

ping

To diagnose basic network connectivity on AppleTalk, ATM, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, or source-route bridging (SRB) networks, use the **ping** command in user EXEC or privileged EXEC mode.

```
ping [[protocol [tag] {host-name | system-address}]]
```

Syntax Description		
<i>protocol</i>	(Optional) Protocol keyword, one of appletalk , atm , clns , decnet , ipx , or srb . If a specific protocol is not specified, a basic ping will be sent using IP (IPv4). For extended options for ping over IP, see the documentation for the ping ip command.	Note The ping atm interface atm , ping ip , ping ipv6 , ping sna , and ping vrf commands are documented separately.
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.	
<i>host-name</i>	Host name of the system to ping. If a <i>host-name</i> or <i>system-address</i> is not specified at the command line, it will be required in the ping system dialog.	
<i>system-address</i>	Address of the system to ping. If a <i>host-name</i> or <i>system-address</i> is not specified at the command line, it will be required in the ping system dialog.	

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	The ping sna command was introduced.
	12.1(12c)E	The ping vrf command was introduced.
	12.2(2)T	Support for the IPv6 protocol was added.
	12.2(13)T	The atm protocol keyword was added.
		The following keywords were removed because the Apollo Domain, Banyan VINES, and XNS protocols are no longer supported in Cisco IOS software:
		<ul style="list-style-type: none"> • apollo • vines • xns

Usage Guidelines	
	The ping command sends an echo request packet to an address, and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning. For example, the ping clns command sends International Organization for Standardization (ISO) CLNS echo packets to test the reachability of a remote router over a connectionless Open System Interconnection (OSI) network.

If you enter the **ping** command without any other syntax (**ping**<cr>), the CLI will display an interactive system dialog that prompts you for the additional syntax appropriate to the protocol you specify (See the “Examples” section).

To exit the interactive ping dialog before responding to all the prompts, type the escape sequence. The default escape sequence is **Ctrl-^,X** (Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key). The escape sequence will vary depending on your line configuration. For example, another commonly used escape sequence is **Ctrl-c**.

Table 53 describes the test characters sent by the **ping** facility.

Table 53 ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.



Note

Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and can be answered only by another Cisco router.

The availability of protocol keywords depends on what protocols are enabled on your system.

Issuing the **ping** command in User EXEC mode will generally offer fewer syntax options than issuing the **ping** command in Privileged EXEC mode.

Examples

After you enter the **ping** command in privileged EXEC mode, the system prompts you for a protocol keyword. The default protocol is IP.

If you enter a host name or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample dialog from the **ping** command using default values. The specific dialog varies somewhat from protocol to protocol.

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 54 describes the significant fields shown in the display.

Table 54 ping Field Descriptions for IP

Field	Description
Protocol [ip]:	Prompts for a supported protocol. Default: ip .
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds).
Extended commands [n]:	Specifies whether a series of additional commands appears.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs ¹ configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

1. MTU = maximum transmission unit

The following example verifies connectivity to the neighboring ATM device for the ATM PVC with the virtual path identifier (VPI)/virtual channel identifier (VCI) value 0/16:

```
Router# ping

Protocol [ip]:atm
ATM Interface:atm1/0
VPI value [0]:
VCI value [1]:16
Loopback - End(0), Segment(1) [0]:1
Repeat Count [5]:
Timeout [2]:
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Table 55 describes the default ping fields shown in the display.

Table 55 ping Field Descriptions for ATM

Field	Description
Protocol [ip]:	Prompt for a supported protocol. Enter appletalk , atm , clns , ip , novell , apollo , vines , decnet , or xns . Default: ip .
ATM Interface:	Prompt for the ATM interface.
VPI value [0]:	Prompt for the virtual path identifier. Default: 0.
VCI value [1]:	Prompt for the virtual channel identifier. Default: 1.
Loopback - End(0), Segment(1) [0]:	Prompt to specify end loopback, which verifies end-to-end PVC integrity, or segment loopback, which verifies PVC integrity to the neighboring ATM device. Default: segment loopback.
Repeat Count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Timeout [2]:	Timeout interval. Default: 2 (seconds).
!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/1/1 ms	Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Commands

Command	Description
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests network connectivity on IP networks.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.
ping vrf	Tests the connection in the context of a specific VPN (VRF).

ping ip

To test network connectivity on IP networks, use the **ping ip** command in privileged EXEC mode.

