



Cisco IOS Dial Services Commands

This chapter presents the commands to configure and maintain Cisco IOS dial and access solutions. The commands are presented in alphabetical order. Some commands required for configuring dial and access solutions may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

aaa authorization configuration default

To download static route configuration information from the authorization, authentication, and accounting (AAA) server using TACACS+ or RADIUS, use the **aaa authorization configuration default** command in global configuration mode. To remove static route configuration information, use the **no** form of this command.

```
aaa authorization configuration default {radius | tacacs+}
```

```
no aaa authorization configuration default
```

Syntax Description

radius	Use RADIUS for static route download.
tacacs+	Use TACACS+ for static route download.

Defaults

No configuration authorization is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following example downloads static route information using a TACACS+ server:

```
aaa authorization configuration default tacacs+
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa route download	Enables the download static route feature and sets the amount of time between downloads.
clear ip route download	Clears static routes downloaded from a AAA server.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

aaa route download

To enable the download static route feature and set the amount of time between downloads, use the **aaa route download** command in global configuration mode. To disable this function, use the **no** form of the command.

```
aaa route download [time]
```

```
no aaa route download
```

Syntax Description	<i>time</i> (Optional) Time between downloads, in minutes. The range is 1 to 1440 minutes.
---------------------------	--

Defaults	The default period between downloads (updates) is 720 minutes.
-----------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines	This command is used to download static route details from the authorization, authentication, and accounting (AAA) server if the name of the router is hostname. The name passed to the AAA server for static routes is hostname-1, hostname-2 hostname-n—the router downloads static routes until it fails an index and no more routes can be downloaded.
-------------------------	---

Examples	The following example sets the AAA route update period to 100 minutes:
-----------------	--

```
aaa route download 100
```

Related Commands	Command	Description
	aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
	clear ip route download	Clears static routes downloaded from a AAA server.
	show ip route	Displays all static IP routes, or those installed using the AAA route download function.

absolute-timeout

To set the interval for closing the connection, use the **absolute-timeout** command in line configuration mode. To restore the default, use the **no** form of this command.

absolute-timeout *minutes*

no absolute-timeout

Syntax Description	<i>minutes</i>	Number of minutes after which the user session will be terminated.
--------------------	----------------	--

Defaults	No timeout interval is automatically set.
----------	---

Command Modes	Line configuration
---------------	--------------------

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines	Use the absolute-timeout command line configuration command to configure the EXEC to terminate when the configured number of minutes occurs on the virtual terminal (vty) line. The absolute-timeout command terminates the connection after the specified time period has elapsed, regardless of whether the connection is being used at the time of termination. You can specify an absolute-timeout value for each port. The user is given 20 seconds notice before the session is terminated. You can use this command along with the logout-warning command to notify users of an impending logout.
------------------	---

Cisco IOS software also provides the **session-timeout** and **exec-timeout** line configuration commands for releasing lines when they have been idle for too long.

You can set the **absolute-timeout** command and an AppleTalk Remote Access Protocol (ARAP) timeout for the same line; however, this command supersedes any timeouts set in ARAP. Additionally, ARAP users will receive no notice of any impending termination if you use this command.

Examples	The following example sets an interval of 60 minutes on line 5:
----------	---

```
line 5
 absolute-timeout 60
```

Related Commands	Command	Description
	exec-timeout	Sets the interval that the EXEC command interpreter waits until user input is detected.
	logout-warning	Sets and displays a warning for users about an impending forced timeout.
	session-timeout	Sets the interval for closing the connection on a console or terminal line.

accept dialin

To configure L2TP Network Servers (LNSs) to accept tunneled PPP connections from an L2TP Access Concentrator (LAC) and create an accept-dialin Virtual Private Dialup Network (VPDN) subgroup, use the **accept dialin** command in VPDN group configuration mode. To remove the accept-dialin subgroup from a VPDN group, use the **no** form of this command.

accept dialin

no accept dialin

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VPDN group configuration

Command History	Release	Modification
	11.3(5)AA	This command was introduced.
	12.0(1)T	This command was migrated to Release 12.0 T.
	12.0(5)T	All keywords and arguments were removed and made into separate accept-dialin subgroup commands.

Usage Guidelines For a VPDN group to accept dialin calls, you must also configure the following commands:

- **terminate-from** VPDN group command
- **protocol** VPDN subgroup command
- **virtual-template** accept-dialin command

Once an L2F or L2TP tunnel is established, both dial-in and dial-out calls can use the same tunnel.

This command replies to a dial in L2F or L2TP tunnel open request from the specified peer. Once the LNS accepts the request from a LAC, it uses the specified virtual template to clone new virtual access interfaces. This command replaces the **vpdn incoming** command used in Cisco IOS Release 11.3. The user interface will automatically be upgraded when you reload the router with a 12.0 T or 11.3 AA image.

Typically, you need one VPDN group for each LAC. For an LNS that services many LACs, the configuration can become cumbersome; however, you can use the default VPDN group configuration if all the LACs will share the same tunnel attributes. An example of this scenario would be a LNS that services a large department with many Windows NT L2TP clients that are co-located with the LAC. Each of the Windows NT devices is an L2TP client as well as a LAC. Each of these devices will demand a tunnel to the LNS. If all the tunnels will share the same tunnel attributes you can use a default VPDN group configuration, which excels and simplifies the configuration process.

**Note**

The **vpdn group** command must be configured with the **accept dialin** or **request dialin** command to be functional. The requester initiates a dial in tunnel. The acceptor accepts a request for a dial in tunnel.

Examples

The following example enables the LNS to accept an L2TP tunnel from a LAC named mugsy. A virtual-access interface will be cloned from virtual-template 1:

```
vpdn-group 1
  accept dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname mugsy
```

If you do not use the **terminate-from** command, you automatically enable a default VPDN group, which allows all tunnels to share the same tunnel attributes:

```
vpdn-group 1
! Default L2TP VPDN group
  accept dialin
  protocol l2tp
  virtual-template 1
```

Related Commands

Command	Description
force-local-chap	Forces the LNS to reauthenticate the client.
lcp renegotiation	Allows the LNS to renegotiate the LCP on dial-in calls, using L2TP or L2F.
protocol (VPDN)	Specifies the Layer 2 tunneling protocol that the VPDN subgroup will use.
request dialin	Configures a VPDN group to request L2F or L2TP tunnels to a home gateway and creates a request-dialin VPDN subgroup.
terminate-from	Specifies the host name of the remote LAC or LNS that will be required when accepting a VPDN tunnel.
virtual-template	Specifies which virtual template will be used to clone virtual-access interfaces.

accept dialout

To accept requests to tunnel Layer 2 Tunneling Protocol (L2TP) dial-out calls and create an accept-dialout VPDN subgroup, use the **accept dialout** command in VPDN group configuration mode. To remove the accept-dialout subgroup from the VPDN group, use the **no** form of this command.

accept dialout

no accept dialout

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VPDN group configuration

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

Usage Guidelines Only L2TP can be used to dial out, not Cisco's Layer 2 Forwarding (L2F). For a VPDN group to accept dialout calls, you must also configure the following commands:

- **terminate-from** VPDN group command
- **protocol** VPDN subgroup command
- **dialer** accept-dialout command
- **dialer aaa** dialer interface command

Once an L2TP tunnel is established, both dial-in and dialout calls can use the same tunnel.

Examples The following example configures a VPDN group to accept L2TP tunnels for dialout calls from the LNS cerise by using dialer 2 as its dialing resource:

```

vpdn-group 1
accept dialout
protocol l2tp
dialer 2
terminate-from hostname cerise
!
interface Dialer2
ip unnumbered Ethernet0
encapsulation ppp
dialer in-band
dialer aaa
dialer-group 1
ppp authentication chap

```

Related Commands	Command	Description
	dialer	Specifies the dialer interface that an accept-dialout VPDN subgroup will use to dial out calls.
	dialer aaa	Allows a dialer to access the AAA server for dialing information.
	dialer vpdn	Enables a Dialer Profile or DDR dialer to use L2TP dial-out.
	protocol (VPDN)	Specifies the Layer 2 tunneling protocol that the VPDN subgroup will use.
	request dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.
	terminate-from	Specifies the host name of the remote LAC or LNS that will be required when accepting a VPDN tunnel.

access-class (LAT)

To define restrictions on incoming and outgoing connections, use the **access-class** command in line configuration mode. To remove the access list number, use the **no** form of this command.

access-class *access-list-number* {**in** | **out**}

no access-class *access-list-number*

Syntax Description		
	<i>access-list-number</i>	Specifies an integer between 1 and 199 that defines the access list.
	in	Controls which nodes can make local-area transport (LAT) connections into the server.
	out	Defines the access checks made on outgoing connections. (A user who types a node name at the system prompt to initiate a LAT connection is making an outgoing connection.)

Defaults Disabled

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command defines access list numbers that will then be used with the **lat access-list** command to specify the access conditions.

The value supplied for the *access-list-number* argument is used for all protocols supported by the Cisco IOS software. If you are already using an IP access list, you must define local-area transport (LAT) and possibly X.25 access lists permitting connections to everything, to emulate the behavior of previous software versions.

When both IP and LAT connections are allowed from a terminal line and an IP access list is applied to that line with the **access-class** line configuration command, you must also create a LAT access list with the same number if you want to allow any LAT connections from that terminal. You can specify only one incoming and one outgoing access list number for each terminal line. When checking LAT access lists, if the specified list does not exist, the system denies all LAT connections.

Examples The following example configures an incoming access class on virtual terminal line 4:

```
line vty 4
 access-class 4 in
```

■ access-class (LAT)

Related Commands

Command	Description
lat access-list	Specifies access conditions to nodes on the LAT network.

arap callback

To enable an AppleTalk Remote Access (ARA) client to request a callback, use the **arap callback** command in global configuration mode. To disable callback requests, use the **no** form of this command.

arap callback

no arap callback

Syntax Description This command has no arguments or keywords.

Defaults Callback requests are not accepted on lines configured for ARA.

Command Modes Global configuration

Command History	Release	Modification
	11.1	This command was introduced.

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

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

```
arap callback
```

Related Commands	Command	Description
	arap callback	Enables an ARA client to request a callback from an ARA client.
	autoselect	Configures a line to start an ARA, PPP, or SLIP session.
		Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
	ppp bap call	Sets PPP BACP call parameters.
	ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
	server (RLM)	Enables the Cisco IOS software to call back clients that request a callback from the EXEC level.
	virtual-profile aaa	Enables virtual profiles by AAA configuration.

arap dedicated

To configure a line to be used only as an AppleTalk Remote Access (ARA) connection, use the **arap dedicated** command in line configuration mode. To return the line to interactive mode, use the **no** form of the command.

arap dedicated

no arap dedicated

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

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

```
line 3
 arap dedicated
```

arap enable

To enable AppleTalk Remote Access (ARA) for a line, use the **arap enable** command in line configuration mode. Use the **no** form of this command to disable ARA.

arap enable

no arap enable

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following example enables ARA on a line:

```
line 3
 arap enable
```

Related Commands	Command	Description
	appletalk routing	Enables AppleTalk routing.
	autoselect	Configures a line to start an ARA, PPP, or SLIP session.

arap net-access-list

To control Macintosh access to networks, use the **arap net-access-list** command in line configuration mode. 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.

Defaults

Disabled. The Macintosh has access to all networks.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

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.

Examples

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

Command	Description
arap zonelist	Controls which zones the Apple Macintosh client sees.

arap network

To create a new network/zone and cause it to be advertised, use the **arap network** command in global configuration mode. 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) 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) AppleTalk zone name.

Defaults A new network or zone is not created.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

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

Examples The following example creates a new network/zone:

```
arap network 400 test zone
```

arap nologuest

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

arap nologuest [if-needed]

no arap nologuest

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 or password.
---------------------------	------------------	---

Defaults	Disabled
-----------------	----------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.

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 nologuest** command if you are using modified Common Command Language (CCL) scripts and the **login tacacs** command.

Examples The following example prohibits guests from logging in to the router:

```
line 3
 arap enable
 arap nologuest
```

arap require-manual-password

To require users to enter their password manually at the time they log in, use the **arap require-manual-password** command in line configuration mode. Use the **no** form of this command to disable the manual password-entry requirement.

arap require-manual-password

no arap require-manual-password

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines This command only works for AppleTalk Remote Access Protocol (ARAP) 2.0 connections.

Examples 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	Command	Description
	enable password	Sets a local password to control access to various privilege levels.
	login (line)	Enables password checking at login and defines the method (local or TACACS+).
	peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.

arap timelimit

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

arap timelimit [*minutes*]

no arap timelimit

Syntax Description	<i>minutes</i> (Optional) Maximum length of time (in minutes) for a session.				
Defaults	Unlimited session length				
Command Modes	Line configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.0	This command was introduced.
Release	Modification				
10.0	This command was introduced.				
Usage Guidelines	After the specified length of time, the session will be terminated.				
Examples	<p>The following example specifies a maximum length of 20 minutes for ARA sessions:</p> <pre>line 3 arap enable arap timelimit 20</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>arap warningtime</td> <td>Sets when a disconnect warning message is displayed.</td> </tr> </tbody> </table>	Command	Description	arap warningtime	Sets when a disconnect warning message is displayed.
Command	Description				
arap warningtime	Sets when a disconnect warning message is displayed.				

arap warningtime

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

arap warningtime [*minutes*]

no arap warningtime

Syntax Description	<i>minutes</i>	(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 router sends a message to the Macintosh client, which causes a warning message to appear on the user's screen.
---------------------------	----------------	--

Defaults	Disabled
-----------------	----------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.

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

Examples The following example shows a line configured for 20-minute AppleTalk Remote Access (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 Commands	Command	Description
	arap timelimit	Sets the maximum length of an ARA session for a line.

arap zonelist

To control what zones the Macintosh client sees, use the **arap zonelist** command in line configuration mode. 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	<i>zone-access-list-number</i>
	One of the <i>list</i> values configured using the AppleTalk access-list zone or access-list additional-zones commands.

Defaults	Disabled. The Macintosh will see all defined zones.
----------	---

Command Modes	Line configuration
---------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

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

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

Hiding a zone from users is not the same as preventing them from sending and receiving packets from the networks that make up that zone. For true security, an **arap net-access-list** command must be issued to prevent traffic to and from those networks.

Examples

The following example enables AppleTalk Remote Access (ARA) on line 3; the Macintosh will see only zones permitted by access list 650.

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

Related Commands	Command	Description
	arap net-access-list	Controls Apple Macintosh access to networks.

async default ip address

The **peer default ip address** command replaces the **async default ip address** command.

See the description of the **peer default ip address** command in this book for more information.

async default routing

To enable the router to pass routing updates to other routers over the AUX port configured as an asynchronous interface, use the **async default routing** command in interface configuration mode. Use the **no** form of this command to disable dynamic addressing.

async default routing

no async default routing

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **async default routing** command to define the default behavior for router-to-router communication over connections to the AUX port configured as an asynchronous interface. This command is commonly used to enable two routers to communicate over an async dial backup link.

To require a remote user to manually configure routing over connections to the AUX port configured as an asynchronous interface, use the **async dynamic routing** command.

Examples

The following example enables routing over asynchronous interface 0:

```
interface async 0
async default routing
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.

async dynamic address

To specify dynamic asynchronous addressing, use the **async dynamic address** command in interface configuration mode. Use the **no** form of this command to disable dynamic addressing.

async dynamic address

no async dynamic address

Syntax Description This command has no arguments or keywords.

Defaults Dynamic addressing is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You can control whether addressing is dynamic (the user specifies the address at the EXEC level when making the connection), or whether default addressing is used (the address is forced by the system). If you specify dynamic addressing, the router must be in interactive mode and the user will enter the address at the EXEC level.

It is common to configure an asynchronous interface to have a default address and to allow dynamic addressing. With this configuration, the choice between the default address or a dynamic addressing is made by users when they enter the **slip** or **ppp** EXEC command. If the user enters an address, it is used, and if the user enters the **default** keyword, the default address is used.

Examples The following example shows dynamic addressing assigned to async interface six.

```
interface ethernet 0
 ip address 10.0.0.1 255.0.0.0
interface async 6
 async dynamic address
```

Related Commands	Command	Description
	peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.

async dynamic routing

To enable manually configured routing on an asynchronous interface, use the **async dynamic routing** command in interface configuration mode. Use the **no** form of this command to disable routing protocols; static routing is still used.

async dynamic routing

no async dynamic routing

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **async dynamic routing** command is commonly used to manually bring up PPP from an EXEC session.

Examples

The following example shows how to enable manually configured routing on asynchronous interface 1. The **ip tcp header-compression passive** command enables Van Jacobson TCP header compression and prevents transmission of compressed packets until a compressed packet arrives from the asynchronous link.

```
interface async 1
  async dynamic routing
  async dynamic address
  async default ip address 1.1.1.2
  ip tcp header-compression passive
```

A remote user who establishes a PPP or SLIP connection to this asynchronous interface can enable routing by using the **/routing** switch or the **ppp/routing** command.

However, if you want to establish routing by default on connections to an asynchronous interface, use the **async default routing** command when you configure the interface.

Related Commands	Command	Description
	async default routing	Enables the router to pass routing updates to other routers over the AUX port configured as an asynchronous interface.
	async dynamic address	Specifies dynamic asynchronous addressing versus default addressing.
	ip tcp header-compression	Enables TCP header compression.

async mode dedicated

To place a line into dedicated asynchronous mode using Serial Line Internet Protocol (SLIP) or PPP encapsulation, use the **async mode dedicated** command in interface configuration mode. Use the **no** form of this command to return the line to interactive mode.

async mode dedicated

no async mode dedicated

Syntax Description This command has no arguments or keywords.

Defaults Asynchronous mode is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines With dedicated asynchronous network mode, the interface will use either SLIP or PPP encapsulation, depending on which encapsulation method is configured for the interface. An EXEC prompt does not appear, and the router is not available for normal interactive use.

If you configure a line for dedicated mode, you will not be able to use the **async dynamic address** command, because there is no user prompt.

Examples The following example assigns an IP address to an asynchronous line and places the line into network mode. Setting the stop bits to 1 enhances performance.

```
interface async 4
  async default ip address 172.31.7.51
  async mode dedicated
  encapsulation slip

line 20
  location Joe's computer
  stopbits 1
  speed 115200
```

Related Commands	Command	Description
	async mode interactive	Returns a line that has been placed into dedicated asynchronous network mode to interactive mode, thereby enabling the slip and ppp EXEC commands.

async mode interactive

To return a line that has been placed into dedicated asynchronous network mode to interactive mode, thereby enabling the **slip** and **ppp** EXEC commands, use the **async mode interactive** command in interface configuration mode. Use the **no** form of this command to prevent users from implementing Serial Line Internet Protocol (SLIP) and PPP at the EXEC level.

async mode interactive

no async mode interactive

Syntax Description This command has no arguments or keywords.

Defaults Asynchronous mode is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Interactive mode enables the **slip** and **ppp** EXEC commands. In dedicated mode, there is no user EXEC level. The user does not enter any commands, and a connection is automatically established when the user logs in, according to the configuration.

