



Dial Technologies Commands

This chapter presents the commands to configure and maintain Cisco IOS dial and access applications in alphabetical order. See the “Introduction” chapter for information about the types of applications and configurations these commands are used in. Some commands required for configuring dial and access configurations 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	RADIUS static route download.
tacacs+	TACACS+ 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 static route download 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 this command.

```
aaa route download [time] [authorization method-list]
```

```
no aaa route download
```

Syntax Description

<i>time</i>	(Optional) Time between downloads, in minutes. The range is from 1 to 1440 minutes.
authorization <i>method-list</i>	(Optional) Specify a named method list to which RADIUS authorization requests for static route downloads are sent. If these attributes are not set, all RADIUS authorization requests will be sent to the servers that are specified by the default method list.

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.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2(8)T	The authorization keyword was added; the <i>method-list</i> argument was added.

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
```

The following example sets the AAA route update period to 10 minutes and sends static route download requests to the servers specified by the method list name "list1":

```
aaa route download 10 authorization list1
```

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.

accept-dialin

To create an accept dial-in VPDN subgroup that configures a tunnel server to accept requests from a network access server (NAS) to tunnel dial-in calls, and to enter accept dial-in VPDN subgroup configuration mode, use the **accept-dialin** command in VPDN group configuration mode. To remove the accept dial-in VPDN subgroup configuration from a virtual private dialup network (VPDN) group, use the **no** form of this command.

accept-dialin

no accept-dialin

Syntax Description This command has no arguments or keywords.

Defaults No accept dial-in VPDN subgroups are configured.

Command Modes VPDN group configuration

Command History	Release	Modification
	11.3(5)AA	This command was introduced and replaced the vpdn incoming command used in Cisco IOS Release 11.3.
	12.0(1)T	This command was implemented on additional router and access server platforms.
	12.0(5)T	The original keywords and arguments were removed and made into separate accept-dialin subgroup commands.
	12.1(1)T	This command was enhanced to support dial-in Point-to-Point Protocol over Ethernet (PPPoE) calls.

Usage Guidelines Use the **accept-dialin** command on a tunnel server to configure a VPDN group to accept requests to establish dial-in VPDN tunnels from a NAS. Once the tunnel server accepts the request from a NAS, it uses the specified virtual template to clone new virtual access interfaces.

To configure a VPDN group to accept dial-in calls, you must also configure the following commands:

- The **protocol** command from accept dial-in VPDN subgroup configuration mode
- The **virtual-template** command from accept dial-in VPDN subgroup configuration mode
- The **terminate-from** command in VPDN group configuration mode



Note

If you create a VPDN group without configuring a **terminate-from** command, a default VPDN group is automatically enabled. Incoming tunnel requests from any hostname will use the attributes specified in the default VPDN group, unless a specific VPDN group is configured with a **terminate-from** command using that hostname.

Typically, you need one VPDN group for each NAS that will be tunneling to the tunnel server. For a tunnel server that services many NASs, the configuration can become cumbersome. If all the NASs will share the same tunnel attributes, you can simplify the configuration by using the default VPDN group configuration, or by creating a VPDN default group template using the **vpdn-template** command.

The tunnel server can also be configured to request the establishment of Layer 2 Tunnel Protocol (L2TP) dial-out VPDN tunnels to a NAS using the **request-dialout** command. Dial-in and dial-out calls can use the same L2TP tunnel.

Examples

The following example enables the tunnel server to accept Layer 2 Forwarding (L2F) tunnels from a NAS named router23. A virtual-access interface will be cloned from virtual-template 1.

```
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2f
Router(config-vpdn-acc-in)# virtual-template 1
!
Router(config-vpdn)# terminate-from hostname router23
```

The following example configures the router so that tunnels requested by the NAS named router16 are created with the tunnel attributes specified by VPDN group 1, while any other incoming L2TP tunnel request will use the settings configured in the default VPDN group, VPDN group 2:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 2
!
Router(config-vpdn)# terminate-from hostname router16

Router(config)# vpdn-group 2
! Default L2TP VPDN group
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 3
```

Related Commands

Command	Description
protocol (VPDN)	Specifies the tunneling protocol that a VPDN subgroup will use.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
request-dialout	Creates a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out L2TP tunnels to a NAS, and enters request dial-out VPDN subgroup configuration mode.
terminate-from	Specifies the hostname 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.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.
vpdn-template	Enters VPDN template configuration mode to configure a VPDN template.

accept-dialout

To create an accept dial-out VPDN subgroup that configures a network access server (NAS) to accept requests from a tunnel server to tunnel Layer 2 Tunneling Protocol (L2TP) dial-out calls, and to enter accept dial-out VPDN subgroup configuration mode, use the **accept-dialout** command in VPDN group configuration mode. To remove the accept dial-out VPDN subgroup configuration from the virtual private dialup network (VPDN) group, use the **no** form of this command.

accept-dialout

no accept-dialout

Syntax Description This command has no arguments or keywords.

Defaults No accept dial-out VPDN subgroups are configured.

Command Modes VPDN group configuration

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

Usage Guidelines Use the **accept-dialout** command on a NAS to configure a VPDN group to accept requests for dial-out VPDN tunnels from a tunnel server. L2TP is the only tunneling protocol that can be used for dial-out VPDN tunnels.

For a VPDN group to accept dial-out calls, you must also configure the following commands:

- The **terminate-from** command in VPDN group configuration mode
- The **protocol l2tp** command in accept dial-out VPDN subgroup configuration mode
- The **dialer** command in accept dial-out VPDN subgroup configuration mode
- The **dialer aaa** command in dialer interface configuration mode

The NAS can also be configured to request the establishment of dial-in VPDN tunnels to a tunnel server using the **request-dialin** command. Dial-in and dial-out calls can use the same L2TP tunnel.