```
ping ip {host-name | ip-address} [data [hex-data-pattern]] | df-bit | repeat [repeat-count] | size
[datagram-size] [source {source-address | source-interface} ] [timeout seconds] [validate]
[verbose]
```

Syntax Description	
<i>host-name</i>	Host name of the system to ping.
<i>system-address</i>	Address of the system to ping.
data <i>hex-data-pattern</i>	(Optional) Specifies the data pattern. Range is from 0 to FFFF.
df-bit	(Optional) Enables the “do-not-fragment” bit in the IP header.
repeat <i>repeat-count</i>	(Optional) Specifies the number of pings sent. The range is from 1 to 2147483647. The default is 5.
size	(Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping.
<i>datagram-size</i>	(Optional) Range is from 40 to 18024.
source	(Optional) Specifies the source address or source interface.
<i>source-address</i>	(Optional) IP address to use as the source in the ping packets.
<i>source-interface</i>	(Optional) Name of the interface from which the ping should be sent, and the Interface ID (slot/port/number). Interface name keywords include the following: <ul style="list-style-type: none"> • async (Asynchronous Interface) • bvi (Bridge-Group Virtual Interface) • ctunnel • dialer • ethernet • fastEthernet • lex • loopback • multilink (Multilink-group interface) • null • port-channel (Ethernet channel of interfaces) • tunnel • vif (PGM Multicast Host interface) • virtual-template • virtual-tokenring • xtagatm (Extended Tag ATM interface) <p>The availability of these keywords depends on your system hardware.</p>
timeout <i>seconds</i>	(Optional) Specifies the timeout interval in seconds. The default is 2 seconds. Range is from 0 to 3600.

validate	(Optional) Validates the reply data.
verbose	(Optional) Enables verbose output, which lists individual ICMP packets, as well as Echo Responses.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0	The data , df-bit , repeat , size , source , timeout , and validate keywords were added.

Usage Guidelines

The **ping** command sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

To abnormally terminate a ping session, type the escape sequence—by default, **Ctrl-^ X**. You type the default by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

[Table 56](#) describes the test characters that the ping facility sends.

Table 56 ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
U	A destination unreachable error protocol data unit (PDU) was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.

**Note**

Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are only answered by another Cisco router.

Examples

After you enter the **ping** command in privileged mode, the system prompts you for a protocol keyword. The default protocol is IP.

If you enter a host name or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

The optional **data**, **df-bit**, **repeat**, **size**, **source**, **timeout**, and **validate** keywords can be used to avoid extended **ping** command output. You can use as many of these keywords as you need, and you can use them in any order after the *host-name* or *system-address* arguments.

Although the precise dialog varies somewhat from protocol to protocol, all are similar to the ping session using default values shown in the following output:

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

Table 57 describes the default ping fields shown in the display.

Table 57 ping Field Descriptions

Field	Description
Protocol [ip]:	Prompts for a supported protocol. The default is IP.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. The default is none.
Repeat count [5]:	Prompts for the number of ping packets that will be sent to the destination address. The default is 5 packets.
Datagram size [100]:	Prompts for the size of the ping packet (in bytes). The default is 100 bytes.
Timeout in seconds [2]:	Prompts for the timeout interval. The default is 2 seconds.
Extended commands [n]:	Specifies whether a series of additional commands appears.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the MTUs configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
!!!!	Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type.
Success rate is 100 percent	Indicates the percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Indicates the round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

Related Commands

Command	Description
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping vrf	Tests the connection in the context of a specific VPN (VRF).

ping vrf

To test a connection in the context of a specific VPN connection, use the **ping vrf** command in Exec mode.

