

show tgrm

To display information for debugging purposes about defined trunk groups and interfaces that have been assigned to the trunk groups, use the **show tgrm** command in EXEC mode.

show tgrm

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (>)

Command History

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

Examples

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

```
Router# show tgrm

      Trunk   Any in  Vce in   Data in
      Group # Any out Vce out   Data out

      2       65535   65535   65535
              65535   65535   65535
              0 Retries
              Interface Se1/0/1:15   Data = 0, Voice = 0, Free = 30
              Interface Se1/0/8:15   Data = 2, Voice = 0, Free = 28

              Total calls for trunk group:Data = 2, Voice = 0, Free = 58
              Selected Voice Interface :Se1/0/1:15
              Selected Data Interface  :Se1/0/1:15
```

[Table 131](#) describes the significant fields shown in the display.

Table 131 *show tgrm* Field Descriptions

Field	Description
Trunk Group #	Number of a defined trunk group.
Any in, Vce In, Data In, Any out, Vce out, Data out	Trunk group settings that specify whether incoming and outgoing voice and data traffic is allowed. The nonconfigured number 65535 indicates that max-calls values have not been configured in the global trunk group command.
Retries	Defined maximum number of retries.
Interface	Specified interface, number of channels currently used for voice and data, and number of free channels.

Table 131 *show tgrm Field Descriptions (continued)*

Field	Description
Total calls for trunk group	Number of calls to and from the trunk group, number of channels used for voice and data, and number of free channels.
Selected Voice Interface	Interface or trunk to be used next for a voice call.
Selected Data Interface	Interface or trunk to be used next for a data call.

show trunk group

To display information for one or more trunk groups, use the **show trunk group** command in user EXEC or privileged EXEC mode.

show trunk group [*name* [*cic*] [*sort* [*ascending* | *descending*]]]

Syntax Description	
<i>name</i>	(Optional) Trunk group to display.
<i>cic</i>	(Optional) Displays the Circuit Identification Code (CIC) number.
<i>sort</i>	(Optional) Sorts the output by trunk group number, in ascending or descending order.
<i>ascending</i>	(Optional) Specifies ascending display order for the trunk groups. This is the default.
<i>descending</i>	(Optional) Specifies descending display order for the trunk groups.

Command Default Trunk groups display in ascending order.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	12.2(11)T	This command was introduced.
	12.3(11)T	This command was modified. This command was enhanced to support dial-out trunk groups.
	12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
	12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
	15.0(1)XA	This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for incoming and outgoing calls.
	12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The cic keyword was added.
	15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Examples The following sample output shows that for trunk group 1, preemption is enabled, with a preemption tone timer of 10 seconds, and the preemption level is flash.

```
Router# show trunk group 1

Trunk group: 1
  Description:
  trunk group label: 1

  Translation profile (Incoming):
  Translation profile (Outgoing):
```

show trunk group

```

LPCOR (Incoming): local_group
LPCOR (Outgoing): local_group

Preemption is enabled
Preemption Tone Timer is 10 seconds
Preemption Guard Timer is 60 milliseconds

Hunt Scheme is least-used
Max Calls (Incoming):  NOT-SET (Any)  NOT-SET (Voice) NOT-SET
(Data)
Max Calls (Outgoing):  NOT-SET (Any)  NOT-SET (Voice) NOT-SET
(Data)
Retries: 0

Trunk Se0/3/0:15      Preference DEFAULT
  Member Timeslots : 1-5
  Total channels available : 5
  Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 5
Trunk Se0/3/1:15      Preference DEFAULT
  Member Timeslots : 1-2
  Total channels available : 0
  Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
Trunk Se1/0/0:15      Preference DEFAULT
  Member Timeslots : 1-31
  Total channels available : 0
  Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
Trunk Se1/0/1:15      Preference DEFAULT
  Member Timeslots : 1-10
  Total channels available : 0
  Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0

Total calls for trunk group: Data = 0, Voice = 0, Modem = 0
                             Pend = 0, Free = 5

Preemption Call Type:  Active  Pending
Flash-Override        NA      0
Flash                 0      0
Immediate             0      0
Priority              0      0
Routine              0      0

Total                0      0

Active preemption call-type shows the number of calls
of each priority level which can be preempted by
higher preemption level calls.

Pending preemption call-type shows the number of calls
of each priority level which are pending for the completion
of call preemption.

advertise_flag 0x00000040, capacity timer 25 sec tripl_config_mask 0x00000000
AC_curr 5, FD_curr 0, SD_curr 0

succ_curr 0 tot_curr 1
succ_report 0 tot_report 1
changed 1 replacement position 0

```

Table 132 describes the significant fields shown in the output. Fields are listed in alphabetical order.

Table 132 *show trunk group Field Descriptions*

Field	Description
Description	Description of the trunk group if entered with the description (trunk group) command.
trunk group label	Name of the trunk group.
Translation profile (Incoming)	List of incoming translation profiles.
Translation profile (Outgoing)	List of outgoing translation profiles.
LPCOR (Incoming)	Setting of the lpcor incoming command.
LPCOR (Outgoing)	Setting of the lpcor outgoing command.
Preemption is	Indicates whether preemption is enabled or disabled.
Preemption level	The preemption level for voice calls to be preempted by a DDR call.
Preemption tone timer	The expiry time for the preemption tone for the outgoing calls being preempted by a DDR call.
Hunt Scheme	Name of the idle channel hunt scheme used for this trunk group.
Max calls (incoming)	Maximum number of incoming calls handled by this trunk group.
Max calls (outgoing)	Maximum number of outgoing calls handled by this trunk group.
Retries	Number of times the gateway tries to complete the call on the same trunk group.
Total calls for trunk group	List of the total calls across all trunks in the trunk group.
Preemption Call Type	List of preemption levels for active and pending calls.
Data	Number of currently used data channels on the trunk or total data calls used by the trunk group.
Free	Number of currently available channels on the trunk or total available calls for the trunk group.
Member timeslots	Member timeslots for this trunk.
Pending	Number of pending channels.
Preference	Preference of the trunk in the trunk group. If DEFAULT appears, the trunk does not have a defined preference.
Total channels available	Number of available channels for the trunk.
Trunk group	ID of the trunk group member.
Voice	Number of currently used voice channels on the trunk or total voice calls used by the trunk group.

Related Commands

Command	Description
description (trunk group)	Includes a specific description of the trunk group interface.
hunt-scheme least-idle	Specifies the method for selecting an available incoming or outgoing channel.
trunk group	Initiates a trunk group definition.
trunk group timeslots	Directs an outbound synchronous or asynchronous call initiated by DDR to use specific DS0 channels of an ISDN circuit.

show vtemplate

To display information about all configured virtual templates, use the **show vtemplate** command in privileged EXEC mode.

show vtemplate

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The show display was modified to display the interface type of the virtual template and to provide counters on a per-interface-type basis for IPsec virtual tunnel interfaces.
12.2(33)SRA	This comand was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This comand was integrated into Cisco IOS Release 12.2(33)SXH.

Examples The following is sample output from the **show vtemplate** command:

```
Router# show vtemplate
```

```
Virtual access subinterface creation is globally enabled
```

	Active Interface	Active Subinterface	Subint Capable	Pre-clone Available	Pre-clone Limit	Interface Type
Vt1	0	0	Yes	--	--	Serial
Vt2	0	0	Yes	--	--	Serial
Vt4	0	0	Yes	--	--	Serial
Vt21	0	0	No	--	--	Tunnel
Vt22	0	0	Yes	--	--	Ether
Vt23	0	0	Yes	--	--	Serial
Vt24	0	0	Yes	--	--	Serial

```
Usage Summary
```

		Interface	Subinterface
Current	Serial in use	1	0
Current	Serial free	0	3
Current	Ether in use	0	0
Current	Ether free	0	0
Current	Tunnel in use	0	0
Current	Tunnel free	0	0
Total		1	3
Cumulative	created	8	4
Cumulative	freed	0	4

```

Base virtual access interfaces: 1
Total create or clone requests: 0
Current request queue size: 0
Current free pending: 0

Maximum request duration: 0 msec
Average request duration: 0 msec
Last request duration: 0 msec

Maximum processing duration: 0 msec
Average processing duration: 0 msec
Last processing duration: 0 msec
Last processing duration:0 msec

```

Table 133 describes the significant fields shown in the example.

Table 133 *show vtemplate Field Descriptions*

Field	Description
Virtual access subinterface creation is globally...	The configured setting of the virtual-template command. Virtual access subinterface creation may be enabled or disabled.
Active Interface	The number of virtual access interfaces that are cloned from the specified virtual template.
Active Subinterface	The number of virtual access subinterfaces that are cloned from the specified virtual template.
Subint Capable	Specifies if the configuration of the virtual template is supported on the virtual access subinterface.
Pre-clone Available	The number of precloned virtual access interfaces currently available for use for the particular virtual template.
Pre-clone Limit	The number of precloned virtual access interfaces available for that particular virtual template.
Current in use	The number of virtual access interfaces and subinterfaces that are currently in use.
Current free	The number of virtual access interfaces and subinterfaces that are no longer in use.
Total	The total number of virtual access interfaces and subinterfaces that exist.
Cumulative created	The number of requests for a virtual access interface or subinterface that have been satisfied.
Cumulative freed	The number of times that the application using the virtual access interface or subinterface has been freed.
Base virtual-access interfaces	This field specifies the number of base virtual access interfaces. The base virtual access interface is used to create virtual access subinterfaces. There is one base virtual access interface per application that supports subinterfaces. A base virtual access interface can be identified from the output of the show interfaces virtual-access command.
Total create or clone requests	The number of requests that have been made through the asynchronous request API of the virtual template manager.