Examples The following example configures a VPDN group on the NAS to accept L2TP tunnels for dial-out calls from the tunnel server TS23 using dialer 2 as its dialing resource:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialout
Router(config-vpdn-acc-ou)# protocol l2tp
Router(config-vpdn-acc-ou)# dialer 2
!
Router(config-vpdn)# terminate-from hostname TS23
!
```

■ accept-dialout

```

Router(config)# interface Dialer2
Router(config-if)# ip unnumbered Ethernet0
Router(config-if)# encapsulation ppp
Router(config-if)# dialer in-band
Router(config-if)# dialer aaa
Router(config-if)# dialer-group 1
Router(config-if)# 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 tunneling protocol that a VPDN subgroup will use.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
request-dialout	Creates a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out L2TP tunnels to a NAS, and enters request dial-out VPDN subgroup configuration mode.
terminate-from	Specifies the hostname of the remote router that will be required when accepting a VPDN tunnel.

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.
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.

async default routing



Note

Beginning in Cisco IOS Release 12.3(11)T, the **async default routing** command is replaced by the **routing dynamic** command. See the **routing dynamic** command for more information.

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

async default routing

no async default routing

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(11)T	This command was replaced by the routing dynamic command.

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. To disable dynamic addressing, use the **no** form of this command.

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 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 asynchronous 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. To disable routing protocols, use the **no** form of this command; 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

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
  peer default IP address 10.1.1.2
  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. To return the line to interactive mode, use the **no** form of this command.

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
 peer 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. To prevent users from implementing Serial Line Internet Protocol (SLIP) and PPP at the EXEC level, use the **no** form of this command.

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 asynchronous interface 6 into interactive asynchronous mode:

```
interface async 6
peer 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 1](#).

Table 1 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.

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	Keyword	Description
	lapb-ta	Link Access Procedure, Balanced (LAPB) for an ISDN terminal adapter.
	ppp	PPP encapsulation on the interface.
	v120	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 172.17.36.10 name EB1 234
  dialer map ip 172.17.36.9 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 the serial interface after you have configured the virtual terminals to handle asynchronous traffic:

```
vtty-asynch
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. To disable automatic line disconnect, use the **no** form of this command.

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 causes the EXEC to issue the **exit** command when the last connection closes. The **autohangup** command is useful for the 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. To disable this function on a line, use the **no** form of this command.

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

```
no autoselect [timeout]
```

Syntax Description

arap	ARA session.
ppp	PPP session.
slip	SLIP session.
during-login	Displays the username and/or password prompt without the user pressing the Return key. After the user logs in, the autoselect function begins.
timeout seconds	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 seconds

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 noguest if-needed
```

Related Commands

Command	Description
arap use-tacacs	Enables TACACS for ARA authentication.
arap warning time	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, use 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 <i>number</i>	(Optional) Limits sessions per backup. The limit can range from 0 to 32767. The default is no limit set.
priority <i>number</i>	(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 on the following platforms only: Cisco AS5200 and Cisco AS5300.

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-group customer1-vpdngroup

Router(config-vpdn)# ?

VPDN group configuration commands:
  accept-dialin  VPDN accept-dialin group configuration
  accept-dialout VPDN accept-dialout group configuration
  default        Set a command to its defaults
  description    Description for this VPDN group
  exit          Exit from VPDN group configuration mode
  ip            IP settings for tunnel
  no            Negate a command or set its defaults
  request-dialin VPDN request-dialin group configuration
```

```
request-dialout  VPDN request-dialout group configuration
source-ip       Set source IP address for this vpdn-group
```

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

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

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 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.

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. To return to the default so that as soon as the primary fails, the secondary is immediately brought up without delay, use the **no** form of this command.

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

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

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

Defaults 0 second delay

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. To disable this feature, use the **no** form of this command.

Cisco 7200 Series and Cisco 7500 Series Routers Only

backup interface *slot/port-adapter/port*

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

Other Cisco Routers

backup interface *interface-type interface-number*

no backup interface *interface-type interface-number*

Syntax Description		
	<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.
	<i>interface-type</i> <i>interface-number</i>	Interface type and port number to use as the backup interface.

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.



Note

Routers support only serial and ISDN backup interfaces. Access servers support both asynchronous and serial backup interfaces.

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. To disable this feature, use the **no** form of this command.

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
```

■ backup interface dialer

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

```
interface serial 1
 ip unnumbered loopback0
 backup interface dialer 1
 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
```

busyout (port)

To disable a port by waiting for the active services on the specified port to terminate, use the **busyout** command in port configuration mode. To reenble the ports, use the **no** form of this command.

busyout

no busyout

Syntax Description This command has no arguments or keywords.

Defaults Busyout is not enabled.

Command Modes Port configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **busyout** command disables a port by waiting for the active services on the specified port to terminate. Use the **no** form of this command to reenble the ports.

Examples

The following example will disable service processing element (SPE) ports 1 to 10 on slot 1 once active services have terminated:

```
Router(config)# port 1/1 1/10
Router(config-port)# busyout
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
shutdown (port)	Disables a port.
show spe	Displays SPE status.

busyout (privileged EXEC)

To inform a central-office switch that a channel is out-of-service, and to busyout an entire card on a dial shelf and remove it from dial services, use the **busyout** (privileged EXEC) command in privileged EXEC mode. To cancel busyout, use the **no** form of this command.

busyout *shelfslotport*

no busyout *shelfslotport*

Syntax Description

shelfslotport Shelf number, slot number, and port number. You must include the slash marks.

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 E1 and DMM HMM (Double Modem Module [12] Hex Modem Module [6]).

Usage Guidelines

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.

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 signaling, there is a limit on the amount of traffic that the exchange can accept on the signaling 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 the **busyout** command 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 (channel)	Forces a DS0 timeslot on a controller into the busyout state.
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 (spe)

To disable active calls on the specified service processing elements (SPEs), use the **busyout** command in SPE configuration mode. To reenable the SPEs, use the **no** form of this command.

busyout

no busyout

Syntax Description This command has no arguments or keywords.