Examples The following example places async interface 6 into interactive asynchronous mode:

```
interface async 6
  async default ip address 172.31.7.51
  async mode interactive
  ip unnumbered ethernet 0
```

Related Commands	Command	Description
	async mode dedicated	Places a line into dedicated asynchronous mode using SLIP or PPP encapsulation.

authen-before-forward

To configure a network access server (NAS) to request authentication of a complete username before making a forwarding decision for dial-in Layer 2 Tunnel Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnels belonging to a virtual private dialup network (VPDN) group, use the **authen-before-forward** command in VPDN group configuration mode. To disable this configuration, use the **no** form of this command.

authen-before-forward

no authen-before-forward

Syntax Description This command has no arguments or keywords.

Command Default L2TP or L2F tunnels are forwarded to the tunnel server without first requesting authentication of the complete username.

Command Modes VPDN group configuration

Command History

Release	Modification
11.3(9) AA	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T and was modified to be available only when the request-dialin VPDN subgroup is enabled.

Usage Guidelines

To configure the NAS to perform authentication of dial-in L2TP or L2F sessions belonging to a specific VPDN group before the sessions are forwarded to the tunnel server, use the **authen-before-forward** command in VPDN group configuration mode.

To configure the NAS to perform authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server, configure the **vpdn authen-before-forward** command in global configuration mode.

You must configure a request dial-in VPDN subgroup by issuing the **request-dialin** command before you can configure the **authen-before-forward** command. Removing the **request-dialin** configuration will remove the **authen-before-forward** command configuration from the VPDN group.

Enabling the **authen-before-forward** command instructs the NAS to authenticate the complete username before making a forwarding decision based on the domain portion of the username. A user may be forwarded or terminated locally depending on the information contained in the users RADIUS profile. Users with forwarding information in their RADIUS profile are forwarded based on that information. Users without forwarding information in their RADIUS profile are either forwarded or terminated locally based on the Service-Type in their RADIUS profile. The relationship between forwarding decisions and the information contained in the users RADIUS profile is summarized in Table 3.

Table 3 Forwarding Decisions Based on RADIUS Profile Attributes

Forwarding Information Is	Service-Type Is Outbound	Service-Type Is Not Outbound
Present in RADIUS profile	Forward User	Forward User
Absent from RADIUS profile	Check Domain	Terminate Locally

Examples

The following example configures an L2F request dial-in VPDN subgroup that sends the entire username to the authentication, authorization, and accounting (AAA) server when a user dials in with a username that includes the domain cisco.com:

```
vpdn-group 1
 request-dialin
  protocol l2f
  domain cisco.com
 initiate-to ip 10.0.0.1
 local name router32
 authen-before-forward
```

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
request-dialin	Configures a LAC to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, and specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or DNIS.
vpdn authen-before-forward	Configures a NAS to request authentication of a complete username before making a forwarding decision for all dial-in L2TP or L2F tunnels.

autocommand

To configure the Cisco IOS software to automatically execute a command when a user connects to a particular line, use the **autocommand** command in line configuration mode. Use the **no** form of this command to disable the automatic execution.

autocommand *command*

no autocommand *command*

Syntax Description

command Any appropriate EXEC command, including the host name and any switches that occur with the EXEC command.

Defaults

No commands are configured to automatically execute.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command enables you to automatically execute an EXEC command when a user connects to a line.

Examples

The following example forces an automatic connection to a host named host21 (which could be an IP address):

```
line vty 4
  autocommand connect host21
```

autodetect encapsulation

To enable automatic detection of the encapsulation types operating over a point-to-point link to a specified serial or ISDN interface, use the **autodetect encapsulation** command in interface configuration mode. To disable automatic dynamic detection of the encapsulation types on a link, use the **no** form of this command.

autodetect encapsulation {lapb-ta | ppp | v120}

no autodetect encapsulation {lapb-ta | ppp | v120}

Syntax Description	lapb-ta	Automatically detects Link Access Procedure, Balanced (LAPB) for an ISDN terminal adapter.
	ppp	Automatically detects PPP encapsulation on the interface.
	v120	Automatically detects V.120 encapsulation on B channels.

Defaults No default behavior or values.

Command Modes Interface configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.0(4)T	The lapb-ta keyword was added.

Usage Guidelines At least one encapsulation type is required in the command, but you can specify additional encapsulation types.

Use this command to enable the specified serial or ISDN interface to accept calls and dynamically change the encapsulation in effect on the interface when the remote device does not signal the call type. For example, if an ISDN call does not identify the call type in the Lower Layer Compatibility fields and is using an encapsulation that is different from the one configured on the interface, the interface can change its encapsulation type dynamically.

This command enables interoperation with ISDN terminal adapters that use V.120 encapsulation but do not signal V.120 in the call setup message. An ISDN interface that by default answers a call as synchronous serial with PPP encapsulation can change its encapsulation and answer such calls.

Autodetection of LAPB traffic on an ISDN terminal adapter is now possible, by adding the keyword **lapb-ta** to the command line. This allows recognition of incoming LAPB-TA calls.