Table 133 *show vtemplate Field Descriptions (continued)*

Field	Description
Current request queue size	The number of items in the virtual template manager work queue.
Current free pending	The number of virtual access interfaces whose final freeing is pending. These virtual access interfaces cannot currently be freed because they are still in use.
Maximum request duration	The maximum time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Average request duration	The average time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Last request duration	The time that it took from the time that the asynchronous request was made until the application was notified that the request was done for the most recent request.
Maximum processing duration	The maximum time that the virtual template manager spent satisfying the request.
Average processing duration	The average time that the virtual template manager spent satisfying the request.
Last processing duration	The time that the virtual template manager spent satisfying the request for the most recent request.

Related Commands

Command	Description
clear counters	Clears interface counters.
show interfaces virtual-access	Displays status, traffic data, and configuration information about a specified virtual access interface.
virtual-template	Specifies which virtual template will be used to clone virtual access interfaces.

shutdown (port)

To disable a port, use the **shutdown** command in port configuration mode. To change the administrative state of a port from out-of-service to in-service, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Command Default Port is enabled.

Command Modes Port configuration (config-port)

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 and support was added for the Cisco AS5350.

Usage Guidelines The **shutdown** command disables a port.



Note

The **shutdown** command is similar to the **modem shutdown** MICA technologies modem command.

Examples The following example disables ports 1 to 18 and then reenables them:

```
Router(config)# port 1/1 1/18
Router(config-port)# shutdown
Router(config-port)# no shutdown
```

Related Commands	Command	Description
	busyout (port)	Disables a port by causing the system to wait for the active services on the port to terminate.
	clear port	Resets the NextPort port and clears any active call.
	clear spe	Reboots all specified SPEs.

Command	Description
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

shutdown (spe)

To take a service processing element (SPE) out of service, use the **shutdown** command in SPE configuration mode. To change the administrative state of this SPE from down to up, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Command Default SPE is in service.

Command Modes SPE configuration (config-spe)

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 and support was added for the Cisco AS5350.

Examples

The following example disables SPE ports 1 to 18 and then reenables them:

```
Router(config)# spe 1/1 1/18
Router(config-spe)# shutdown
Router(config-spe)# no shutdown
```

Related Commands

Command	Description
busyout (port)	Disables a port by causing the system to wait for the active services on the port to terminate.
clear spe	Reboots all specified SPEs.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

signaling-class cas

To define a signaling class with a template formed by directives guiding the Call Service Module (CSM) to process the digit sequence, use the **signaling-class cas** command in global configuration mode. To remove the signaling class assignment, use the **no** form of this command.

signaling-class cas *name*

no signaling-class cas *name*

Syntax Description

<i>name</i>	The signaling class name, which specifies the template that processes the ANI/DNIS delimiter.
-------------	---

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

The signaling class is referred by the *name* argument.

Examples

The following example enables the **signaling-class cas** command:

```
signaling-class cas test
profile incoming S*a<*d<*n
controller T1 1/0/1
cas-custom 1
class test
```

Related Commands

Command	Description
class (controller)	Activates the signaling-class cas command.
profile incoming	Defines a template formed by directives guiding the CSM to process the digit sequence for a signaling class.

snapshot client

To configure a client router for snapshot routing, use the **snapshot client** command in interface configuration mode. To disable a client router, use the **no** form of this command.

snapshot client *active-time* *quiet-time* [**suppress-statechange-updates**] [**dialer**]

no snapshot client *active-time* *quiet-time* [**suppress-statechange-updates**] [**dialer**]

Syntax Description		
<i>active-time</i>		Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer ranging from 5 to 100. There is no default value. A typical value is 5 minutes.
<i>quiet-time</i>		Amount of time, in minutes, that routing entries are frozen and remain unchanged between active periods. Routes are not aged during the quiet period, so they remain in the routing table as if they were static entries. This argument can be an integer ranging from 8 to 100000. There is no default value. The minimum quiet time is generally the active time plus 3.
suppress-statechange-updates		(Optional) Disables the exchange of routing updates each time the line protocol goes from “down” to “up” or from “dialer spoofing” to “fully up.”
dialer		(Optional) Specifies that the client router dials up the remote router in the absence of regular traffic.

Command Default Snapshot routing is disabled.
The *active-time* and *quiet-time* arguments have no default values.

Command Modes Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines The value of the *active-time* argument must be the same for the client and server routers.
To specify that the remote server routers be called by this client router during each active period, use the **dialer map snapshot** command.

Examples The following example configures a client router for snapshot routing:

```
interface dialer 1
  snapshot client 5 600 suppress-statechange-updates dialer
```

Related Commands

Command	Description
clear resource-pool	Ends the quiet period on a client router within 2 minutes.
dialer map snapshot	Defines a dialer map for the Cisco snapshot routing protocol on a client router connected to a DDR interface.
show snapshot	Displays snapshot routing parameters associated with an interface.
snapshot client	Configures a client router for snapshot routing.
snapshot server	Configures a server router for snapshot routing.

snapshot server

To configure a server router for snapshot routing, use the **snapshot server** command in interface configuration mode. To disable a server router, use the **no** form of this command.

snapshot server *active-time* [**dialer**]

no snapshot server *active-time* [**dialer**]

Syntax Description		
	<i>active-time</i>	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer ranging from 5 to 100. There is no default value. A typical value is 5 minutes.
	dialer	(Optional) Specifies that the client router dials up the remote router in the absence of regular traffic.

Command Default Snapshot routing is disabled.
The *active-time* argument has no default value.

Command Modes Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines The value of the *active-time* argument must be the same for the client and server routers.

Examples The following example configures a server router for snapshot routing:

```
interface dialer 1
 snapshot server 5
```

Related Commands	Command	Description
	show snapshot	Displays snapshot routing parameters associated with an interface.
	snapshot client	Configures a client router for snapshot routing.

source template

To attach a configured customer profile template to a particular customer profile, use the **source template** command in customer profile configuration mode.

source template *name*

Syntax Description	<i>name</i> Customer profile template name.
---------------------------	---

Command Default No templates are sourced or attached to a customer profile.

Command Modes Customer profile configuration

Command History	Release	Modification
	12.0(6)T	This command was introduced.

Usage Guidelines All PPP and peer-default commands are allowed for a particular customer profile template under this grouping.

Examples The following example shows the creation and configuration of a customer profile template named cisco1-direct and its subsequent assignment to the customer profile cisco1:

```
template cisco1-direct
 multilink {max-fragments num | max-links num | min-links num}
 peer match aaa-pools
 peer default ip address pool cisco1-numbers
 ppp ipcp dns 10.1.1.1 10.2.2.2
 ppp multilink
 exit
 resource-pool profile customer cisco1
 source template cisco1-direct
```

Related Commands	Command	Description
	template	Accesses the template configuration mode for configuring a particular customer profile template.

spe

To enter service processing element (SPE) configuration mode and set the range of SPEs, use the **spe** command in global configuration mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

```
spe {slot | slot/spe} [slot | slot/spe]
```

Cisco AS5800 with the Universal Port Card (UPC)

```
spe {shelf/slot | shelf/slot/spe} [shelf/slot | shelf/slot/spe]
```

Syntax Description	slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. A range of slots can be specified by entering a second value for the <i>slot</i> argument.
	<i>slot/spe</i>	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark. A range of ports can be specified by entering a second value for the <i>slot/spe</i> argument.
	<i>shelf/slot</i>	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark. A range of slots can be specified by entering a second value for the <i>shelf/slot</i> argument.
	<i>shelf/slot/spe</i>	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks. A range of ports can be specified by entering a second value for the <i>shelf/slot/spe</i> argument.

Command Default No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XI1	This command was introduced.
	12.0(5)T	This command was implemented on the Cisco AS5200 and Cisco AS5300 platforms.
	12.1(1)XD	This command was implemented 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 and support was added for the Cisco AS5350.

Usage Guidelines

The **spe** global configuration command enables the SPE configuration mode. Configure your SPE by specifying a slot and an SPE associated with the slot; or, you can configure a range of SPEs by specifying the first and last SPE in the range.

To exit SPE configuration mode, use the **exit** command.

Examples

The following example shows the **spe** command being used from global configuration mode to access the SPE configuration mode for the SPE range from 1/2 to 1/4:

```
Router(config)# spe 5/4 5/6
Router(config-spe)# ?
SPE Configuration Commands:
  busyout   Busyout SPE
  default   Set a command to its defaults
  exit      Exit from SPE Configuration Mode
  firmware  Firmware used for the SPE
  help      Description of the interactive help system
  no        Negate a command or set its defaults
  shutdown  Take the SPE out of Service
```

When the universal gateway is booted, the **spe** global configuration command specifies the location from where the firmware image is downloaded to the SPE. If the **spe** configuration command is used to download the firmware from Flash memory and then subsequently the **no** version of the exact command is entered, then the **spe** command downloads the embedded firmware.

**Note**

Use this command when traffic is low because the **spe** download does not begin until the modems have no active calls.

**Caution**

The **spe** command is a configuration command. Save it using the **write memory** command; otherwise, the configuration is not saved. If the configuration is not saved, the downloading of the specified firmware does not occur after the next reboot.

The following example shows the **spe** command being used from global configuration mode to access the SPE configuration mode for the range of SPEs from 1/2 to 1/4 on the Cisco AS5400:

```
Router(config)# spe 1/2 1/4
```

The following example specifies the range for use of the **shutdown** command:

```
Router(config)# spe 1/1 1/18
Router(config-spe)# shutdown
Router(config-spe)# no shutdown
```

Related Commands

Command	Description
exit	Exits SPE configuration mode.
show spe	Displays SPE status.

spe call-record modem

To generate a modem call record at the end of each call, use the **spe call-record modem** command in global configuration mode. To cancel the request to generate the reports, use the **no** form of the command.

```
spe call-record modem {max-userid number | quiet}
```

```
no spe call-record modem {max-userid number | quiet}
```

Syntax Description

max-userid <i>number</i>	Maximum length of the user ID for the modem call record report in number of bytes. The range is from 0 to 100.
quiet	Disables logging to console and terminal, but not to syslog.