Defaults Busyout is not enabled.

Command Modes SPE configuration

Command History	Release	Modification
	12.1(1)XD	This command was introduced on the Cisco AS5400.
	12.1(3)T	This command was implemented on the Cisco AS5800.
	12.1(5)XM1	This command was implemented on the Cisco AS5350.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines You can perform autodiagnostic tests and firmware upgrades when you put the SPEs in the Busyout state. Active ports on the specified SPE will change the state of the specified range of SPEs to the BusyoutPending state. The state changes from BusyoutPending to Busyout when all calls end. Use the **show spe** command to display the state of the range of SPEs. Use the **shutdown** command to override the **busyout** command. Use the **no busyout** command to reenable the SPEs.

Examples The following example shows all active ports on SPE 1 to 10 on slot 1 being busied out:

```
spe 1/1 1/10
  busyout
```

Related Commands	Command	Description
	clear port	Resets the NextPort port and clears any active call.
	clear spe	Reboots all specified SPEs.
	shutdown (port)	Disables a port.
	show spe	Displays SPE status.

call progress tone country

To specify the country code for retrieving the call progress tone parameters from the call progress tone database, use the **call progress tone country** command in global configuration mode. To cancel the previous setting and to generate the call progress tones according to modem settings, use the **no** version of this command.

call progress tone country *country-name*

no call progress tone country *country-name*

Syntax Description

<i>country-name</i>	Selects default call progress tones (ring and cadence settings) for the specified country. Valid entries are: argentina, australia, austria, belgium, brazil, canada, china, colombia, cyprus, czech-republic, denmark, finland, france, germany, greece, hongkong, hungary, iceland, india, indonesia, ireland, israel, italy, japan, korea, luxembourg, malaysia, mexico, netherlands, peru, philippines, poland, portugal, russia, singapore, slovakia, slovenia, south-africa, spain, sweden, switzerland, taiwan, thailand, turkey, unitedkingdom, usa, and venezuela.
---------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Defaults

Default modem settings. (The *country-name* keyword **northamerica** was the default in Cisco IOS Releases earlier than release 12.0(3)XG; **usa** is the default country keyword for Cisco IOS Release 12.0(3)XG and later releases.)

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced.
12.0(4)XI	This command was enhanced with additional country keywords.

Usage Guidelines

Use the **call progress tone country** configuration to specify the country for call progress tone generation. While in many cases the country is chosen automatically on the basis of the modem setting, automatic selection does not work for all users because many modems do not support all countries and many users choose the “us” or “default-t1” or “default-e1” setting on their modem.

This command affects the tones generated at the local interface and does not affect any information passed to the remote end of a connection or any tones generated at the remote end of a connection.

For dial platforms (AS5200, AS5300, and AS5800), call progress tones are used only for the resource pool management application. Resource pool management assumes that the call progress tone selection is global. Select only one call progress tone set, and it will globally override country settings on all ports.

Examples

The following example shows the call progress tone set for Japan tone parameters:

```
call progress tone country japan
```

Related Commands

Command	Description
show call progress tone	Displays the contents of the internal CP tone database for a specific country.

callback forced-wait

To force the Cisco IOS software to wait before initiating a callback to a requesting client, use the **callback forced-wait** command in global configuration mode. To disable the forced waiting period, use the **no** form of this command.

callback forced-wait

no callback forced-wait

Syntax Description This command has no arguments or keywords.

Defaults The forced waiting period is not set.

Command Modes Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command when the router is calling back a modem that initiated a call, then dropped the connection, but requires a rest period before subsequent input is accepted.

Examples

The following example sets a waiting period during which a callback chat script is delayed from being sent on an outgoing target line:

```
callback forced-wait
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
chat-script	Places calls over a modem and logs in to remote systems.
debug callback	Displays callback events when the router is using a modem and a chat script to call back on a terminal line.
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)	Defines the IP addresses of the server.

called-number (modem pool)

To assign a called party number to a pool of modems, use the **called-number** command in modem pool configuration mode. To remove a number from a modem pool, use the **no** form of this command.

called-number *number* [**max-conn** *number*]

no called-number *number* [**max-conn** *number*]

Syntax Description

<i>number</i>	Called number for a modem pool.
max-conn <i>number</i>	(Optional) Maximum number of simultaneous connections allowed for the called party number.

Defaults

Disabled

Command Modes

Modem pool configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

A called party number is a telephone number that is used to reach a remote destination. For example, a mobile laptop dials a called party number to reach the POP of an ISP. Some ISPs set up several called party numbers to enable remote clients to dial in, but to the end user, it appears and functions as one unified service.

Cisco's implementation of a called party number is based on the dialed number identification service (DNIS). You can configure multiple DNIS numbers in a single modem pool. However, the same DNIS number cannot be used in multiple modem pools. Each modem pool must be assigned different DNIS numbers.

Use the **max-conn** option to provide overflow protection, which specifies a maximum number of simultaneous connections that a called party number can consume. For example, if you create one modem pool to serve two or more services or customers, this option guarantees how many modems each service or customer can have access to at any given time.

The Cisco IOS software also includes a feature that simplifies the called number configuration. By using an x variable as the last digit in a called telephone number (for example, issuing the **called-number 408555121x** command), clients dialing different called numbers such as 4085551214 or 4085551215 will automatically be sent to the same modem pool. The x variable is a floating place holder for digits 1 through 9.



Note

Modem pools using MICA technologies or Microcom modems support incoming analog calls over ISDN PRI. However, only MICA modems support modem pooling for CT1 and CE1 configurations with channel associated signaling.

Examples

In the following example, the modem pool called v90service is virtually partitioned between two customers using different DNIS numbers. The **pool-range** command assigns modems 1 to 110 to the shared modem pool. The **called-number 5551212 max-conn 55** command assigns the DNIS number 5551212 to the v90service modem pool. The total number of simultaneous connections is limited to 55. The **called-number 4441212 max-conn 55** command assigns the DNIS number 4441212, which is for a different customer, to the same v90service modem pool. The total number of simultaneous connections is also set to 55.