```
ping vrf vrf-name [tag] [connection] target-address [connection-options]
```

Syntax Description

<i>vrf-name</i>	The name of the VPN (VRF context).
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
<i>connection</i>	(Optional) Connection options include atm , clns , decnet , ip , ipv6 , ipx , sna , or srp . The default is ip .
<i>target-address</i>	The destination ID for the ping operation. Usually, this is the IP-address of the host. For example, the target for an IP ping in a VRF context would be the IP address or domain name of the target host. <ul style="list-style-type: none"> If the target address is not specified, the CLI will enter the interactive dialog for ping.
<i>connection-options</i>	Each connection type may have its own set of connection options. For example, connection options for IP include source , df-bit , and timeout . See the appropriate ping command documentation for details.

Defaults

The default connection type for ping is IP (specifically, IPv4).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(12c)E, 12.2	This command was introduced.

Usage Guidelines

A VPN routing/forwarding (VRF) instance is used to identify a VPN. To check if a configured VRF is working, you can use the **ping vrf** command.

When attempting to ping from a provider edge (PE) router to a customer edge (CE) router, or from a PE router to PE router, the standard **ping** command will not usually work. The **ping vrf** command allows you to ping the IP addresses of LAN interfaces on CE routers.

If you are on a PE router, be sure to indicate the specific VRF (VPN) name, as shown in the “Examples” section.

If all required information is not provided at the command line, the system will enter the interactive dialog (extended mode) for ping.

Examples

In the following example, the target host in the domain 209.165.201.1 is pinged (using IP/ICMP) in the context of the “Customer_A” VPN connection.

```
Router# ping vrf Customer_A 209.165.201.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 176/264/576 ms
```

Pressing the Enter key before providing all of the required options will begin the interactive dialog for ping. In the following example, the interactive dialog is started after the “ip” protocol is specified, but no address is given:

```
Router# ping vrf Customer_B ip
```

```
Target IP address: 209.165.200.225
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
Packet has IP options: Total option bytes= 39, padded length=40
Record route: <*>
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
.
.
.
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The following example shows the various options for IP in the **ping vrf** command:

```
Router# show parser dump exec | include ping vrf
```

```
1 ping vrf <string>
1 ping vrf <string> ip <string>
1 ping vrf <string> ip (interactive)
1 ping vrf <string> ip <string>
1 ping vrf <string> ip <string> source <address>
1 ping vrf <string> ip <string> source <interface>
1 ping vrf <string> ip <string> repeat <1-2147483647>
1 ping vrf <string> ip <string> size Number
1 ping vrf <string> ip <string> df-bit
1 ping vrf <string> ip <string> validate
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> ip <string> verbose
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
```

```
1 ping vrf <string> tag
1 ping vrf <string> atm
1 ping vrf <string> ipv6
1 ping vrf <string> appletalk
1 ping vrf <string> decnet
1 ping vrf <string> clns
1 ping vrf <string> ipx
1 ping vrf <string> sna
1 ping vrf <string> srb
```

Related Commands

Command	Description
ping	Diagnoses basic network connectivity to a specific host.
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests the connection to a remote host on the network using IPv4.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.

policy (ERM)

<i>protocol</i>	(Optional) Protocol keyword, one of atm , clns , decnet , ipx , or srb . Note The ping atm interface atm , ping ip , ping ipv6 , ping sna , and ping vrf commands are documented separately.
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
<i>host-name</i>	Host name of the system to ping. If a <i>host-name</i> or <i>system-address</i> is not specified at the command line, it will be required in the ping system dialog.
<i>system-address</i>	Address of the system to ping. If a <i>host-name</i> or <i>system-address</i> is not specified at the command line, it will be required in the ping system dialog.

To configure an ERM resource policy, use the **policy** command in ERM configuration mode. To disable this function, use the **no** form of this command.

```
policy policy-name [global | type resource-user-type]
```

```
no policy policy-name
```

Syntax Description

<i>policy-name</i>	Name of the policy you want to configure.
global	(Optional) Configures a global policy.
type resource-user-type	(Optional) Specifies a type for the policy you are configuring. The <i>resource-user-type</i> argument specifies the name of the resource user type.

Command Default

Disabled

Command Modes

ERM configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

You can configure a resource policy only in ERM configuration mode.