Command Default

An SPE call record is enabled.

Command Modes

Global 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 and support was added for the Cisco AS5350.

Usage Guidelines

The **spe modem-call-record** command generates a modem call record at the end of each call.



Note

The **spe call-record modem** command is similar to the **modem call-record** command.

Examples

The following example displays an SPE call record:

```
Router# configure terminal
Router(config)# spe call-record modem max-userid 50
Router(config)# end
Router#
00:18:30: %SYS-5-CONFIG_I: Configured from console by console
Router# write memory
Building configuration...
[OK]
```

The following is a partial example of traces generated when a call terminates. The logs from the **show port modem log** command do not change as a result of using the **spe call-record modem** command.

```
.
.
.
%LINK-3-UPDOWN: Interface Async5/105, changed state to down
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/2/15,
shelf/slot/port=5/37, call_id=EE, userid=touraco-e1-4, ip=79.188.24.1,
calling=(n/a), called=35160, std=V.34+, prot=LAP-M, comp=V.42bis,
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=286/266, bad=0, rx/tx
ec=16/6, bad=0, time=96, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/1/24,
shelf/slot/port=5/38, call_id=FD, userid=touraco-e1-4, ip=79.205.24.1,
calling=(n/a), called=35170, std=V.34+, prot=LAP-M, comp=V.42bis,
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=289/267, bad=0, rx/tx
ec=17/7, bad=0, time=93, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/3/15,
shelf/slot/port=5/2, call_id=FF, userid=touraco-e1-4, ip=79.200.24.1,
calling=(n/a), called=35170, std=V.34+, prot=LAP-M, comp=V.42bis,
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=287/270, bad=0, rx/tx
ec=17/7, bad=0, time=92, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/3/10,
shelf/slot/port=5
.
.
.
```

Related Commands

Command	Description
modem call-record	Activates the logging of a summary of modem events upon the termination of a call.

spe country

To specify the country while setting the modem card parameters (including country code and encoding), use the **spe country** command in global configuration mode. To set the country code to the default value, use the **no** form of this command.

```
spe country {country-name | e1-default | t1-default}
```

```
no spe country {country-name | e1-default | t1-default}
```

Syntax Description

country-name	Name of the country, See Table 134 for a list of supported country name keywords.
e1-default	Use this command when using the E1 interface.
t1-default	Use this command when using the T1 interface.

Command Default

Disabled

Command Modes

Global 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 and support was added for the Cisco AS5350.

Usage Guidelines

On the Cisco universal gateway, DS0 companding law selection is configured for the entire system rather than on individual voice ports. Set the **spe country** command to the appropriate country.

If T1 lines are configured, the default is **t1-default**; if E1 lines are configured, the default is **e1-default**.

The Cisco universal gateway must be in an Idle state (no calls are active) for the **spe country** command to function. All sessions on all modules in all slots must be in the Idle state.



Note

The **spe country** command is similar to the **modem country mica** and **modem country microcom_hdms** commands.

Table 134 lists the country names and corresponding companding law.

Table 134 Country Names and Corresponding Companding Law

Keyword	Country	Companding Law
australia	Australia	a-law
austria	Austria	a-law
belgium	Belgium	a-law
china	China	a-law
cyprus	Cyprus	a-law
czech-republic	Czech/Slovak Republic	a-law
denmark	Denmark	a-law
e1-default	Default for E1	a-law
finland	Finland	a-law
france	France	a-law
germany	Germany	a-law
hong-kong	Hong Kong	u-law
india	India	a-law
ireland	Ireland	a-law
israel	Israel	a-law
italy	Italy	a-law
japan	Japan	u-law
malaysia	Malaysia	a-law
netherlands	Netherlands	a-law
new-zealand	New Zealand	a-law
norway	Norway	a-law
poland	Poland	a-law
portugal	Portugal	a-law
russia	Russia	a-law
singapore	Singapore	a-law
south-africa	South Africa	a-law
spain	Spain	a-law
sweden	Sweden	a-law
switzerland	Switzerland	a-law
t1-default	Default for T1	u-law
taiwan	Taiwan	u-law
thailand	Thailand	a-law
turkey	Turkey	a-law
united-kingdom	United Kingdom	a-law
usa	United States of America	u-law

Examples

The following example configures the setting of the country code to the default for E1:

```
Router(config)# spe country e1-default
```

The following example configures the setting of the country code to the default for T1:

```
Router(config)# spe country t1-default
```

Related Commands

Command	Reference
modem country mica	Configures the modem country code for a bank of MICA technologies modems.
modem country microcom_hdms	Configures the modem country code for a bank of Microcom modems.
show spe	Displays SPE status.

spe download maintenance

To perform download maintenance on service processing elements (SPEs) that are marked for recovery, use the **spe download maintenance** command in global configuration mode. To disable download maintenance on SPEs, use the **no** form of the command.

```
spe download maintenance { time hh:mm | stop-time hh:mm | max-spes number-of-spes | window time-period | expired-window { drop-call | reschedule } }
```

```
no spe download maintenance { time hh:mm | stop-time hh:mm | max-spes number-of-spes | window time-period | expired-window { drop-call | reschedule } }
```

Syntax Description

time <i>hh:mm</i>	Time of the day to start the download maintenance activity. Enter the value in the format of the variable as shown in hours and minutes. Default is 03:00 a.m.
stop-time <i>hh:mm</i>	Time of the day to stop the download maintenance activity. Enter the value in the format of the variable as shown in hours and minutes.
max-spes <i>number-of-spes</i>	Maximum number of SPEs that can simultaneously be in maintenance. The value ranges from 1 to 10,000. Default is equal to 20 percent of the maximum number of SPEs in each NextPort Dial Feature Card (DFC).
window <i>time-period</i>	Time window to perform the maintenance activity. The value ranges from 0 to 360 minutes. Default is 60 minutes.
expired-window	Action to take if SPE maintenance is not completed within the specified window. Default is reschedule .
drop-call	Expired window choice that forces download by dropping active calls.
reschedule	Expired window choice that defers recovery to the next maintenance time (default for the expired-window keyword).

Command Default

Enabled

Command Modes

Global 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 and support was added for the Cisco AS5350.

Usage Guidelines

The SPE download maintenance activity takes place when SPEs are marked for recovery. The settings are enabled by default. When you want to change the default settings to a desired setting, use the **spe download maintenance** command parameters to perform SPE download maintenance activity with the specific changes.

Enter the **time** *hh:mm* keyword to set a time to start the SPE download maintenance activity. Then enter the **stop-time** *hh:mm* keyword to set a time to stop the download maintenance. Next enter the **max-spes** *number-of-spes* keyword to set the number of SPEs for the download maintenance. Then enter the **window** *time-period* keyword to set a time period to perform the download maintenance. Finally, enter the **expired-window** keyword to set actions in the event the SPE download maintenance is not completed in the set **window** *time-period*.

The download maintenance activity starts at the set start **time** and steps through all the SPEs that need recovery and the SPEs that need a firmware upgrade and starts maintenance on the maximum number of set SPEs for maintenance. The system waits for the **window** delay time for all the ports on the SPE to become inactive before moving the SPE to the Idle state. Immediately after the SPE moves to the Idle state, the system starts to download firmware. If the ports are still in use by the end of **window** delay time, depending upon the **expired-window** setting, connections on the SPE ports are shut down and the firmware is downloaded by choosing the **drop-call** option, or the firmware download is rescheduled to the next download maintenance time by choosing the **reschedule** option. This process continues until the number of SPEs under maintenance is below the **max-spes** value, or until the **stop-time** value (if set), or until all SPEs marked for recovery or upgrade have had their firmware reloaded.

Examples

The following example displays the SPE download maintenance with the different keyword parameters:

```
Router(config)# spe download maintenance time 03:00

Router(config)# spe download maintenance stop-time 04:00

Router(config)# spe download maintenance max-spes 50

Router(config)# spe download maintenance window 30

Router(config)# spe download maintenance expired-window reschedule
```

Related Commands

Command	Description
firmware location	Downloads firmware into Cisco integrated modems.
firmware upgrade	Specifies the method in which the SPE will be downloaded.
show spe version	Displays the firmware version on an SPE.
spe recovery	Sets an SPE port for recovery.

spe log-size

To set the size of the port event log, use the **spe log-size** command in global configuration mode. To restore the default size, use the **no** version of this command.

spe log-size *number*

no spe log-size

Syntax Description	<i>number</i>	The number of recorded events. Valid values for the <i>number</i> argument range from 0 to 100. The default value is 50 events.
--------------------	---------------	---

Command Default	The port event log records 50 events.
-----------------	---------------------------------------

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

Command History	Release	Modification
	12.1(1)XD	This command was introduced on the Cisco AS5400.
	12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T on the Cisco AS5400 and 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 and support was added for the Cisco AS5350.

Examples The following example sets the size of the event log to 70 events:

```
Router(config)# spe log-size 70
```

Related Commands	Command	Description
	show port digital log	Displays the digital data event log with the oldest event first.
	show port modem log	Displays the modem port history event log or modem test log.

spe recovery

To set a service processing element (SPE) port for recovery, use the **spe recovery** command in global configuration mode. To disable SPE recovery or to restore the default **port-threshold** value, use the **no** form of this command.

```
spe recovery {port-action {disable | recover} | port-threshold number-failures}
```

```
no spe recovery {port-action | port-threshold}
```

Syntax Description

port-action	Action to apply to the port for recovery when the configured port-threshold value has been exceeded.
disable	Sets the port to the bad state.
recover	Sets the port for recovery.
port-threshold <i>number-failures</i>	Number of consecutive failed attempts made on the port before the port-action keyword is applied. The range is from 1 to 10000. The default value is 30.

Command Default

There is no default **port-action** value. SPE recovery is disabled. The default **port-threshold** value is 30 failed attempts.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(2.3)T1	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 and implemented on the Cisco AS5350.

