid
  AppleTalk zone is Underworld
```

Table 14-3 describes the fields shown in the display.

Table 14-3 Show AppleTalk Interface Field Descriptions for a Nonextended Network

Field	Description
Ethernet0 is up	Type of interface and whether it is currently active and inserted into the network (up) or inactive and not inserted (down).
line protocol is up	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether keepalives are successful).
AppleTalk address is <i>address</i> , 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 <i>zone</i>	Name of the zone that this interface is in.

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
Ethernet0  10.82    Extended    up                    up
Async 0    unassigned not config'd  administratively down  n/a
```

Table 14-4 describes the fields shown in the display.

Table 14-4 Show AppleTalk Interface Brief Field Descriptions

Field	Description
Interface	Interface and unit identifiers.
Address	Address assigned to the interface.

show appletalk interface

Field	Description
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 is up and running on the interface.

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
      172.16.199.1@[27001n,69a,72s] 45 secs   'S/W Test Lab'
```

Table 14-5 describes the fields shown in the display.

Table 14-5 Show AppleTalk MacIP Clients Field Descriptions

Field	Description
172.16.199.1@	Client IP address.
[27001n,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 your MACIP 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 172.16.199.221, ZONE 'S/W Test Lab' STATE is server_up
Resource #1 DYNAMIC 172.16.199.1-172.16.199.10, 1/10 IP in use
Resource #2 STATIC 172.16.199.11-172.16.199.20, 0/10 IP in use
```

Table 14-6 describes the fields shown in the display.

Table 14-6 Show AppleTalk MacIP Servers Field Descriptions

Field	Description
MACIP SERVER 1	Number of the MacIP server. This number is assigned arbitrarily.
IP 172.16.199.221	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 14-8 lists the possible states. If the server remains in the “resource_wait” state, check that resources have been assigned to this server with either the appletalk macip dynamic or the appletalk macip static command.
Resource #1 DYNAMIC 172.16.199.1-172.16.199.10, 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 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 in Table 14-7. Table 14-8 describes the state functions listed in Table 14-7. These are the states that are displayed by the **show appletalk macip-servers** command.

Table 14-7 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	Shutdown and wait for resources

Table 14-8 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.

State	Description
initial	State at which all servers start.
resource-wait	The server waits until a client range for the server has been configured.
send_confirms	The server requests a response from 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	Server has registered. This 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 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 access server, 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 an access server 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 access server.

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 14-9 describes the fields shown in the display.

Table 14-9 Show AppleTalk MacIP Traffic Field Descriptions

Field	Description
MACIP_DDP_IN	Number of DDP packets received by the access server.
MACIP_DDP_IP_OUT	Number of DDP packets received by the access server that were sent to the IP network.

Field	Description
MACIP_DDP_NO_CLIENT_SERVICE	MacIP servers are configured to serve a specific range of IP addresses. If a client (Macintosh) has been assigned an IP address that is not in the server range, and then tries to route a packet through the MacIP server, the packet is dropped and this statistic is incremented. This situation usually arises when the server is restarted after being configured with a different range of addresses, because the client Macintosh must reboot and obtain a new address.
MACIP_IP_IN	Number of IP packets received by the access server.
MACIP_IP_DDP_OUT	Number of IP packets received by the access server that were sent to the AppleTalk network.
MACIP_SERVER_IN	Number of packets destined for MacIP servers.
MACIP_SERVER_OUT	Number of packets sent by MacIP servers.
MACIP_SERVER_BAD_ATP	This statistic is incremented if MacIP receives a badly formatted AppleTalk ATP packet.
MACIP_SERVER_ASSIGN_IN	Counts the total number of assignment request packets received by MacIP.
MACIP_SERVER_ASSIGN_OUT	Counts the total number of assignment request packet replies sent by MacIP. It should be equal to the MACIP_SERVER_ASSIGN_IN statistic.
MACIP_SERVER_INFO_IN	This statistic counts the total number of information request packets received by MacIP. The information request is sent by MacIP clients after it has received its address assignment.
MACIP_SERVER_INFO_OUT	This statistic counts the total number of information request packets sent by MacIP. The information response contains the IP subnet mask, the IP broadcast address, the default IP router, the default domain name, and the IP address of the configured domain name server.

Related Command
show appletalk traffic

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 14-10 describes the fields shown in the display.

Table 14-10 Show AppleTalk Traffic Field Descriptions

Field	Description
Rcvd:	This section describes the packets that the access server has received.
357741 total	Total number of packets the access server 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 access server. 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 access server.
0 access denied	Number of packets discarded because they were denied by an access list.
0 for MacIP	Number of AppleTalk packets the access server received that were encapsulated within an IP packet.
0 bad MacIP	Number of bad MacIP packets the access server 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 being received while the access server 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 access server.
Sent:	This section describes the packets that the access server has transmitted.
550293 generated	Number of packets sent that were generated by the access server.
66495 forwarded	Number of packets sent that were forwarded by the access server.
1840 fast forwarded	Number of packets sent using routes from the fast-switching cache.
0 forwarded from MacIP	Number of IP packets the access server 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 access server 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 access server could not send because it knew of no route to the destination.