Examples

The following example shows how to configure a resource policy with the policy name `cpu_mem_policy` and the resource type `iosprocess`:

```
Router(config-erm)# policy cpu_mem_policy type iosprocess
```

Related Commands

Command	Description
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
show resource database	Displays the resource database details.
show resource owner	Displays the resource owner details.
show resource relationship	Displays the resource relationship details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level resource owners.

policy (resource group)

To apply an already configured policy to a specified resource group, use the **policy** command in resource group configuration mode. To disable this function, use the **no** form of this command.

policy *policy-name*

no policy *policy-name*

Syntax Description	<i>policy-name</i>	Applies the specified policy to a resource group. The <i>policy-name</i> argument specifies the name of the policy you want to apply to the resource group.
Command Default	Disabled	
Command Modes	Resource group configuration	
Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines

Before applying a policy to a resource group, you must configure a resource policy using the **policy** *policy-name* command in ERM configuration mode and create a resource group using the **user group** *resource-group-name* **type** *resource-user-type* command in ERM configuration mode.

When you apply a policy using the **policy** *policy-name* command in resource group configuration mode, you are applying a policy (which contains the thresholds) to the resource group you created using the **user group** *resource-group-name* **type** *resource-user-type* command in ERM configuration mode.

For example, say you have created a resource group with the name lowPrioUsers and iosprocess as the type. You have some low-priority RUs or tasks like HTTP and SNMP, and you want to set a threshold for all the low-priority RUs together, not separately. You must add the RUs to the resource group using the **instance** *instance-name* command and then apply a resource policy. If the resource policy you applied sets a minor rising threshold value of 10% for the resource group, then when the accumulated usage of both HTTP and SNMP RUs crosses the 10% mark, a notification is sent to the RUs in the resource group lowPrioUsers. That is, if HTTP usage is 4% and SNMP usage is 7%, then a notification is sent to the resource group. This facility helps to set thresholds for a group of RUs, as it is difficult to set a threshold for every single RU.

Examples

The following example shows how to apply a resource policy named cpu_mem_policy to a resource group named lowPrioUsers:

```
Router(config-erm)# user group lowPrioUsers type iosprocess
Router(config-res-group)# policy group-policy1
```

Related Commands	Command	Description
	instance (resource group)	Adds the RUs to the resource group.
	policy (ERM)	Configures an ERM resource policy.
	resource policy	Enters ERM configuration mode.
	user (ERM)	Creates a resource group.

policy-list

To associate a policy list with a Command Scheduler occurrence, use the **policy-list** command in kron-occurrence configuration mode. To delete a policy list from the Command Scheduler occurrence, use the **no** form of this command.

policy-list *list-name*

no policy-list *list-name*

Syntax Description	<i>list-name</i>	Name of policy list. If the <i>list-name</i> is new, a policy list structure will be created. If the <i>list-name</i> is not new, the existing policy list will be edited.
--------------------	------------------	--

Defaults	No policy list is associated.
----------	-------------------------------

Command Modes	Kron-occurrence configuration (config-kron-occurrence)
---------------	--

Command History	Release	Modification
	12.3(1)	This command was introduced.

Usage Guidelines

Use the **policy-list** command with the **kron occurrence** command to schedule one or more policy lists to run at the same time or interval. Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy list containing EXEC command line interface (CLI) commands to be scheduled to run on the router at a specified time.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and can it be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a Command Scheduler occurrence named may and associate a policy list named sales-may with the occurrence:

```
Router(config)# kron occurrence may at 6:30 may 20 oneshot
Router(config-kron-occurrence)# policy-list sales-may
```

Related Commands	Command	Description
	cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
	kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
	kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.

poll-interval

To configure the polling interval for a bulk statistics schema, use the **poll-interval** command in Bulk Statistics Schema configuration mode. To remove a previously configured polling interval, use the **no** form of this command.

poll-interval *minutes*

no poll-interval *minutes*

Syntax Description	<i>minutes</i>	Polling interval of data for this schema in minutes. The valid range is from 1 minute to 20000 minutes. The default is 5 minutes.
---------------------------	----------------	---

Defaults Object instances are polled once every five minutes.