```
modem-pool v90service
  pool-range 1-110
  called-number 5551212 max-conn 55
  called-number 4441212 max-conn 55
```

The following configuration rejects the **pool-range 30** command because modem TTY line 30 is already a member of the modem pool v90service, which was configured in the previous example. Each modem in the access server is automatically assigned to a unique TTY line. TTY line numbers are assigned according to your shelf, slot, or port hardware configuration.

```
modem-pool v34service
# pool-range 30
```

Related Commands

Command	Description
clear modempool-counters	Clears active or running counters associated with one or more modem pools.
modem-pool	Creates a new modem pool or specifies an existing modem pool, which allows you to physically or virtually partition your access server for dial-in and dial-out access.
pool-range	Assigns a range of modems to a modem pool.
show modem-pool	Displays the configuration and connection status for one or more modem pools.

calltracker call-record

To enable call record SYSLOG generation for the purpose of debugging, monitoring, or externally saving detailed call record information, use the **calltracker call-record** command in global configuration mode. To disable call record SYSLOG generation, use the **no** form of this command.

```
calltracker call-record {terse | verbose} [quiet]
```

```
no calltracker call-record {terse | verbose} [quiet]
```

Syntax Description

terse	Generates a brief set of call records containing a subset of the data stored within Call Tracker used primarily to manage calls.
verbose	Generates a complete set of call-records containing all of the data stored within Call Tracker used primarily to debug calls.
quiet	(Optional) Call record will be sent only to configured SYSLOG server and not to console.

Defaults

Call Tracker call record logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

SYSLOG call records will be generated in the order of ten seconds of call termination. A small delay is needed to ensure that all subsystems finish reporting all appropriate information on call termination. Furthermore, the process of logging is considered a very low priority with respect to normal call processing and data routing. As such, logging all call records can be guaranteed if Call Tracker is properly configured. However, the delay from the time a call actually terminated can vary if the CPU is busy handling higher-priority processes.

Call Tracker records must be found within the History table for at least one minute after call termination for this capability to work. As such, one must ensure that Call Tracker history collection is not disabled with the **calltracker history** configuration options.

Because the call rates possible on a high-capacity access server can be rather large and the information provided by the call records is substantial, simply enabling normal SYSLOG call records can make the use of the console difficult. As such, by using the **quiet** option and having a SYSLOG server configured to capture the call records, the console can be freed from displaying any call records, yet still have the call records captured by a SYSLOG server.

Related Commands

Command	Description
calltracker history max-size	Sets the maximum calls saved in the history table.
calltracker history retain-mins	Sets the number of minutes to save calls in the history table.
calltracker timestamp	Displays the millisecond value of the call setup time in the Call Record (CDR) on the access server.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

calltracker enable

To enable Call Tracker on the access server, use the **calltracker enable** command in global configuration mode. To restore the default condition, use the **no** form of this command.

calltracker enable

no calltracker enable

Syntax Description This command has no arguments or keywords.

Defaults Call Tracker is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Usage Guidelines To enable real-time call statistics from the MICA technologies modem to Call Tracker, you must configure the **modem link-info poll time** command.

Examples The following shows how to enable the Call Tracker feature:

```
calltracker enable
calltracker history max-size number
calltracker history retain-mins minutes
calltracker call-record terse
snmp-server packet-size byte-count
snmp-server queue-length length
snmp-server enable traps calltracker
snmp-server host host community-string calltracker
```

Related Commands	Command	Description
	calltracker history max-size	Sets the maximum calls saved in the history table.
	calltracker history retain-mins	Sets the number of minutes to save calls in the history table.
	calltracker timestamp	Displays the millisecond value of the call setup time in the Call Record (CDR) on the access server.
	debug calltracker	Displays debug messages tracing the Call Tracker processing flow.
	dnis	Enables Call Tracker SYSLOG support for generating detailed Call Records.
	modem link-info poll time	Sets the polling interval at which link statistics are retrieved from the MICA modem.

show call calltracker active	Displays all information stored within the Call Tracker active database for all active calls.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.
snmp-server host	Specifies the host to receive Call Tracker traps.

calltracker history max-size

To set the maximum number of call entries stored in the Call Tracker history table, use the **calltracker history max-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

calltracker history max-size *number*

no calltracker history max-size *number*

Syntax Description

<i>number</i>	Maximum call entries to store in the Call Tracker history table. The valid range is from 0 through 10 times the maximum DS0 supported on a platform. A value of 0 prevents any history from being saved.
---------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Defaults

The default maximum is dynamically calculated to be 1 times the maximum DS0 supported on a platform.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Be careful when extending the maximum number of call entries stored in the Call Tracker history table, as this activity causes Call Tracker to use more memory resources to store the additional call data. Network access server memory consumption must be considered when increasing this parameter. The active call table is not affected by this command.

Examples

The following example sets the history table size to 50 calls:

```
calltracker history max-size 50
```

Related Commands

Command	Description
calltracker history retain-mins	Sets the number of minutes to save calls in the history table.
calltracker timestamp	Displays the millisecond value of the call setup time in the Call Record (CDR) on the access server.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

calltracker history retain-mins

To set the number of minutes for which call entries are stored in the Call Tracker history table, use the **calltracker history retain-mins** command in global configuration mode. To restore the default value, use the **no** form of this command.

calltracker history retain-mins *minutes*

no calltracker history retain-mins *minutes*

Syntax Description	<i>minutes</i>	The length of time to store calls in the Call Tracker history table. The valid range is from 0 through 26,000 minutes. A value of 0 prevents any history from being saved.
---------------------------	----------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Defaults	The default number of minutes is 5000.
-----------------	----------------------------------------

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

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Usage Guidelines	Active calls are not affected by this command. Entries in the active table are retained as long as the calls are connected.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------

Examples	The following example sets the retention time for the history table to 5000 minutes:
-----------------	--------------------------------------------------------------------------------------