Field	Description
0 no source	Number of packets the access server sent when it did not know its own address. This should happen only if something is seriously wrong with the access server or network configuration.
DDP:	This section describes DDP packets seen by the access server.
387265 long	Number of DDP long packets.
0 short	Number of DDP short packets.
0 macip	Number of IP packets encapsulated in an AppleTalk DDP packet that the access server 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 access server when it was configured for NBP proxy transition usage.
57875 replies sent	Number of NBP replies the access server has sent.
59947 forwards	Number of NBP forward requests the access server has received.
418674 lookups	Number of NBP lookups the access server 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 access server has received.
0 requests	Number of RTMP requests the access server 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 access server 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 access server has broadcast.
0 replies	Number of RTMP replies the access server has sent.
ATP:	This section describes ATP packets.
0 received	Number of ATP packets the access server received.
ZIP:	This section describes ZIP packets.
13619 received	Number of ZIP packets the access server has received.
33633 sent	Number of ZIP packets the access server 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 access server received.
0 discarded	Number of AEP packets the access server discarded.

show appletalk traffic

Field	Description
0 illegal	Number of illegal AEP packets the access server received.
0 generated	Number of AEP packets the access server generated.
0 replies sent	Number of AEP replies the access server sent.
Responder:	This section describes Responder Request packets.
0 received	Number of Responder Request packets the access server received.
0 illegal	Number of illegal Responder Request packets the access server received.
0 unknown	Number of Responder Request packets the access server received that it did not recognize.
0 replies sent	Number of Responder Request replies the access server sent.
0 failures	Number of Responder Request replies the access server could not send.
AARP:	This section describes AARP packets.
85 requests	Number of AARP requests the access server received.
149 replies	Number of AARP replies the access server received.
100 probes	Number of AARP probe packets the access server sent.
84 martians	Number of AARP packets the access server 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 access server did not recognize.
278 sent	Number of AARP packets the access server sent.
0 failures	Number of AARP packets the access server 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 encapsulation	Number of packets discarded because they had the wrong encapsulation. That is, nonextended AppleTalk packets were on an extended AppleTalk network, or vice versa.
0 bad SNAP discrimination	Number of packets discarded because they had the wrong SNAP discriminator. This occurs when another AppleTalk device has implemented an obsolete or incorrect packet format.

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

zone-name (Optional) Name of a zone

Command Mode

EXEC

Usage Guidelines

If you omit the optional *zone-name* argument, all entries in the zone information table are displayed. 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. 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 14-11 describes the fields shown in the display.

Table 14-11 Show AppleTalk Zone Field Descriptions

Field	Description
Name	Name of the zone.
Network(s)	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 ozone
AppleTalk Zone Information for ozone:
Valid for nets: 4140-4140
Not associated with any interface.
Not associated with any access list.
```

Table 14-12 describes the fields shown in the display.

Table 14-12 Show AppleTalk Zone Field Descriptions for a Specific Zone Name

Field	Description
AppleTalk Zone Information for ozone:	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

show arap

To display information about a running ARAP connection, use the **show arap** user EXEC command.

```
show arap [line-number]
```

Syntax Description

line-number (Optional) Number of the line on which an ARAP connection is established and active

Command Mode

EXEC

Usage Guidelines

Use the **show arap** command with no arguments to display a summary of the ARAP traffic since the access server was last booted.

Sample Display

The following is sample output from the **show arap** command:

```
Router# show arap  
Statistics are cumulative since last reboot  
Total ARAP connections: 2  
Total Appletalk packets output: 157824  
Total Appletalk packets input: 12465
```

These fields refer to the sum of all of the ARA connections since the box was last reloaded.

The following example results in a display of information about ARA activity on a specific line (line 3):

```
Router# show arap 3  
  
Active for 23 minutes  
"Unlimited time left" or "22 minutes left"  
"Doing smartbuffering" or "Smartbuffering disabled"  
Appletalk packets output: 157824  
Appletalk packets input: 12465  
Appletalk packets overflowed: 1642  
Appletalk packets dropped: 586  
V42bis compression efficiency (incoming/outgoing): {percentage/percentage}  
MNP4 packets received: 864  
MNP4 packets sent: 1068  
MNP4 garbled packets received: 4  
MNP4 out of order packets received: 0  
MNP4 packets resent: 0  
MNP4 nobuffers: 0
```

Table 14-13 describes the fields shown in the display.

Table 14-13 Show ARAP Field Descriptions

Field	Description
Active for {integer} minutes	Number of minutes since ARAP started on the line.
Unlimited time left or {integer} minutes left	Remaining time limit on the line, if applicable on the line.
Doing smartbuffering or Smartbuffering disabled	Obsolete. Always says Doing smartbuffering.
Appletalk packets output:	Number of AppleTalk packets that have been received from the Macintosh and out to the network during this connection.
Appletalk packets input:	Number of AppleTalk packets have been received from the network and sent to the Macintosh during this connection.
Appletalk packets overflowed:	Number of packets from the network that have been dropped because the link to the Macintosh was congested.
Appletalk packets dropped:	Number of packets from the network that have been dropped because it was unnecessary to pass them (frequently RTMP).
V42bis compression efficiency (incoming/outgoing):	Performance of the v42bis protocol underneath ARA, expressed as percentage of incoming/percentage outgoing. If the efficiency is low, a network user is probably copying already compressed files across the link. Generally, low efficiency means slow performance.
MNP4 packets received:	Number of link-level packets that have been received from the Macintosh.
MNP4 packets sent:	How many link-level packets have been sent to the Macintosh.
MNP4 garbled packets received:	Number of garbled packets that have been received from the Macintosh.
MNP4 out of order packets received:	Number of out-of-order packets that have been received from the Macintosh.
MNP4 packets resent:	Number of times packets have been resent. Each of these fields indicates line noise. The higher the value, the higher the noise.
MNP4 nobuffers:	How many times MNP4 has run out of buffers. This field should be zero.