Command Modes Bulk Statistics Schema configuration (config-bulk-sc)

Command History	Release	Modification
	12.0(24)S	This command was introduced.
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines The **poll-interval** command sets how often the MIB instances specified by the schema and associated object list are to be polled. Collected data is stored in the local bulk statistics file for later transfer.

Examples In the following example the polling interval for bulk statistics collection is set to once every 3 minutes in the schema called Ethernet2/1-CAR:

```
Router(config)# snmp mib bulkstat schema Ethernet2/1-CAR
Router(config-bulk-sc)# object-list CAR-mib
Router(config-bulk-sc)# poll-interval 3
Router(config-bulk-sc)# instance wildcard oid 3.1
Router(config-bulk-sc)# exit
```

Related Commands	Command	Description
	snmp mib bulkstat schema	Names a bulk statistics schema and enters Bulk Statistics Schema configuration mode.

printer

To configure a printer and assign a server tty line (or lines) to it, use the **printer** command in global configuration mode. To disable printing on a tty line, use the **no** form of this command.

```
printer printer-name {line number | rotary number} [newline-convert | formfeed]
```

```
no printer
```

Syntax Description

<i>printer-name</i>	Printer name.
line <i>number</i>	Assigns a tty line to the printer.
rotary <i>number</i>	Assigns a rotary group of tty lines to the printer.
newline-convert	(Optional) Converts newline (linefeed) characters to a two-character sequence “carriage-return, linefeed” (CR+LF).
formfeed	(Optional) Causes the Cisco IOS software to send a form-feed character (ASCII 0x0C) to the printer tty line immediately following each print job received from the network.

Defaults

No printers are defined by default.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command enables you to configure a printer for operations and assign either a single tty line or a group of tty lines to it. To make multiple printers available through the same printer name, specify the number of a rotary group.

In addition to configuring the printer with the **printer** command, you must modify the file `/etc/printcap` on your UNIX system to include the definition of the remote printer in the Cisco IOS software. Refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* for additional information.

Use the optional **newline-convert** keyword in UNIX environments that cannot handle single-character line terminators. This converts newline characters to a carriage-return, linefeed sequence. Use the **formfeed** keyword when using the line printer daemon (lpd) protocol to print and your system is unable to separate individual output jobs with a form feed (page eject). You can enter the **newline-convert** and **formfeed** keywords together and in any order.

Examples

In the following example a printer named `printer1` is configured and output is assigned to tty line 4:

```
Router(config)# printer printer1 line 4
```

Related Commands

Command	Description
clear line	Returns a terminal line to idle state.

private

To save user EXEC command changes between terminal sessions, use the **private** command in line configuration mode. To restore the default condition, use the **no** form of this command.

private

no private

Syntax Description

This command has no arguments or keywords.

Defaults

User-set configuration options are cleared with the **exit** EXEC command or when the interval set with the **exec-timeout** line configuration command has passed.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command ensures that the terminal parameters set by the user remain in effect between terminal sessions. This behavior is desirable for terminals in private offices.

Examples

In the following example, line 15 (in this example, vty 1) is configured to keep all user-supplied settings at system restarts:

```
Router(config)# line 15
Router(config-line)# private
```

Related Commands

Command	Description
exec-timeout	Sets the interval that the EXEC command interpreter waits until user input is detected.
exit	Exits any configuration mode, or closes an active terminal session and terminates the EXEC.

process cpu statistics limit entry-percentage

To set the process entry limit and the size of the history table for CPU utilization statistics, use the **process cpu statistics limit entry-percentage** command in global configuration mode. To disable CPU utilization statistics, use the **no** form of this command.

process cpu statistics limit entry-percentage *number* [**size** *seconds*]

no process cpu statistics limit entry-percentage

Syntax Description

<i>number</i>	Sets the percentage (1 to 100) of CPU utilization that a process must use to become part of the history table.
<i>size seconds</i>	(Optional) Changes the duration of time in seconds for which CPU statistics are stored in the history table. Valid values are 5 to 86400. The default is 600.

Defaults

size seconds: 600 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Use the **process cpu statistics limit entry-percentage** command to set the entry limit and size of CPU utilization statistics.