```
calltracker history retain-mins 5000
```

Related Commands	Command	Description
	calltracker history max-size	Sets the maximum calls saved in the history table.
	calltracker timestamp	Displays the millisecond value of the call setup time in the Call Record (CDR) on the access server.
	show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
	show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

calltracker timestamp

To display the millisecond value of the call setup time in the Call Record (CDR) on the access server, use the **calltracker timestamp** command in global configuration mode. To restore the default value, use the no form of this command.

calltracker timestamp msec

no calltracker timestamp msec

Syntax Description This command has no arguments or keywords.

Defaults The default value of the call setup time does not contain milliseconds. It is in the hh:mm:ss form.

Command Modes Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3.t.
12.4T	This command was integrated into Cisco IOS Release 12.4T.
12.4	This command was integrated into Cisco IOS Release 12.4.

Usage Guidelines

This AS5400 command is used to add a milliseconds timestamp (hh:mm:ss.ms) to call detail records. These call records of originating and terminating calls are written to flat files on the subscriber server. These files may be passed periodically from the subscriber to the publisher server. Third party applications such as billing and accounting use CDR data.

All calltracker commands (including calltracker timestamp) are only supported for dial services and not for voice.

Examples

The following configuration example shows calltracker options and a display of calltracker active including timestamp.

```
u5400#configure t
Enter configuration commands, one per line. End with CNTL/Z.
u5400(config)#calltracker ?
  call-record  Generate a SYSLOG Call Record at end of call
  enable      start calltracker
  history     Aspects of the CT History Table
  timestamp   CDR timestamp config

u5400(config)#calltracker timestamp ?
```

```

msec Shows millisecond value in timestamp

u5400(config)#calltracker timestamp msec ?
<cr>

u5400#show call calltracker active
----- call handle = 206 -----
status-Active, service=PPP, origin=Anser, category-Modem
DSO slot/port/dsl/chan=7/0/0/19, called=40852 68222,calling=(n/a)
userid=myusername, ip=10.1.1.2, mask=10.1.1.2
setup=08/05/2003 19.04.41.645, conn=0.01,phys=23.73,service=16.33,authen=26.33
init rx/tx b-rate=28800/28800,rx/tx chars=0/0
resource slot/port=4/97, mp bundle=0,charged units=0,acctid=198
ibd handle=0x0, tty handle=0x63B4F010, tcb handle=0x0

```

Related Commands

Command	Description
calltracker enable	Enables Call Tracker on the access server.
calltracker history retain-mins	Sets the number of minutes to save calls in the history table.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

call-type

To reject particular types of calls, use the **call-type** command in call discriminator profile configuration mode. To disable this feature, use the **no** form of this command.

call-type { **all** | **digital** | **speech** | **v110** | **v120** }

no call-type { **all** | **digital** | **speech** | **v110** | **v120** }

Syntax Description

all	All calls.
digital	Digital calls.
speech	Speech calls.
v110	V.110 calls.
v120	V.120 calls.

Defaults

All calls are accepted by the network access server.

Command Modes

Call discriminator profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **call-type** call discriminator command to reject particular types of calls. Call type **all** is mutually exclusive for all other call types. If call type **all** is set in the discriminator, no other call types are allowed. Also, once a DNIS is associated with a call type in a discriminator, it cannot be used in any other discriminator.

Examples

The following example shows the call discriminator being configured to reject speech calls for the call discriminator profile named “userd3”:

```
resource-pool profile discriminator userd3
  call-type speech
```

call-type cas

To statically set the call-type override for incoming channel-associated signaling (CAS) calls, use the **call-type cas** command in DNIS group configuration mode. To disable this service, use the **no** form of this command.

call-type cas {digital | speech}

no call-type cas {digital | speech}

Syntax Description

digital	Override call type to digital. The incoming call with the DNIS in the called group is treated as a digital call type.
speech	Override call-type to speech. The incoming call with the DNIS in the called group is treated as a speech call type.

Defaults

No default behavior or values.

Command Modes

DNIS group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **call-type cas** DNIS group configuration command to set the call-type override. From the resource pooling call-type perspective, use CT1 (CAS) to support either analog calls (speech) or digital calls (switched 56K).

Switched 56K calls are digital calls that connect to High-Level Data Link Control (HDLC) framers. Unlike ISDN, it is impossible to communicate the call type in CT1. Therefore, switched 56K services in CT1 can be differentiated by the DNIS numbers. This command identifies that the call arriving with the DNIS in the DNIS group is assigned to the call type specified in the command.

Examples

The following example shows the DNIS group configuration mode being accessed to use the **call-type cas** command to set the call type override for CAS to **speech**:

```
dialer dnis group modem-group1
  call-type cas speech
```

cas-group (E1 controller)

To configure channel-associated signaling (CAS) on an E1 controller, use the **cas-group** command in controller configuration mode. To disable CAS for one or more time slots, use the **no** form of this command.

cas-group *channel timeslots range type signal*

no cas-group *channel timeslots range type signal*

Syntax Description

<i>channel</i>	Single channel group number from 0 to 30.
timeslots <i>range</i>	Time slot or time slot range, which can be from 1 to 31. You can specify a time slot range (for example, 1-29), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). The 16th time slot is reserved for out-of-band signaling.
type <i>signal</i>	Type of CAS. Configure the signal type that your central office uses. For Cisco 5800 series access servers, replace the <i>signal</i> keyword with one of the following signal types: <ul style="list-style-type: none"> • e&m-fgb [dtmf [dnis] mf [dnis]]—Specifies ear and mouth channel signaling with feature group B support, which includes the wink-start protocol. The optional signal tones are DTMF and MF with the option of provisioning DNIS. • e&m-fgd—Specifies ear and mouth channel signaling with feature group D support, which includes the wink-start protocol. • e&m-immediate-start—Specifies ear and mouth channel signaling with immediate-start support. • fxs-ground-start—Specifies Foreign Exchange Station ground-start signaling support. • fxs-loop-start—Specifies Foreign Exchange Station loop-start signaling support. • p7—Specifies the P7 switch type. • r2-analog [dtmf r2-compelled [ani] r2-non-compelled [ani] r2-semi-compelled [ani]] • r2-digital [dtmf r2-compelled [ani] r2-non-compelled [ani] r2-semi-compelled [ani]] • r2-pulse [dtmf r2-compelled [ani] r2-non-compelled [ani] r2-semi-compelled [ani]] • sas-ground-start—Specifies Special Access Station ground-start signaling support. • sas-loop-start—Specifies Special Access Station loop-start signaling support.

type <i>signal</i> (continued)	<p>For the Cisco 3600 series access servers, replace the <i>signal</i> variable with one of the following signal types:</p> <ul style="list-style-type: none"> • r2-analog {r2-compelled [ani] r2-non-compelled [ani] r2-semi-compelled [ani]} • r2-digital {r2-compelled [ani] r2-non-compelled [ani] r2-semi-compelled [ani]} • r2-pulse {r2-compelled [ani] r2-non-compelled [ani] r2-semi-compelled [ani]} <p>The following descriptions are provided for the previous R2 syntax bullets:</p> <p>r2-analog—Specifies R2 ITU Q411 analog line signaling, which reflects the on/off switching of a tone in frequency-division multiplexing circuits (before TDM circuits were created). The tone is used for line signaling.</p> <p>r2-digital—Specifies R2 ITU Q421 digital line signaling, which is the most common signaling configuration. The A and B bits are used for line signaling.</p> <p>r2-pulse—Specifies R2 ITU supplement 7 pulse line signaling, which is a transmitted pulse that indicates a change in the line state.</p> <p>dtmf—Specifies the DTMF tone signaling (Cisco 5800 series access server only).</p> <p>r2-compelled [ani]—Specifies R2 compelled register signaling. You can also specify provisioning the ANI address option.</p> <p>r2-non-compelled [ani]—Specifies R2 noncompelled register signaling.</p> <p>r2-semi-compelled [ani]—Specifies R2 semicomped register signaling.</p>
------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Defaults

No CAS is configured on the controller. All R2 signaling types have DNIS turned on by default.

Command Modes

Controller configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.0(1)T	This command was implemented on the Cisco 3600 series.

Usage Guidelines

Use this command to configure support for incoming and outgoing call signals (such as on-hook and off-hook) on each E1 controller.

If you specify the time slot range 1-31, the system software automatically uses the 16th time slot to transmit the channel associated signaling.

The signaling you configure on the access server must match the signaling used by the central office. For example if the central office switch is forwarding R2 analog signaling to a Cisco AS5800, then the access server's E1 controller must also be configured for R2 analog signaling (**r2-analog**).

All R2 signaling options have DNIS support turned on by default. If you enable the **ani** option, the collection of DNIS information is still performed. Specifying the **ani** option does not disable DNIS. DNIS is the number being called. ANI is the caller's number. For example, if you are configuring router A to call router B, then the DNIS number is router B, the ANI number is router A. ANI is very similar to Caller ID.

To customize the R2 signaling parameters, refer to the **cas-custom** controller configuration command. When you enable the **cas-group** command, the **cas-custom** command is automatically setup to be polled for configuration information. However, unless you enable or turn on specific features with the **cas-custom** command, the cas-custom feature has an empty set of signaling parameters.

**Note**

Only integrated MICA modems support E1 R2 signaling on Cisco access servers.

DNIS is automatically collected for modem pools and R2 tone signaling. You do not need to specify the collection of DNIS information with the **cas-group** command. However, if you are using non-R2 tone signaling, the system must be manually configured to collect DNIS information. For non-R2 cas signaling, DNIS collection is done only for E&M-fgb.

Examples

In most cases, you will configure the same channel-associated signaling on each E1 controller. The following examples configure signaling and customized parameters on controller E1 2 using the **cas-group** and **cas-custom** controller configuration commands.

The following example configures the E1 controller on a Cisco 5800 series access server. To configure a Cisco 3600 series access server, replace the command:

```
controller e1 2/1/0
```

with the command:

```
controller e1 2
```

**Note**

The actual channel associated signaling is configured on the 16th time slot, which is the reason why this time slot does not come up in the following output.

```
Router(config-controller)# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config-controller)# controller e1 2/1/0
```

```
Router(config-controller)# cas-group 1 timeslots 1-31 type r2-digital r2-compelled ani
```

```
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 1 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 2 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 3 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 4 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 5 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 6 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 7 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 8 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 9 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 10 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 11 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 12 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 13 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 14 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 15 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 17 is up
```

```

%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 18 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 19 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 20 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 21 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 22 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 23 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 24 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 25 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 26 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 27 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 28 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 29 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 30 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 31 is up

```

The following example shows all the supported E1 signaling types on a Cisco AS5800:

```
Router(config-controller)# cas-group 1 timeslots 1-31 type ?
```

```

e&m-fgb          E & M Type II FGB
e&m-fgd          E & M Type II FGD
e&m-immediate-start E & M Immediate Start
fxs-ground-start FXS Ground Start
fxs-loop-start   FXS Loop Start
p7              P7 Switch
r2-analog        R2 ITU Q411
r2-digital       R2 ITU Q421
r2-pulse         R2 ITU Supplement 7
sas-ground-start SAS Ground Start
sas-loop-start   SAS Loop Start

```