Usage Guidelines

Failure of an SPE port to connect after repeated tries indicates that a problem exists in the SPE or firmware. An SPE port in this state is recovered by downloading firmware.

When an SPE port fails to connect consecutively for a number of times, as specified by the **port-threshold** *number-failures* keyword and argument, the SPE is moved to a state based on the **port-action** configuration.

If the **spe recovery port-action recover** command has been configured, when the **port-threshold** *number-failures* value is exceeded, the port is temporarily marked as disabled (“d” state) to avoid further incoming calls, and it is then marked for recovery (“r” state). Any SPE that has a port marked for recovery will download firmware when the SPE is idle (when none of the ports on the SPE have active calls).

If the **spe recovery port-action disable** command has been configured, when the **port-threshold number-failures** value is exceeded, the port is marked as bad (“BAD” state). An SPE with a port that is marked as bad must be explicitly cleared in order for that port to be used again.

If no **port-action** is configured, the port will be marked as not in use (“_” state). An SPE with a port marked as not in use will remain unusable until it is explicitly cleared, and the SPE will not accept incoming calls on any of the ports.

SPE recovery can be disabled by issuing the **no spe recovery port-action** command. If SPE recovery is disabled, the SPE will behave as if no **port-action** has been configured.

**Note**

Beginning with Cisco IOS Release 12.1(2.3)T1, the modem recovery action for MICA technologies modems on the Cisco AS5800 platforms is done using the **spe recovery** command rather than the **modem recovery** command.

Examples

The following example configures the SPE to recover ports that exceed the call failure threshold:

```
Router(config)# spe recovery port-action recover
```

The following example sets a value of 50 for the number of consecutive failed attempts on the port before the **port-action** keyword is applied:

```
Router(config)# spe recovery port-threshold 50
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
firmware upgrade	Specifies an SPE firmware upgrade method.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe version	Displays the firmware version on an SPE and displays the version to firmware file mappings.
spe download maintenance	Performs download maintenance on SPEs that are marked for recovery.

start-character

To set the flow control start character, use the **start-character** command in line configuration mode. To remove the character, use the **no** form of this command.

start-character *ascii-number*

no start-character

Syntax Description	<i>ascii-number</i>	Decimal representation of the start character.
---------------------------	---------------------	--

Command Default	Decimal 17
------------------------	------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	This command defines the character that signals the start of data transmission when software flow control is in effect. Refer to the “ASCII Character Set and Hex Values” appendix in the <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i> for a list of ASCII characters.
-------------------------	--

Examples	The following example changes the start character to Ctrl-B, which is decimal 2:
-----------------	--

```
line 2
 start-character 2
```

Related Commands	Command	Description
	flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.
	stop-character	Sets the flow control stop character.
	terminal start-character	Changes the flow control start character for the current session.

start-chat

To specify that a chat script start on a specified line at any point, use the **start-chat** command in privileged EXEC mode. To stop the chat script, use the **no** form of this command.

```
start-chat regexp [[aux | console | vty] line-number [dialer-string]]
```

```
no start-chat
```

Syntax Description	
<i>regexp</i>	Name of a regular expression or modem script to be executed. If there is more than one script with a name that matches the argument <i>regexp</i> , the first script found will be used.
<i>line-number</i>	(Optional) Line number on which to execute the chat script. If you do not specify a line number, the current line number is chosen. If the specified line is busy, the script is not executed and an error message appears. If the dialer-string argument is specified, line-number must be entered; it is not optional if you specify a dialer string. This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal (VTY) lines.
<i>dialer-string</i>	(Optional) String of characters (often a telephone number) to be sent to a DCE. If you enter a dialer string, you must also specify <i>line-number</i> , or the chat script <i>regexp</i> will not start.
aux	(Optional) Specifies the auxiliary line.
console	(Optional) Specifies the primary terminal line.
vty	(Optional) Specifies the virtual terminal.

Command Default	
	If you do not specify a line number, the current line number is chosen. If the specified line is busy, the script is not executed and an error message appears. If the dialer-string argument is specified, line-number must be entered; it is not optional if you specify a dialer string. This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal (VTY) lines.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. The aux , console , and vty keywords were added.
	12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
	12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

This command provides modem dialing commands for a chat script that you want to apply immediately to a line. If you do not specify a line, the script runs on the current line. If the specified line is already in use, the script is not activated and an error message appears.

The argument *regex* is used to specify the name of the modem script that is to be executed. The first script that matches the argument in this command and the **dialer map** command will be used. For more information about regular expressions, refer to the “Regular Expressions” appendix in this publication.

This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal lines.

Examples

The following example shows how to force a dialout on line 8 using the script named “telebit”:

```
Router# start-chat telebit 8
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.
script dialer	Specifies a default modem chat script.
script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.

stop-character

To set the flow control stop character, use the **stop-character** command in line configuration mode. To remove the character, use the **no** form of this command.

stop-character *ascii-number*

no stop-character

Syntax Description	<i>ascii-number</i>	Decimal representation of the stop character.
---------------------------	---------------------	---

Command Default	Decimal 19
------------------------	------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	This command defines the character that signals the end of data transmission when software flow control is in effect. Refer to the “ASCII Character Set and Hex Values” appendix in the <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i> for a list of ASCII characters.
-------------------------	--

Examples	The following example changes the stop character to Ctrl-E, which is decimal 5:
-----------------	---

```
line 3
 stop-character 5
```

Related Commands	Command	Description
	flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.
	source template	Sets the flow control start character.
	stop-character	Sets the flow control stop character.

tdm clock priority

To configure the clock source and priority of the clock source used by the time-division multiplexing (TDM) bus on the Cisco AS5350, AS5400, and AS5850 access servers, use the **tdm clock priority** command in global configuration mode. To return the clock source and priority to the default values, use the **no** form of this command.

tdm clock priority *priority-number* { *slot/ds1-port* | *slot/ds3-port:ds1-port* | **external** | **freerun** }

no tdm clock priority *priority-number* { *slot/ds1-port* | *slot/ds3-port:ds1-port* | **external** | **freerun** }

Syntax Description		
<i>priority-number</i>		Priority of the clock source. The priority range is from 1 to 99. A clock set to priority 100 will not drive the TDM bus.
<i>slot/ds1-port</i>		Trunk-card slot is a value from 1 to 7. DS1 port number controller is a value between 0 and 7. Specify with a slash separating the numbers; for example, 1/1.
<i>slot/ds3-port:ds1-port</i>		Trunk-card slot is a value from 1 to 7. DS3 port specifies the T3 port. DS1 port number controller is a value from 1 to 28. Specify with a slash separating the slot and port numbers, and a colon separating the DS1 port number. An example is 1/0:19.
external		Synchronizes the TDM bus with an external clock source that can be used as an additional network reference.
freerun		Selects the free-running clock from the local oscillator when there is no good clocking source from a trunk card or an external clock source.

Command Default If no clocks are configured, the system uses a default, primary clock. An external clock is never selected by default; it must be explicitly configured.

Command Modes Global configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines The TDM bus can receive an input clock from one of three sources on the gateway:

- CT1, CE1, and CT3 trunk cards
- An external T1/E1 clock source feed directly through the Building Integrated Timing Supply (BITS) interface port on the motherboard
- Free-running clock providing clock from an oscillator

**Note**

BITS is a single building master timing supply. BITS generally supplies DS1- and DS0-level timing throughout an office. BITS is the clocks that provide and distribute timing to a wireline network's lower levels.

Trunk-Card Ports

The TDM bus can be synchronized with any trunk cards. On the CT1/CE1 trunk card, each port receives the clock from the T1/E1 line. The CT3 trunk card uses an M13 multiplexer to receive the DS1 clock. Each port on each trunk-card slot has a default clock priority. Also, clock priority is configurable through the **tdm clock priority** command.

External Clock

The TDM bus can be synchronized with an external clock source that can be used as an additional network reference. If no clocks are configured, the system uses a primary clock through a software-controlled default algorithm. If you want the external T1/E1 clock (from the BITS interface) as the primary clock source, you must configure it using the **external** keyword with the **tdm clock priority** command; the external clock is never selected by default.

The BITS interface requires a T1 line composite clock reference set at 1.544 MHz and an E1 line composite clock reference set at 2.048 MHz.

Free-Running Clock

If there is no good clocking source from a trunk card or an external clock source, then select the free-running clock from the internal oscillator using the **freerun** keyword with the **tdm clock priority** command.

Examples

In the following example, BITS clock is set at priority 1:

```
AS5400(config)# tdm clock priority priority 1 external
```

In the following example, a trunk clock from a CT1 trunk card is set at priority 2 and uses slot 4 and DS1 port (controller) 6:

```
AS5400(config)# tdm clock priority priority 2 4/6
```

In the following example, a trunk clock from a CT3 trunk card is set at priority 2 and uses slot 1, DS3 port 0, and DS1 port 19:

```
AS5400(config)# tdm clock priority priority 2 1/0:19
```

In the following example, free-running clock is set at priority 3:

```
AS5400(config)# tdm clock priority priority 3 freerun
```

Related Commands

Command	Description
dial-tdm-clock	Configures the clock source and priority of the clock source used by the TDM bus on the dial shelf of the Cisco AS5800.
show tdm clocks	Displays default system clocks and clock history.

template

To access the template configuration mode for configuring a particular customer profile template, use the **template** command in global configuration mode. To delete the template of the specified name, use the **no** form of this command.

template *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]

no template *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]

Syntax Description

<i>name</i>	Identifies the template.
default	(Optional) Sets the command to its defaults.
exit	(Optional) Exits from resource-manager configuration mode.
multilink	(Optional) Configures multilink parameters.
no	(Optional) Negates the command or its defaults.
peer	(Optional) Accesses peer parameters for point-to-point interfaces.
ppp	(Optional) Accesses Point-to-Point Protocol.