Automatic detection is attempted for the first 10 seconds after the link is established or the first five packets exchanged over the link, whichever is first.

Examples

The following example configures BRI 0 to call and receive calls from two sites, use Point-to-Point Protocol (PPP) encapsulation on outgoing calls, and use Challenge Handshake Authentication Protocol (CHAP) authentication on incoming calls. This example also enables BRI 0 to configure itself dynamically to answer calls that use V.120 but that do not signal V.120.

```
interface bri 0
  encapsulation ppp
  autodetect encapsulation v120
  no keepalive
  dialer map ip 131.108.36.10 name EB1 234
  dialer map ip 131.108 36.9 name EB2 456
  dialer-group 1
  isdn spid1 0146334600
  isdn spid2 0146334610
  isdn T200 1000
  ppp authentication chap
```

The following example enables the LAPB-TA and V.120 protocols for autodetection on interface serial0:23 after you have configured the virtual terminals to handle asynchronous traffic:

```
vty-async
interface serial0:23
  autodetect encapsulation lapb-ta v120
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.

autohangup

To configure automatic line disconnect, use the **autohangup** command in line configuration mode. This command causes the EXEC to issue the **exit** command when the last connection closes. Use the **no** form of this command to disable automatic line disconnect.

autohangup

no autohangup

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command is useful for UNIX UNIX-to-UNIX Copy Program (UUCP) applications that automatically disconnect lines because UUCP scripts cannot issue the **exit** command to hang up the telephone.

Examples The following example enables automatic line disconnect on lines 5 through 10:

```
line 5 10
 autohangup
```

autoselect

To configure a line to start an Appletalk Remote Access (ARA), PPP, or Serial Line Internet Protocol (SLIP) session, use the **autoselect** command in line configuration mode. Use the **no** form of this command to disable this function on a line.

autoselect { **arap** | **ppp** | **slip** | **during-login** | **timeout** *seconds* }

no autoselect [*timeout*]

Syntax Description

arap	Configures the Cisco IOS software to allow an ARA session to start up automatically.
ppp	Configures the Cisco IOS software to allow a PPP session to start up automatically.
slip	Configures the Cisco IOS software to allow a SLIP session to start up automatically.
during-login	The username and/or password prompt is displayed without pressing the Return key. After the user logs in, the autoselect function begins.
timeout <i>seconds</i>	Sets a timeout period from 1 to 120 seconds for the autoselect process. This argument applies only when the arap , ppp , or slip keyword functions are enabled and has no effect when the during-login keyword function is enabled.

Defaults

ARA session
No timeout default

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3	The following keywords were added: <ul style="list-style-type: none"> • during-login • no autoselect • timeout <i>seconds</i>

Usage Guidelines

This command eliminates the need for users to enter an EXEC command to start an ARA, PPP, or SLIP session.



Note

SLIP does not support authentication. For PPP and ARAP, you must enable authentication.

The **autoselect** command configures the Cisco IOS software to identify the type of connection being requested. For example, when a user on a Macintosh running ARA selects the Connect button, the Cisco IOS software automatically starts an ARAP session. If, on the other hand, the user is running SLIP or PPP and uses the **autoselect ppp** or **autoselect slip** command, the Cisco IOS software automatically starts a PPP or SLIP session, respectively. This command is used on lines making different types of connections.

A line that does not have **autoselect** configured views an attempt to open a connection as noise. The router does not respond and the user client times out.

When a timeout period is configured and the initial sample byte is not received before that timeout period, a default EXEC process (if configured) is initiated.

**Note**

After the modem connection is established, a Return is required to evoke a response, such as to get the username prompt. You might need to update your scripts to include this requirement. Additionally, the activation character should be set to the default and the exec-character-bits set to 7. If you change these defaults, the application cannot recognize the activation request.

Examples

The following example enables ARA on a line:

```
line 3
 arap enable
 autoselect arap
```

The following example enables a timeout of 30 seconds on a PPP-enabled line:

```
line 7
 autoselect ppp
 autoselect timeout 30
```

The following example enables ARA on a line and allows logins from users with a modified CCL script and an unmodified script to log in:

```
line 3
 arap enable
 autoselect arap
 autoselect during-login
 arap nologin if-needed
```

Related Commands

Command	Description
arap use-tacacs	Enables TACACS for ARA authentication.
arap warningtime	Sets when a disconnect warning message is displayed.
ppp authentication chap	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication pap	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp bap call	Sets PPP BACP call parameters.
ppp use-tacacs	Enables TACACS for PPP authentication.

backup

To configure an IP backup endpoint address, enter the **backup** command in VPDN group configuration mode. To remove this function, enter the **no** form of this command.

backup ip *ip-address* [**limit number** [**priority number**]]

no backup ip *ip-address* [**limit number** [**priority number**]]

Syntax Description

ip <i>ip-address</i>	IP address of the HGW/LNS at the other end of the tunnel. This is the IP endpoint at the end of the tunnel, which is an HGW/LNS router.
limit number	(Optional) Limits sessions per backup. The limit can range from 0 to 32767. The default is no limit set.
priority number	(Optional) Priority level. Loadsharing is priority 1. Backup priority is between 2 and 32,767. The highest priority is 2, which is the first home gateway router to receive backup traffic. The lowest priority is 32,767. The priority group is used to support multiple levels of loadsharing and backup. The default is the lowest priority.

Defaults

No default behavior or values. This function is used only if it is configured.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced and applies to Cisco AS5200 and Cisco AS5300 access servers only.

Usage Guidelines

Use the **backup** VPDN group configuration command to configure an IP backup endpoint address.

Examples

The following examples show that the **backup** command is not available in the command line interface until you enter the **request dialin** command:

```
Router(config-vpdn)# vpdn-group customer1-vpdngroup
```

```
Router(config-vpdn)# ?
```

```
VPDN group configuration commands:
```

```
  accept  Accept a tunnel open request
  default Set a command to its defaults
  exit    Exit from VPDN group configuration mode
  no     Negate a command or set its defaults
  request Request to open a tunnel
```

```
Router(config-vpdn)# request dialin l2tp ip 10.2.2.2 domain customerx
```

```
?
```

```
VPDN group configuration commands:
```

```
  backup      Add backup address
  default     Set a command to its defaults
  dnis        Accept a DNIS tunnel
  domain      Accept a domain tunnel
  exit        Exit from VPDN group configuration mode
  force-local-chap Force a CHAP challenge to be instigated locally
  l2tp        L2TP specific commands
  lcp         LCP specific commands
  loadsharing Add loadsharing address
  local       local information, like name
  multilink   Configure limits for Multilink
  no         Negate a command or set its defaults
  request     Request to open a tunnel
```

The following example shows an IP backup endpoint address of 10.1.1.1 configured with a backup session limit of 5:

```
Router(config-vpdn)# backup ip 10.1.1.1 limit 5
```

Related Commands

Command	Description
request dialin	Configures a VPDN group to request L2F or L2TP tunnels to a home gateway and creates a request-dialin VPDN subgroup.

backup delay

To define how much time should elapse before a secondary line status changes after a primary line status has changed, use the **backup delay** command in interface configuration mode. Use the **no** form of this command to return to the default, so that as soon as the primary fails, the secondary is immediately brought up without delay.

backup delay {*enable-delay* | **never**} {*disable-delay* | **never**}

no backup delay {*enable-delay* | **never**} {*disable-delay* | **never**}

Syntax Description

<i>enable-delay</i>	Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line.
<i>disable-delay</i>	Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line.
never	Prevents the secondary line from being activated or deactivated.

Defaults

0 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

For environments in which spurious signal disruptions appear as intermittent lost carrier signals, we recommend that you enable some delay before activating and deactivating a secondary line.

Examples

The following example sets a 10-second delay on deactivating the secondary line (serial interface 0); however, the line is activated immediately:

```
interface serial 0
 backup delay 0 10
```

backup interface

To configure an interface as a secondary or dial backup, use the **backup interface** command in interface configuration mode. Use the **no** form of this command to disable this feature.

backup interface *type number*

no backup interface *type number*

Cisco 7200 series and Cisco 7500 series routers

backup interface *slot/port-adapter/port*

no backup interface *slot/port-adapter/port*

Syntax	Description
<i>type number</i>	Interface type and port number to use as the backup interface.
<i>slot/port-adapter/port</i>	Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines The interface you define with this command can back up only one other interface.

Examples The following example sets serial 1 as the backup line to serial 0:

```
interface serial 0
 backup interface serial 1
```

backup interface dialer

To configure a dialer interface as a secondary or dial backup, use the **backup interface dialer** command in interface configuration mode. Use the **no** form of this command to disable this feature.

backup interface dialer *number*

no backup interface dialer *number*

Syntax Description	<i>number</i>	Dialer interface number to use as the backup interface.
Defaults	Disabled	
Command Modes	Interface configuration	
Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Multiple dialer interfaces can use the same dialer pool, which might have a single ISDN interface as a member. Thus, that ISDN interface can back up different serial interfaces and can make calls to different sites.

Examples The following example shows the configuration of a site that backs up two leased lines using one BRI. Two dialer interfaces are defined. Each serial (leased line) interface is configured to use one of the dialer interfaces as a backup. Both of the dialer interfaces use dialer pool 1, which has BRI 0 as a member. Thus, BRI 0 can back up two different serial interfaces and can make calls to two different sites.