```
Router(config-controller)# cas-group 1 timeslots 1-31 type r2-analog ?
```

```

dtmf             DTMF tone signaling
r2-compelled     R2 Compelled Register signaling
r2-non-compelled R2 Non Compelled Register signaling
r2-semi-compelled R2 Semi Compelled Register signaling
<cr>

```

R2 signaling parameters can be customized with the **cas-custom** controller configuration command:

```
Router(config-controller)# cas-custom 1?
```

CAS custom commands:

```

caller-digits  Digits to be collected before requesting CallerID
category       Category signal
country        Country Name
default        Set a command to its defaults
exit           Exit from cas custom mode
invert-abcd    invert the ABCD bits before tx and after rx
metering       R2 network is sending metering signal
nc-congestion  Non Compelled Congestion signal
no             Negate a command or set its defaults

```

cas-group (T1 controller)

To configure channelized T1 time slots with robbed-bit signaling, and R1 channel-associated signaling, use the **cas-group** command in controller configuration mode. To disable signaling for one or more time slots, use the **no** form of this command.

Cisco AS5200, Cisco AS5300, and Cisco AS5800 Series Access Servers

cas-group *channel* **timeslots** *range* **type** *signal*

no cas-group *channel* **timeslots** *range* **type** *signal*

R1 Channel-Associated Signaling

cas-group *channel* **timeslots** *range* **type** **r1-modified** {**ani-dnis** | **dnis**}

no cas-group *channel* **timeslots** *range* **type** **r1-modified** {**ani-dnis** | **dnis**}

Syntax Description

channel	Single channel group number from 0 to 30.
timeslots <i>range</i>	Time slot or time slot range, which can be from 1 to 24 for T1, and from 1 to 31 for E1. You can specify a time slot range (for example, 1-31), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-7, 8, 17-31). The 16th time slot is reserved for out-of-band signaling.
type <i>signal</i>	Type of robbed-bit signaling. Replace the <i>signal</i> variable with one of the following signal types. The keywords service , data , and voice are used for switched 56K configuration. These keywords are described at the end of this syntax description table. <ul style="list-style-type: none"> e&m-rgb [dtmf [dnis] [service {data voice}] [service {data voice}] [mf [dnis] [service {data voice}]—Specifies ear and mouth channel signaling with feature group B support, which includes the wink-start protocol. Use the options dtmf [dnis] to configure DTMF tone signaling with optional DNIS provisioning. Use the options mf [dnis] to configure MF tone signaling with optional DNIS provisioning. Use the options service {data voice} for switched 56K configurations. (See the end of this syntax description table for more information about these switched 56K keywords.) e&m-rgd [service {data voice}]—Specifies ear and mouth channel signaling with feature group D support, which includes the wink-start protocol. Use the options service {data voice} for switched 56K configurations. (See the end of this syntax description table for more information.) e&m-immediate-start [service {data voice}]—Specifies ear and mouth channel signaling with immediate-start support. Use the options service {data voice} for switched 56K configurations. (See the end of this syntax description table for more information.) fxs-ground-start [service {data voice}]—Specifies Foreign Exchange Station ground-start signaling support. Use the options [service {data voice} for switched 56K configurations. (See the end of this syntax description table for more information.)

type <i>signal</i> (continued)	<ul style="list-style-type: none"> • fxs-loop-start [service {data voice}]—Specifies Foreign Exchange Station loop-start signaling support. Use the options service {data voice} for switched 56K configurations. (See the end of this syntax description table for more information.) • r1-modified ani-dnis—Indicates R1 signaling will collect ani and dnis information. • r1-modified dnis—Indicates R1 signaling will collect only dnis information. • sas-ground-start [service {data voice}]—Specifies Special Access Station ground-start signaling support. Use the options service {data voice} for switched 56K configurations. (See the end of this syntax description table for more information.) • sas-loop-start [service {data voice}]—Specifies Special Access Station loop-start signaling support. Use the options service {data voice} for switched 56K configurations. • service—(Optional) Specifies the type of services provided for scenarios involving switched 56K connections. Do not include this option in the cas-group command statement if you are not using the access server to provide switched 56K connections. • data—Enables switched 56K digital data services on the specified range of time slots. The data is directly read from the time slot or channel. Time slots configured with this option will not accept analog modem calls. • voice—Enables analog modem services on the specified range of time slots. The call is forwarded to the modems for demodulation. Time slots configured with this option will not accept switched 56K digital calls.
------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Defaults

For ISDN PRI, the **cas-group** command is disabled.

If the channelized T1 is not configured as a PRI, the default value for line signaling is **e&m-fgb** and the default value for tone signaling is **DTMF**.

The R1 signaling default value is **ani-dnis**.

Command Modes

Controller configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3 T	The following signaling keywords were added: <ul style="list-style-type: none"> • service • data • voice The R1 keyword was added.

Usage Guidelines

Use the **cas-group** command to configure T1 controllers with different types of robbed-bit signaling, such as on-hook and off-hook for E&M feature group B (**e&m-fgb**).

If you want to collect DNIS information on a T1 controller, you must manually configure it on the access server. DNIS collection is performed only for E&M-fgb. To collect DTMF DNIS for E&M-fgb under a controller T1 configuration, enter the **cas-group 0 timeslots 1-24 type e&m-fgb dtmf dnis** command. To collect MF DNIS for E&M-fgb, enter the **cas-group 0 timeslots 1-24 type e&m-fgb mf dnis** command.

Examples

The following example configures all 24 channels with ear and mouth robbed-bit signaling with feature group B support:

```
Router(config-controller)# controller T1 0
Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb

%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 1 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 2 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 3 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 4 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 5 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 6 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 7 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 8 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 9 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 10 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 11 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 12 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 13 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 14 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 15 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 16 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 17 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 18 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 19 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 20 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 21 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 22 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 23 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 24 is up
```

The following example configures the required signaling to support modem pooling and the digital number identification service (DNIS) over channelized T1 lines on a Cisco AS5300. The only supported signaling and tone types for modem pooling over CT1 RBS are E&M feature group B, DTMF tones, and MF tones. By configuring DNIS as part of the **cas-group** command, the system can collect DNIS digits for incoming calls, which can be redirected to specific modem pools setup for different customers or services. Additionally, you must be running MICA modems in the system and have at least 10% of your total modems in the default modem pool. Free modems are needed in the default pool to detect the incoming called number or DNIS before handing the call off to the appropriate modem pool. Therefore, two modems are actually needed to handle each incoming call.

**Note**

Make sure that your switch provides inband address information for incoming analog calls before you enable this feature.

```
controller t1 0
cas-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
exit
```

```
modem-pool accounts1
pool-range 30-50
called-number 2000 max-conn 21
exit
```

The following example configures a Cisco AS5200 to accept switched 56K digital calls on both of its T1 controllers:

```
copy running-config startup-config
```

The following example configures switched 56K digital services and analog modem services on one controller. Each service is assigned its own range of timeslots. Switched 56K calls are assigned to timeslots 1 through 15. Analog modem calls are assigned to timeslots 16 through 24. However, you must use different channel group numbers in each **cas-group** command entry.

```
controller T1 0
cas-group 0 timeslots 1-15 type e&m-fgb service data
cas-group 1 timeslots 16-24 type e&m-fgb service voice
framing esf
clock source line secondary
linecode b8zs
exit
```

The following example configures R1 signaling on a Cisco AS5200 (T1 interface) and specifies the collection of both ANI and DNIS information:

```
cas-group 1 timeslots 1-24 type r1-modified ani-dnis
```

The following example configures R1 modified signaling on a Cisco AS5800 (T1 interface) and specifies the collection of both ANI and DNIS information:

```
Router(config-controller)# cas-group 1 timeslots 1-24 type r1-modified ani-dnis
Router(config-controller)# ^Z
Router(config-controller)# debug csm
```

Call Switching Module debugging is on

```
1d16h:%CONTROLLER-5-UPDOWN:Controller E1 1/1/0, changed state to up
*Dec 17 11:27:47.946:allocate slot 4 and port 2 is allocated

*Dec 17 11:27:47.946:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IDLE: ev_DSX0_CALL.
*Dec 17 11:27:47.961:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IC1_RING: ev_MODEM_OFFHOOK.
*Dec 17 11:27:49.413:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IC2_COLLECT_ADDR_INFO:
ev_IC_DNIS_INFO_COLLECTED.
*Dec 17 11:27:50.265:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IC2_COLLECT_ADDR_INFO:
ev_IC_ADDR_INFO_COLLECTED.
*Dec 17 11:27:50.265:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IC4_WAIT_FOR_CARRIER:
ev_DSX0_CONNECTED.
```

```
Router(config-controller)# show modem csm 1/4/2
```

```
VDEV_INFO:slot 4, port 2
vdev_status(0x00000001):VDEV_STATUS_ACTIVE_CALL.
csm_state(0x00000205)=CSM_IC5_CONNECTED, csm_event_proc=0x60665CB0, current call thru
Channelize line
invalid_event_count=0, wdt_timeout_count=0
watchdog timer is not activated
wait_for_dialing:False, wait_for_bchan:
pri_chnl=(E1 1/1/0:0), vdev_chnl=(s4, c2)
start_chan_p=0, chan_p=61994BC4, time_slot=0
The calling party phone number =
The called party phone number = 6789
ring_no_answer=0, ic_failure=0, ic_complete=1
dial_failure=0, oc_failure=0, oc_complete=0
```

```
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, busyout=0, modem_reset=0
call_duration_started=1d16h, call_duration_ended=00:00:00, total_call_duration=00:00:00
```

```
Router(config-controller)# debug mica msm
```

```
MICA modems state machine debugging is on
```

```
DA-Slot4#
```

```
1d16h:Msm2:MSM_IN_SERVICE:n_ring_ind:cc0x200 si5 dc3 ms0 cr56000,75
1d16h:Msm2:MSM_PREPARE:m_state_trans:newst MODEM_STATE_SETUP
1d16h:Msm2:MSM_SETUP:m_dig_det:di=0x23 (#)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x41 (A)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x36 (6)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x37 (7)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x38 (8)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x39 (9)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x42 (B)
1d16h:Msm2:MSM_COLLECTING_ANI_PREFIX:m_dig_det:di=0x23 (#)
1d16h:Msm2:MSM_COLLECTING_ANI:m_dig_det:di=0x41 (A)
1d16h:Msm2:MSM_COLLECTING_ANI:m_dig_det:di=0x42 (B)
1d16h:Msm2:MSM_COLLECTING_ANI_SUFFIX:t_timeout:
1d16h:Msm2:MSM_CALL_VERIFICATION:n_call_acc:
1d16h:Msm2:MSM_TRAINING_NEGNG:m_state_trans:newst MODEM_STATE_CONNECT
1d16h:Msm2:MSM_TRAINING_NEGNG:m_state_trans:newst MODEM_STATE_LINK
1d16h:Msm2:MSM_TRAINING_NEGNG:m_state_trans:newst MODEM_STATE_TRAINUP
1d16h:Msm2:MSM_TRAINING_NEGNG:m_state_trans:newst MODEM_STATE_EC_NEGOTIATING
1d16h:Msm2:MSM_TRAINING_NEGNG:m_state_trans:newst MODEM_STATE_STEADY_STATE
```