Command Default

No templates are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

All PPP and peer-default commands are enabled for a customer profile template under this grouping.

Examples

The following example shows the creation and configuration of a customer profile template named “cisco1-direct” and its subsequent assignment to the customer profile “cisco1”:

```
template cisco1-direct
  multilink max-fragments 10
  peer match aaa-pools
  peer default ip address pool cisco1-numbers
  ppp ipcp dns 10.1.1.1 10.2.2.2
  ppp multilink
  exit
resource-pool profile customer cisco1
source template cisco1-direct
```

Related Commands

Command	Description
source template	Attaches a configured customer profile template to a customer profile.

test modem back-to-back

To diagnose an integrated modem that may not be functioning properly, use the **test modem back-to-back** command in EXEC mode.

```
test modem back-to-back first-slot/port second-slot/port
```

Syntax Description		
<i>first-slot/port</i>	Slot and modem number of the first test modem. You must include the slash mark	
<i>second-slot/port</i>	Slot and modem number of the second test modem. You must include the slash mark	

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	Use this command to perform back-to-back testing of two modems. You might need to enable this command on several different combinations of modems to determine which one is not functioning properly.
------------------	---

Examples	The following example performs a back-to-back modem test between modem 2/0 and modem 2/1 and removes modem 2/1 (which is associated with TTY line 26) from all dial-in and dial-out services:
----------	---

```
Router# test modem back-to-back 2/0 2/1
```

```
back2back 2/0 2/1
```

```
Repetitions (of 10-byte packets) [1]:
```

```
Router#
```

```
%MODEM-5-B2BCONNECT: Modems (2/0) and (2/1) connected in back-to-back test:
```

```
CONNECT9600/REL-MNPM
```

```
%MODEM-5-B2BMODEMS: Modems (2/0) and (2/1) completed back-to-back test: success/packets = 2/2
```

Related Commands	Command	Description
	modem bad	Removes an integrated modem from service and indicates it as suspected or proven to be inoperable.
	test port modem back-to-back	Tests two specified ports back-to-back and transfers a specified amount of data between the ports.

test port modem back-to-back

To test two specified ports back-to-back and transfer a specified amount of data between the ports, use the **test port modem back-to-back** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

```
test port modem back-to-back slot/port
```

Cisco AS5800 with the Universal Port Card (UPC)

```
test port modem back-to-back shelfslot/port
```

Syntax Description	slot/port	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. Port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark.
	shelfslot/port	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323. You must include the slash marks.

Command Default No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	11.3	The test modem back-to-back form of this command was introduced.
	12.1(1)XD	This command was implemented 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 and support was added for the Cisco AS5350.

Usage Guidelines The **test port modem back-to-back** command should be performed on different combinations to determine a good port.



Note The **test port modem back-to-back** command is similar to the **test modem back-to-back** MICA technologies modem command.

Examples

The following example displays a back-to-back test:

```
Router# test port modem back-to-back 1/1/1
```

```
Repetitions (of 10-byte packets) [1]:
```

```
*Mar 02 12:13:51.743:%PM_MODEM_MAINT-5-B2BCONNECT:Modems (2/10) and (3/20) connected in  
back-to-back test:CONNECT33600/V34/LAP
```

```
*Mar 02 12:13:52.783:%PM_MODEM_MAINT-5-B2BMODEMS:Modems (3/20) and (2/10) completed  
back-to-back test:success/packets = 2/2
```

Related Commands

Command	Description
port modem autotest	Automatically and periodically performs a modem diagnostic test for modems inside the universal gateway or router.
port modem startup test	Performs diagnostic testing for all modems.
show port modem test	Displays the modem port history event log or modem test log.
test modem back-to-back	Diagnoses an integrated modem that may not be functioning properly.

timeout absolute

To specify a timeout period that controls the duration for which a session can be connected before it is terminated, use the **timeout absolute** command in interface configuration mode. To remove the session timeout period, use the **no** form of this command.

timeout absolute *minutes* [*seconds*]

no timeout absolute

Syntax Description		
	<i>minutes</i>	Session lifetime, in minutes. The range is 0 to 71582787.
	<i>seconds</i>	(Optional) Session lifetime, in seconds. The range is 0 to 59.

Command Default No timeout absolute parameter is set.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	11.3	This command was introduced.

Examples The following example shows how to impose a 15-minute (900-second) idle timeout and a 12-hour (720-minute) absolute timeout for session connections:

```
interface Serial0:23
  dialer idle-timeout 900
  timeout absolute 720
!
interface Serial11:23
  dialer idle-timeout 900
  timeout absolute 720
.
.
.
```

Related Commands	Command	Description
	ppp idle timeout	Sets the PPP timeout idle parameter.
	dialer idle-timeout	Specifies the idle time before the line is disconnected.

timer

To set the Redundant Link Manager (RLM) timer, use the **timer** command in RLM configuration mode. The associated options can overwrite the default setting of timeout values. To disable this function, use the **no** form of this command.

```
timer { force-down | keepalive | minimum-up | open-wait | recovery | retransmit | switch-link }
seconds
```

```
no timer { force-down | keepalive | minimum-up | open-wait | recovery | retransmit |
switch-link } seconds
```

Syntax Description

force-down	After RLM enters the down state, RLM will stay in the down state for a certain amount of time to make sure that the remote end will also enter the down state. After this occurs, both can be forced to be in sync again. This timer can also prevent RLM links from going up and down rapidly in an unstable network environment.
keepalive	A keepalive packet will be sent out from Network Access Server (NAS) to CSC periodically.
minimum-up	After a link is recovered from the failure state and RLM is in the up state, RLM will wait for a minimum time to make sure the new recovered link is stabilized before doing any operation.
open-wait	To overcome the latency while opening several links at the same time, RLM will use this timer to wait before opening the new links, and then choose the link with the highest weighting to become the active signaling link.
recovery	When the network access server (NAS) loses the active connection to CSC, it will try to reestablish the connection within the interval specified by this command. If it fails to reestablish the connection, RLM will declare that the RLM signaling link is down.
retransmit	Because RLM is operating under UDP, it needs to retransmit the control packet if the packet is not acknowledged within this retransmit interval.
switch-link	The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM will go into the recovery state.
<i>seconds</i>	Time, in seconds, before executing the designated function. Valid values for the seconds argument range from 1 to 600 seconds.

Defaults

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following example configures a ten second retransmission timer for unacknowledged control packets:

```
timer retransmit 10
```

Related Commands

Command	Description
clear interface virtual-access	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.

trunk activate port-threshold

To specify the percentage of available port resources required to enable a trunk card transmitter, use the **trunk activate port-threshold** command in global configuration mode. To restore the default value, use the **no** form of this command.

trunk activate port-threshold *resource-percentage*

no trunk activate

Syntax Description

<i>resource-percentage</i>	Decimal integer from 0 through 100 that indicates the percentage of universal port Dial Feature Card (DFC) resources required before a trunk line is enabled.
----------------------------	---

Command Default

No resource percentage is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **trunk activate port-threshold** command if you have a CT3 DFC and one or more universal port DFCs on the same platform and calls are dropped at system startup. This command enables the universal port modules to initialize before calls are routed to the platform. If the universal port modules do not initialize, the platform is identified as unavailable and calls are dropped.

Examples

The following example shows how to set the port threshold for the trunk card to 70 percent:

```
Router(config)# trunk activate port-threshold 70
```

trunk group (global)

To define or modify the definition of a trunk group and to enter trunk group configuration mode, use the **trunk group** command in global configuration mode. To delete the trunk group, use the **no** form of this command.

trunk group *name*

no trunk group *name*

Syntax Description

<i>name</i>	Name of the trunk group. Valid names contain a maximum of 63 alphanumeric characters.
-------------	---

Command Default

No trunk group is defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **trunk group** command to assign a number or a name to a set of trunk characteristics. The set of characteristics, or *profile*, is assigned to specific trunks as part of the usual trunk configuration steps.

The **trunk group** command initiates the profile definition and switches from global configuration to trunk group configuration mode. Additional commands are available to construct the characteristics of the profile.

Up to 1000 trunk groups can be configured on the gateway provided that the gateway has sufficient memory to store the profiles. If you see the message “Trunk group name could not be added as the threshold has been reached”, enter the **debug tgrm** command and check the number of trunk groups or check for insufficient memory.

To associate a trunk group with an interface, use the **trunk-group** (interface) command. A trunk group that was created using the **trunk group** (global) command can be associated with an interface. However, a trunk group need not be defined globally before being associated with an interface. If a trunk group has not been defined globally, it will be created by issuing the **trunk-group** (interface) command.