```
interface dialer0
 ip unnumbered loopback0
 encapsulation ppp
 dialer remote-name Remote0
 dialer pool 1
 dialer string 5551212
 dialer-group 1

interface dialer1
 ip unnumbered loopback0
 encapsulation ppp
 dialer remote-name Remote1
 dialer pool 1
 dialer string 5551234
 dialer-group 1

interface bri 0
 encapsulation PPP
 dialer pool-member 1
 ppp authentication chap
```

```
interface serial 0
 ip unnumbered loopback0
 backup interface dialer 0
 backup delay 5 10
```

```
interface serial 1
 ip unnumbered loopback0
 backup interface dialer1
 backup delay 5 10
```

backup load

To set a traffic load threshold for dial backup service, use the **backup load** command in interface configuration mode. To return to the default value, use the **no** form of this command.

backup load {*enable-threshold* | **never**} {*disable-load* | **never**}

no backup load {*enable-threshold* | **never**} {*disable-load* | **never**}

Syntax Description

<i>enable-threshold</i>	Percentage of the primary line's available bandwidth that the traffic load must exceed to enable dial backup.
<i>disable-load</i>	Percentage of the available bandwidth that the traffic load must be less than to disable dial backup. The transmitted or received load on the primary line plus the transmitted or received load on the secondary line is less than the value entered for the <i>disable-load</i> argument to disable dial backup.
never	The secondary line is never activated or deactivated because of the traffic load.

Defaults

No threshold is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the transmitted or received load on the primary line is greater than the value assigned to the *enable-threshold* argument, the secondary line is enabled.

The secondary line is disabled when one of the following conditions occurs:

- The transmitted load on the primary line plus the transmitted load on the secondary line is less than the value entered for the *disable-load* argument.
- The received load on the primary line plus the received load on the secondary line is less than the value entered for the *disable-load* argument.

If the **never** keyword is used instead of an *enable-threshold* argument, the secondary line is never activated because of traffic load. If the **never** keyword is used instead of a *disable-load* argument, the secondary line is never activated because of traffic load.

Examples

The following example sets the traffic load threshold to 60 percent of the primary line serial 0. When that load is exceeded, the secondary line is activated and will not be deactivated until the combined load is less than 5 percent of the primary bandwidth.

```
interface serial 0
 backup load 60 5
 backup interface serial 1
```

busy-message

To create a “host failed” message that displays when a connection fails, use the **busy-message** command in global configuration mode. Use the **no** form of this command to disable the “host failed” message from displaying on the specified host.

busy-message *hostname d message d*

no busy-message *hostname*

Syntax Description		
	<i>hostname</i>	Name of the host that cannot be reached.
	<i>d</i>	Delimiting character of your choice—a pound sign (#) for example. You cannot use the delimiting character in the message.
	<i>message</i>	Message text.

Defaults No message is displayed.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command applies only to Telnet connections.

Follow the **busy-message** command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Defining a “host failed” message for a host prevents all Cisco IOS software-initiated user messages, including the initial message that indicates the connection is “Trying...” The **busy-message** command can be used in the **autocommand** command to suppress these messages.

Examples The following example sets a message that will be displayed on the terminal whenever an attempt to connect to the host named dross fails. The pound sign (#) is used as a delimiting character.

```
busy-message dross #
Cannot connect to host. Contact the computer center.
#
```

busyout

To inform the central-office switch that a channel is out-of-service, use the **busyout** command in privileged EXEC mode. This command does not terminate an existing call; instead, after you hang up or end a call, a new call cannot be established on a channel that has received a **busyout** command instruction.

To busyout an entire card on the dial shelf and remove it from dial services, use the **busyout** privileged EXEC command. To cancel busyout, use the **no** form of the command.

busyout *shelfslot/port*

no busyout *shelfslot/port*

Syntax Description

<i>shelfslot/port</i>	Shelf number, slot number, and port number. You must type in the forward slashes (/).
-----------------------	---

Defaults

Busyout is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced and supported T1 and T3 only.
12.0	This command was enhanced to support T1, T3, E1 and DMM HMM (Double Modem Module [12] Hex Modem Module [6]).

Usage Guidelines

Use the **busyout** command before you remove a card from a shelf. The maintenance LED on the card goes ON after all the channels (or calls) have been terminated. The ON LED indicates that it is safe to remove the card from the shelf.

Use this command to busyout digital signal level 0s (DS0s) on a trunk card or all modems on a modem card.

To busyout an individual DS0, use the **ds0 busyout** controller configuration command.

To display the busyout information, use the **show busyout** privileged EXEC command.

Restrictions

If the trunk card is using ISDN signalling, there is a limit on the amount of traffic that the exchange can accept on the signalling channel. The restrictions are as follows:

- A Busyout can take 1 or 2 minutes to complete for a T1 or T2 trunk card.
- The **no busyout** command cannot be used within 3 minutes of **busyout** and vice versa; otherwise, the command will be rejected.

Examples

The following example enables busyout on the card in dial shelf 5, slot 4:

```
busyout 5/4
```

Related Commands

Command	Description
ds0 busyout	Busyouts one or more DS0s.
modem busyout	Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state.
modem busyout-threshold	Maintains a balance between the number of DS0s and modems.
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.
show dial-shelf	Displays information about the dial shelf, including clocking information.

■ busyout