Examples

The following example creates trunk group 5 and configures the trunk group profile:

```
Router(config)# trunk group 5
Router(config-trunk-group)# carrier-id allcalls
Router(config-trunk-group)# max-calls voice 500 in
Router(config-trunk-group)# hunt-scheme round-robin even up
Router(config-trunk-group)# translation-profile incoming 3
Router(config-trunk-group)# translation-profile outgoing 2
Router(config-trunk-group)# exit
```

The following example creates a trunk group named “mytrunk” and configures the trunk group profile:

```
Router(config)# trunk group mytrunk
Router(config-trunk-group)# carrier-id local
Router(config-trunk-group)# max-calls voice 500
Router(config-trunk-group)# hunt-scheme least-idle
Router(config-trunk-group)# translation-profile incoming 1
Router(config-trunk-group)# translation-profile outgoing 12
Router(config-trunk-group)# exit
```

Related Commands

Command	Description
carrier-id (trunk group)	Identifies the carrier that owns the trunk group.
description (trunk group)	Permits a description to be associated with a trunk group.
hunt-scheme least-idle	Specifies the least-idle channel search method for incoming and outgoing calls.
hunt-scheme least-used	Specifies the least-used channel search method for incoming and outgoing calls.
hunt-scheme longest-idle	Specifies the longest-idle channel search method for incoming and outgoing calls.
hunt-scheme random	Specifies the random channel search method for incoming and outgoing calls.
hunt-scheme round-robin	Specifies the round-robin channel search method for incoming and outgoing calls.
hunt-scheme sequential	Specifies the sequential channel search method for incoming and outgoing calls.
max-calls	Specifies the number of incoming and outgoing voice and data calls that a trunk group can handle.
show trunk group	Displays the configuration of trunk groups.
translation-profile (trunk group)	Defines call number translation profiles for incoming and outgoing calls.
trunk-group (interface)	Assigns an ISDN PRI or NFAS interface to a trunk group.

trunk-group (timeslots)

To direct an outbound synchronous or asynchronous call initiated by dial-on-demand routing (DDR) to use specific B or digital service 0 (DS0) channels of an ISDN circuit on Cisco AS5800 series access servers, use the **trunk-group** command in CAS custom configuration, controller configuration, or interface configuration mode. To delete DS0s from the trunk group, use the **no** form of this command.

trunk-group *name* [**timeslots** *timeslot-list* [**preference** *preference-number*]]

no trunk-group *name* [**timeslots** *timeslot-list* [**preference** *preference-number*]]

Syntax Description

<i>name</i>	Trunk group name or label.
timeslots <i>timeslot-list</i>	(Optional) Selectively adds one or more DS0s from a DS1 to a trunk group. The <i>timeslot-list</i> argument accepts DS0s numbered from 1 to 24 for T1 links, and from 1 to 15 and 17 to 31 for E1 links. Successive DS0 numbers can be specified using commas, and ranges of numbers can be specified using a hyphen to separate the numbers. Groups of ranges can also be entered separated by commas. Default is that all DS0s in the signaling circuit are assigned to the trunk group.
preference <i>preference-number</i>	(Optional) Assigns a preference for DS0 members in a trunk group. Range is from 1 (highest preference) to 64 (lowest preference). The preference keyword appears only when the timeslots keyword has been used to configure DS0s.

Command Default

All DS0s in the signaling circuit are assigned to the trunk group.

Command Modes

CAS custom configuration
Controller configuration
Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Dial-out trunk groups can include individual DS0s from more than one DS1.

Two types of DS0 resources can be pooled: DS0s from common channel signaling circuits (CCS) such as PRI, Non-Facility Associated Signaling (NFAS), Signaling System 7 (SS7), and so on, and DS0s from channel-associated signaling (CAS) circuits.

The large-scale dial-out architecture is an integral part of dial-out trunk groups. The large-scale dial-out architecture is based on dialer rotary groups where physical interfaces are statically bound to dialer interfaces, meaning that the physical interfaces inherit the configuration parameters of the dialer interface. A call placed using a specific dialer interface (dialer rotary) can be done only through a rotary member, and this same rule applies to DDR over DS0 trunk groups.

As an example, a trunk group can have DS0s from three different physical interfaces that are also rotary members of a dialer interface. When an outgoing call is placed through the dialer interface, the Trunk Group Resource Manager (TGRM) provides a DS0 that belongs to a physical interface. The call will fail, however, if the physical interface is *not* a rotary member of a dialer interface. See the “Examples” section for more about the limitations large-scale dial-out places on selecting DS0s from physical interfaces.

The large-scale dial-out framework is used to place outgoing calls over a synchronous or asynchronous line. The framework also enables provisioning of dial-out configurations on an authentication, authorization, and accounting (AAA) server. A trunk group label can be configured as part of a **dialer string** command, or the large-scale dial-out framework can be used to download the trunk group identifier along with the dialer string.

Examples

CAS Configurations

The following examples show how to configure DS0 trunk groups on a CAS:

Example 1

```
Router(config)# controller t1 0
Router(config-controller)# ds0-group 2 timeslots 1-24
Router(config-controller)# cas-custom 2
Router(config-ctrl-cas)# trunk-group label3 timeslots 1-12
```

Example 2

```
Router(config)# controller t1 1
Router(config-controller)# ds0-group 3 timeslots 1-24
Router(config-controller)# cas-custom 3
Router(config-ctrl-cas)# trunk-group label1 timeslots 1-5,17-23 preference 1
Router(config-ctrl-cas)# trunk-group label2 timeslots 6-8,10-12,15 preference 2
```

NFAS Configuration

The following example shows how to configure NFAS/SS7 circuits. With these circuits, signaling can take place over a circuit different than the one over which the data is being transported. The DS0 dial-out trunk group configuration is done in controller configuration mode, because the trunk group is configured under the NFAS primary serial interface, all the NFAS group interface member DS0s are added into the trunk group. The NFAS primary serial interface will *not* have the **timeslots** keyword enabled under its configuration mode. The **timeslots** option is not available in the serial interface configuration mode because a serial interface may represent an NFAS serial interface. Remember that trunk group configurations under the NFAS member controllers and the respective serial interface (D channel) are mutually exclusive.

```
Router(config)# controller T1 0
Router(config-controller)# pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 0
Router(config-controller)# trunk-group L1 timeslots 1-5 preference 1
Router(config-controller)# trunk-group L2 timeslots 12-14 preference 2
Router(config-controller)# exit
Router(config)# controller T1 1
Router(config-controller)# pri-group timeslots 1-24 nfas_d backup nfas_int 1 nfas_group 0
Router(config-controller)# trunk-group L3 timeslots 1-5
Router(config-controller)# trunk-group L4 timeslots 12-14 preference 4
Router(config-controller)# exit
Router(config)# controller T1 3
Router(config-controller)# pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 0
Router(config-controller)# trunk-group L5 timeslots 7,9,11
Router(config-controller)# trunk-group L6 timeslots 2,4,6,14-16 preference 6
.
.
.
```

Configuring and Associating DS0 Trunk Groups for DDR

The following examples show how to configure the dialer interface and apply a static dial-out trunk configuration on the NAS.

The following example configures a static trunk group dialer association on the NAS:

```
Router(config)# interface dialer 0
Router(config-if)# dialer string 5550112 trunkgroup trunkgroup1
```

The following example configures a static dial-out trunk group on the NAS:

```
Router(config)# controller T1 6/1
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 16 timeslots 1,21-22 preference 1
Router(config-controller)# trunk-group 15 timeslots 18-19
```

The following example configures a dial-out trunk group Cisco AVPair:

```
Cisco-AVPair = "outbound:trunkgroup=number"
```

Dial-Out Trunk Groups in Dialer Rotary Configurations

In the following examples, dial-out trunk groups 15 and 16 have DS0s from PRI interfaces 0:23 and 6:23. These interfaces are also rotary members of dialer interface 0, and are configured correctly for dial-out trunk groups and outbound calling.

The following example configures the AAA server:

```
dialout-out Password="cisco"
  Cisco-AVPair = "outbound:trunkgroup=16"
  Service-Type = Outbound,
  Cisco:AVPair = "outbound:addr*10.121.94.254",
  Cisco:AVPair = "Outbound:dial-number=5551212",

RAS-5400-1 Password="cisco"
  Service-Type = Outbound,
  Framed-Route="10.121.94.254/32 Dialer0 200 name dialout"
  Framed-Route="10.121.94.0/24 10.121.94.254 200"
```

The following example configures a static dial-out trunk group on the NAS:

```
Router(config)# controller t1 0
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 16 timeslots 1,21-22 preference 1
Router(config-controller)# trunk-group 15 timeslots 18-19
.
.
.
Router(config)# interface serial 0:23
Router(config-if)# dialer rotary-group 0
Router(config-if)# exit
Router(config)# controller t1 6
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 16 timeslots 21-22
Router(config-controller)# trunk-group 15 timeslots 18-19 preference 2
.
.
.
Router(config)# interface serial 6:23
Router(config-if)# dialer rotary-group 0
```

In the following example, trunk group 15 has member DS0s from PRI interfaces 0:23, 6:23, and 7:23. When an outgoing call is placed through interface dialer 0, TGRM could return a DS0 that belongs to physical interfaces serial 6:23 or serial 7:23, which are not part of the same rotary group as serial 0:23. Because these physical serial interfaces are not rotary members of interface dialer 0, the call will fail.

The following example configures the AAA server incorrectly:

```
dialout-out Password="cisco"
  Cisco-AVPair = "outbound:trunkgroup=16"
  Service-Type = Outbound,
  Cisco-AVPair = "outbound:addr*10.121.94.254",
  Cisco-AVPair = "Outbound:dial-number=5551212",

RAS-5400-1 Password="cisco"
  Service-Type = Outbound,
  Framed-Route="10.121.94.254/32 Dialer0 200 name dialout"
  Framed-Route="10.121.94.0/24 10.121.94.254 200"
.
.
.
```

The following example configures the static dial-out trunk group on the NAS incorrectly:

```
Router(config)# controller t1 0
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 15 timeslots 1,21-22 preference 1
Router(config-controller)# trunk-group 16 timeslots 18-19
Router(config-controller)# exit
Router(config)# interface serial 0:23
Router(config-if)# dialer rotary-group 0
Router(config-if)# exit
Router(config)# controller t1 6
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 15 timeslots 21-22
Router(config-controller)# trunk-group 16 timeslots 18-19 preference 2
Router(config-controller)# exit
Router(config)# interface serial 6:23
Router(config-if)# dialer rotary-group 1
Router(config-if)# exit
Router(config)# controller t1 7
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 15 timeslots 18-19
Router(config-controller)# exit
Router(config)# interface serial 7:23
Router(config-if)# dialer rotary-group 1
```

Related Commands

Command	Description
dialer rotary group	Includes a specified interface in a dialer rotary group.
dialer string trunkgroup	Specifies a dial-out telephone number and dial-out trunk group name for a static configuration on an NAS.
pri-group timeslots	Specifies an ISDN PRI group on a channelized T1 or E1 controller, and releases the ISDN PRI signaling time slot.
show trunk group	Displays the configuration of a trunk group.

tunnel

To set up a network layer connection to a router, use the **tunnel** command in EXEC mode.

tunnel *host*

Syntax Description	<i>host</i>	Name or IP address of a specific host on a network that can be reached by the router.
---------------------------	-------------	---

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

If you are a mobile user, it is often impractical to dial in to your “home” router from a remote site. The asynchronous mobility feature allows you to dial in to different routers elsewhere on the internetwork while experiencing the same server environment that you would if you were connecting directly to your home router.

This asynchronous host mobility is accomplished by packet tunneling, a technique by which raw data from the dial-in user is encapsulated and transported directly to the host site where your home router performs the actual protocol processing.

You enable asynchronous mobility by entering the **tunnel** command to set up a network layer connection to a specified host. From a router other than a Cisco router, however, you need to use the Telnet protocol.

After a connection is established, you receive an authentication dialog or prompt from your home router and can proceed as if you are connected directly to it. When communications are complete, the network connection can be closed and terminated from either end of the connection.

Examples

The following example establishes a network layer connection with an IBM host named mktg:

```
Router> tunnel mktg
```

virtual-profile aaa



Note

Effective with Cisco IOS Release 12.2, the **virtual-profile aaa** command is not available in Cisco IOS software.

To enable virtual profiles by authentication, authorization, and accounting (AAA) configuration, use the **virtual-profile aaa** command in global configuration mode. To disable virtual profiles, use the **no** form of this command.

virtual-profile aaa

no virtual-profile aaa

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.0(7)T	This command was enhanced to allow virtual profiles to be downloaded from an AAA server using the High-Level Data Link Control (HDLC), Link Access Procedure, Balanced-terminal adapter (LAPB-TA), X.25, and Frame Relay encapsulations, in addition to the originally supported PPP encapsulation.
12.2	This command was removed.

Usage Guidelines

The effect of this command for any specific user depends on the router being configured for AAA and the AAA server being configured for that user's specific configuration information.

In releases later than Cisco IOS Release 12.2, the router automatically creates virtual profiles when AAA attributes require a profile.

Examples

The following example configures virtual profiles by AAA configuration only:

```
virtual-profile aaa
```

Related Commands	Command	Description
	aaa authentication	Enables AAA authentication to determine if a user can access the privileged command level.
	virtual-profile if-needed	Enables virtual profiles by virtual interface template.

virtual-profile if-needed

To specify that a virtual profile be used to create a virtual access interface only if the inbound connection requires a virtual access interface, use the **virtual-profile if-needed** command in global configuration mode. To create virtual access interfaces for every inbound connection, use the **no** form of this command.

virtual-profile if-needed

no virtual-profile if-needed

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

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

Usage Guidelines This command is intended to prevent the creating of virtual-access interfaces for inbound calls on physical interfaces that do not require virtual-access interfaces.

This command is compatible with local, RADIUS, and TACACS+ AAA.

Examples The following example enables selective virtual-access interface creation:

```
virtual-profile if-needed
```

Related Commands	Command	Description
	interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
	virtual-profile aaa	Enables virtual profiles by AAA configuration.
	virtual-profile virtual-template	Enables virtual profiles by virtual interface template.

virtual-profile virtual-template

To enable virtual profiles by virtual interface template, use the **virtual-profile virtual-template** command in global configuration mode. To disable this function, use the **no** form of this command.

virtual-profile virtual-template *number*

no virtual-profile virtual-template *number*

Syntax Description

number Number of the virtual template to apply, ranging from 1 to 30.

Command Default

Disabled. No virtual template is defined, and no default virtual template number is used.

Command Modes

Global configuration

Command History

Release	Modification
11.2F	This command was introduced.

Usage Guidelines

When virtual profiles are configured by virtual templates only, any interface-specific configuration information that is downloaded from the AAA server is ignored in configuring the virtual access interface for a user.

The **interface virtual-template** command defines a virtual template to be used for virtual profiles. Because several virtual templates might be defined for different purposes on the router (such as MLP, PPP over ATM, and virtual profiles), it is important to be clear about the virtual template number to use in each case.

Examples

The following example configures virtual profiles by virtual templates only. The number 2 was chosen because virtual template 1 was previously defined for use by Multilink PPP.

```
virtual-profile virtual-template 2
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

vty-async

To configure all virtual terminal lines on a router to support asynchronous protocol features, use the **vty-async** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no** form of this command.

vty-async

no vty-async

Syntax Description

This command has no arguments or keywords.

Command Default

By default, asynchronous protocol features are not enabled on virtual terminal lines.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **vty-async** command extends asynchronous protocol features from physical asynchronous interfaces to virtual terminal lines. Normally, SLIP and PPP can function only on asynchronous interfaces, not on virtual terminal lines. However, extending asynchronous functionality to virtual terminal lines permits you to run SLIP and PPP on these *virtual asynchronous interfaces*. One practical benefit is the ability to tunnel SLIP and PPP over X.25 PAD, thus extending remote node capability into the X.25 area. You can also tunnel SLIP and PPP over Telnet or LAT on virtual terminal lines. To tunnel SLIP and PPP over X.25, LAT, or Telnet, you use the protocol translation feature in the Cisco IOS software.

To tunnel SLIP or PPP inside X.25, LAT, or Telnet, you can use two-step protocol translation or one-step protocol translation, as follows:

- If you are tunneling SLIP or PPP using the two-step method, you need to first enter the **vty-async** command. Next, you perform two-step translation.
- If you are tunneling SLIP or PPP using the one-step method, you do not need to enter the **vty-async** command. You need to issue only the **translate** command with the SLIP or PPP keywords, because the **translate** command automatically enables asynchronous protocol features on virtual terminal lines.

Examples

The following example enables asynchronous protocol features on virtual terminal lines:

```
vty-async
```

Related Commands

Command	Description
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
translate	Enables asynchronous protocol features on virtual terminal lines.

vty-async dynamic-routing

To enable dynamic routing on all virtual asynchronous interfaces, use the **vty-async dynamic-routing** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, and therefore disable routing on virtual terminal lines, use the **no** form of this command.

vty-async dynamic-routing

no vty-async dynamic-routing

Syntax Description This command has no arguments or keywords.

Command Default Dynamic routing is not enabled on virtual asynchronous interfaces.

Command Modes Global configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines This feature enables IP routing on virtual asynchronous interfaces. When you issue this command and a user later makes a connection to another host using SLIP or PPP, the user must specify **/routing** on the SLIP or PPP command line.

If you had not previously entered the **vty-async** command, the **vty-async dynamic-routing** command creates virtual asynchronous interfaces, and then enables dynamic routing on them.

Examples The following example enables dynamic routing on virtual asynchronous interfaces:

```
vty-async dynamic-routing
```

Related Commands	Command	Description
	async dynamic routing	Enables manually configured routing on an asynchronous interface.
	vty-async	Enables manually configured routing on an asynchronous interface.

vty-async header-compression

To compress the headers of all TCP packets on virtual asynchronous interfaces, use the **vty-async header-compression** command in global configuration mode. To disable virtual asynchronous interfaces and header compression, use the **no** form of this command.

vty-async header-compression [passive]

no vty-async header-compression

Syntax Description

passive (Optional) Outgoing packets are compressed only when TCP incoming packets on the same virtual asynchronous interface are compressed. For SLIP, if you do not specify this option, the Cisco IOS software will compress all traffic. The default is no compression. For PPP, the Cisco IOS software always negotiates header compression.

Defaults

Header compression is not enabled on virtual asynchronous interfaces.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This feature compresses the headers on TCP/IP packets on virtual asynchronous connections to reduce the size of the packets and to increase performance. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers. The TCP header compression technique, described fully in RFC 1144, is supported on virtual asynchronous interfaces using SLIP or PPP encapsulation. You must enable compression on both ends of a connection.

Examples

The following example compresses outgoing TCP packets on virtual asynchronous interfaces only if incoming TCP packets are compressed:

```
vty-async header-compression passive
```

Related Commands

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

vty-async ipx ppp-client loopback

To enable IPX-PPP on virtual terminal lines, use the **vty-async ipx ppp-client loopback** command in global configuration mode. To disable IPX-PPP sessions on virtual terminal lines, use the **no** form of this command.

vty-async ipx ppp-client loopback *number*

no vty-async ipx ppp-client loopback

Syntax Description	<i>number</i>	Number of the loopback interface configured for IPX to which the virtual terminal lines are assigned.
---------------------------	---------------	---

Command Default	IPX over PPP is not enabled on virtual terminal lines.
------------------------	--

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

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines This command enables users to log into the router from a device running a virtual terminal protocol, then issue the PPP command at the EXEC prompt to connect to a remote device.

A loopback interface must already have been defined and an IPX network number must have been assigned to the loopback interface before the **vty-async ipx ppp-client loopback** command will permit IPX-PPP on virtual terminal lines.

Examples The following example enables IPX over PPP on virtual terminal lines:

```
ipx routing
interface loopback0
 ipx network 12345
vty-async ipx ppp-client loopback0
```

Related Commands	Command	Description
		interface loopback
	ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

vty-async keepalive

To change the frequency of keepalive packets on all virtual asynchronous interfaces, use the **vty-async keepalive** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no vty-async keepalive** command. To disable keepalive packets on virtual terminal lines, use the **vty-async keepalive 0** command.

vty-async keepalive *seconds*

no vty-async keepalive

vty-async keepalive 0

Syntax Description	<i>seconds</i> Frequency, in seconds, with which the Cisco IOS software sends keepalive messages to the other end of a virtual asynchronous interface. To disable keepalive packets, use a value of 0. The active keepalive interval range is 1 to 32767 seconds. Keepalive is disabled by default.
---------------------------	---

Command Default	Keepalive is disabled.
------------------------	------------------------

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

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	Use this command to change the frequency of keepalive updates on virtual asynchronous interfaces, or to disable keepalive updates. To determine if keepalive is enabled on an interface, use the show running-config command. If the router has not received a keepalive packet after three update intervals have passed, the connection is considered down.
-------------------------	---

Examples	The following example sets the keepalive interval to 30 seconds:
-----------------	--

```
vty-async keepalive 30
```

The following example sets the keepalive interval to 0 (off):

```
vty-async keepalive 0
```

Related Commands	Command	Description
	keepalive	Sets the keepalive timer for a specific interface.
	show running-config	Displays the contents of the currently running configuration file.

vty-async mtu

To set the maximum transmission unit (MTU) size on virtual asynchronous interfaces, use the **vty-async mtu** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no** form of this command.

vty-async mtu *bytes*

no vty-async

Syntax Description	<i>bytes</i>	MTU size of IP packets that the virtual asynchronous interface can support. The default MTU is 1500 bytes. Valid values for the MTU range from 64 bytes to 1000000 bytes.
---------------------------	--------------	---

Command Default	1500 bytes
------------------------	------------

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

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines Use this command to modify the MTU for packets on a virtual asynchronous interfaces. You might want to change to a smaller MTU size for IP packets transmitted on a virtual terminal line configured for asynchronous functions for any of the following reasons:

- The SLIP or PPP application at the other end only supports packets up to a certain size.
- You want to ensure a shorter delay by using smaller packets.
- The host echoing takes longer than 0.2 seconds.

Do not change the MTU size unless the SLIP or PPP implementation running on the host at the other end of the virtual asynchronous interface supports reassembly of IP fragments. Because each fragment occupies a spot in the output queue, it might also be necessary to increase the size of the SLIP or PPP hold queue if your MTU size is such that you might have a high amount of packet fragments in the output queue.

Examples The following example sets the MTU for IP packets to 256 bytes:

```
vty-async mtu 256
```

Related Commands	Command	Description
	mtu	Adjusts the maximum packet size or MTU size.

vty-async ppp authentication

To enable PPP authentication on virtual asynchronous interfaces, use the **vty-async ppp authentication** command in global configuration mode. To disable PPP authentication, use the **no** form of this command.

```
vty-async ppp authentication {chap | pap}
```

```
no vty-async ppp authentication {chap | pap}
```

Syntax Description

chap	Enables CHAP on all virtual asynchronous interfaces.
pap	Enables PAP on all virtual asynchronous interfaces.

Command Default

No CHAP or PAP authentication for PPP.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command configures the virtual asynchronous interface to either authenticate CHAP or PAP while running PPP. After you have enabled CHAP or PAP, the local router requires a password from remote devices. If the remote device does not support CHAP or PAP, no traffic will be passed to that device.

Examples

The following example enables CHAP authentication for PPP sessions on virtual asynchronous interfaces:

```
vty-async ppp authentication chap
```

Related Commands

Command	Description
ppp bap call	Sets PPP BACP call parameters.
ppp use-tacacs	Enables TACACS for PPP authentication.
vty-async	Configures all virtual terminal lines on a router to support asynchronous protocol features.
vty-async ppp use-tacacs	Enables TACACS authentication for PPP on virtual asynchronous interfaces.

vty-async ppp use-tacacs

To enable TACACS authentication for PPP on virtual asynchronous interfaces, use the **vty-async ppp use-tacacs** command in global configuration mode. To disable TACACS authentication on virtual asynchronous interfaces, use the **no** form of this command.

vty-async ppp use-tacacs

no vty-async ppp use-tacacs

Syntax Description This command has no arguments or keywords.

Command Default TACACS for PPP is disabled.

Command Modes Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command requires the extended TACACS server.

After you have enabled TACACS, the local router requires a password from remote devices.

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

If the username and password are contained in the CHAP password, the CHAP secret is not used by the router. Because most PPP clients require that a secret be specified, you can use any arbitrary string; Cisco IOS software ignores it.

You cannot enable TACACS authentication for SLIP on asynchronous or virtual asynchronous interfaces.

Examples

The example enables TACACS authentication for PPP sessions:

```
vty-async ppp use-tacacs
```

Related Commands

Command	Description
ppp use-tacacs	Enables TACACS for PPP authentication.
vty-async ppp authentication	Enables PPP authentication on virtual asynchronous interfaces.

vty-async virtual-template

To configure virtual terminal lines to support asynchronous protocol functions based on the definition of a virtual interface template, use the **vty-async virtual-template** command in global configuration mode. To disable virtual interface templates for asynchronous functions on virtual terminal lines, use the **no** form of this command.

vty-async virtual-template *number*

no vty-async virtual-template

Syntax Description	<i>number</i>	Virtual interface number.
---------------------------	---------------	---------------------------

Command Default	Asynchronous protocol features are not enabled by default on virtual terminal lines.
------------------------	--

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

Command History	Release	Modification
	10.3	The vty-async command was introduced.
	11.3	The vty-async virtual-template command was introduced.

Usage Guidelines	The vty-async virtual-template command enables you to support tunneling of SLIP or PPP across X.25, TCP, or LAT networks by using two-step protocol translation.
-------------------------	---

Before issuing the **vty-async virtual-template** command, create and configure a virtual interface template by using the **interface virtual-template** command. Configure this virtual interface as a regular asynchronous serial interface. That is, assign the virtual interface template the IP address of the Ethernet interface, and configure addressing, just as on an asynchronous interface. You can also enter commands in interface configuration mode that compress TCP headers or configure CHAP authentication for PPP.

After creating a virtual interface template, apply it by issuing the **vty-async virtual-template** command. When a user dials in through a virtual terminal line, the router creates a virtual access interface, which is a temporary interface that supports the asynchronous protocol configuration specified in the virtual interface template. This virtual access interface is created dynamically, and is freed up as soon as the connection drops.

Before virtual templates were implemented, you could use the **vty-async** command to extend asynchronous protocol functions from physical asynchronous interfaces to virtual terminal lines. However, in doing so, you created a virtual asynchronous interface, rather than the virtual access interface. The difference is that the virtual asynchronous interfaces are allocated permanently, whereas the virtual access interfaces are created dynamically when a user calls in and closed down when the connection drops.

You can have up to 25 virtual templates interfaces, but you can apply only one template to vty-async interfaces on a router. There can be up to 300 virtual access interfaces on a router.

Examples

The following example enables asynchronous protocol features on virtual terminal lines:

```
vty-async
vty-async virtual-template 1
vty-async dynamic-routing
vty-async header-compression
!
interface virtual-template1
 ip unnumbered Ethernet0
 encapsulation ppp
 no peer default ip address
 ppp authentication chap
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
vty-async	Configures all virtual terminal lines on a router to support asynchronous protocol features.

x25 aodi

To enable the Always On/Dynamic ISDN (AO/DI) client on an interface, use the **x25 aodi** command in interface configuration mode. To remove AO/DI client functionality, use the **no** form of this command.

x25 aodi

no x25 aodi

Syntax Description

This command has no arguments or keywords.

Command Default

AO/DI client is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3T	This command was introduced.

Usage Guidelines

Use this command to enable the AO/DI client on an interface.

Examples

The following example enables the AO/DI client on the interface running X.25, using the **x25 aodi** command:

```
interface bri0
  isdn x25 dchannel
  isdn x25 static-tei 8
interface bri0:0
  x25 aodi
  x25 address 12135551234
  x25 htc 4
  x25 win 3
  x25 wout 3
  x25 map ppp 12135556789 interface dialer 1
```



Note

Configuring the BRI interface with the **isdn x25 dchannel** command creates a configurable interface (bri 0:0) for other necessary X.25 commands. Refer to the description for this command earlier in this publication for additional information about this command.

Related Commands

Command	Description
isdn x25 dchannel	Creates a configurable interface for X.25 traffic over the ISDN D channel.

x25 map ppp

To enable a PPP session over the X.25 protocol, use the **x25 map ppp** command in interface configuration mode. To remove a prior mapping, use the **no** form of this command.

```
x25 map ppp x121-address interface cloning-interface [no-outgoing]
```

```
no x25 map ppp x121-address interface cloning-interface [no-outgoing]
```

Syntax Description

<i>x121-address</i>	X.121 address as follows: <ul style="list-style-type: none"> Client side—The calling number. Server side—The called number.
interface <i>cloning-interface</i>	Interface to be used for cloning the configuration.
no-outgoing	(Optional) Ensures that the X.25 map does not originate calls.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3T	This command was introduced.

Usage Guidelines

Use **x25 map ppp** command to allow a PPP session to run over X.25.

The **interface** keyword refers to the interface that will be used to clone the configuration.



Note

For the **x25 map** command used in standard X.25 implementations, refer to the *Cisco IOS Wide-Area Networking Command Reference* publication.

Examples

Client Examples

The following example enables the AO/DI client on the interface and configures the D channel (BRI interface 0:0) with the x25 map statement in order to allow PPP sessions over X.25 encapsulation with the configured AO/DI server:

```
interface BRI0:0
  x25 address 16193368208
  x25 aodi
  x25 htc 4
  x25 win 3
  x25 wout 3
  x25 map ppp 16193368209 interface dialer 1
```

Server Examples

The following example enables the AO/DI server to receive calls from the AO/DI client and configures the D channel (BRI0:0) with the x25 map statement which allows PPP sessions over X.25 encapsulation with the configured AO/DI client. The **no-outgoing** option is used with the x.25 map command since the AO/DI server is receiving, versus initiating, calls.

```
interface BRI0:0
x25 address 16193368209
  x25 htc 4
  x25 win 3
  x25 wout 3
x25 map ppp 16193368208 interface dialer 1 no-outgoing
```

**Note**

Configuring the BRI interface with the **isdn x25 dchannel** command creates a configurable interface (bri 0:0).

Related Commands

Command	Description
isdn x25 dchannel	Creates a configurable interface for X.25 traffic over the ISDN D channel.