Examples

The following example shows how to set an entry limit at 40 percent and a size of 300 seconds:

```
Router(config)# process cpu statistics limit entry-percentage 40 size 300
```

Related Commands

Command	Description
process cpu threshold type	Defines CPU usage thresholds that, when crossed, cause a CPU threshold notification.
snmp-server enable traps cpu	Enables CPU threshold violations traps.
snmp-server host	Specifies the recipient of SNMP notifications.

process cpu threshold type

To set CPU thresholding notification types and values, use the **process cpu threshold type** command in global configuration mode. To disable CPU thresholding notifications, use the **no** form of this command.

```
process cpu threshold type { total | process | interrupt } rising percentage interval seconds
[falling percentage interval seconds]
```

```
no process cpu threshold type { total | process | interrupt }
```

Syntax Description

total	Sets the CPU threshold type to total CPU utilization.
process	Sets the CPU threshold type to CPU process utilization.
interrupt	Sets the CPU threshold type to CPU interrupt utilization.
rising <i>percentage</i>	The percentage (1 to 100) of CPU resources that, when exceeded for the configured interval, triggers a CPU thresholding notification.
interval <i>seconds</i>	The duration of the CPU threshold violation, in seconds (5 to 86400), that must be met to trigger a CPU thresholding notification.
falling <i>percentage</i>	(Optional) The percentage (1 to 100) of CPU resources that, when usage falls below this level for the configured interval, triggers a CPU thresholding notification. <ul style="list-style-type: none"> This value must be equal to or less than that of the rising <i>percentage</i> argument. If not specified, the falling <i>percentage</i> argument is set to the same value as the rising <i>percentage</i> argument.

Defaults

CPU thresholding notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

This command defines CPU usage thresholds that, when crossed, cause a CPU thresholding notification. When this command is enabled, Cisco IOS software polls the system at the configured interval. Notification occurs in two situations:

- When a configured CPU usage threshold is exceeded (**rising** *percentage*)
- When CPU usage falls below the configured threshold (**falling** *percentage*)

Examples

The following example shows how to set the total CPU utilization notification threshold at 80 percent for a rising threshold notification and 20 percent for a falling threshold notification, with a 5-second polling interval.

```
Router(config)# process cpu threshold type total rising 80 interval 5 falling 20
interval 5
```

Related Commands

Command	Description
process cpu statistics limit entry	Sets the entry limit and size of CPU utilization statistics.
snmp-server enable traps cpu	Enables CPU threshold violations traps.
snmp-server host	Specifies the recipient of SNMP notifications.

process-max-time

To configure the amount of time after which a process should voluntarily yield to another process, use the **process-max-time** command in global configuration mode. To reset this value to the system default, use the **no** form of this command.

process-max-time *milliseconds*

no process-max-time *milliseconds*

Syntax Description	<i>milliseconds</i>	Maximum duration (in milliseconds) that a process can run before suspension. The range is from 20 to 200 milliseconds.
---------------------------	---------------------	--

Defaults	The default maximum process time is 200 milliseconds.
-----------------	---

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

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines	Lowering the maximum time a process can run is useful in some circumstances to ensure equitable division of CPU time among different tasks.
-------------------------	---

Only use this command if recommended to do so by the Cisco Technical Assistance Center (TAC).

Examples	The following example limits the duration that a process will run to 100 milliseconds:
-----------------	--

```
Router(config)# process-max-time 100
```

processes cpu autoprofile hog

To enable automatic profiling of CPUHOGs, use the **processes cpu autoprofile hog** command in global configuration mode. To disable this function, use the **no** form of this command.

processes cpu autoprofile hog

no processes cpu autoprofile hog

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Global configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines This command enables automatic profiling of CPUHOGS by monitoring the CPUHOG process and starting the profiling process at the same time.

Examples The following example shows how to enable automatic profiling of CPUHOGS:

```
Router(config)# processes cpu autoprofile hog
```

Related Commands	Command	Description
	show processes cpu autoprofile hog	Displays the profile data for CPUHOG.

processes cpu extended

To enable or disable the collection or to change the history size of extended CPU load, use the **processes cpu extended** command in global configuration mode. If the command is not configured, the default behavior is to collect one minute history. To disable this function, use the **no** form of this command.

processes cpu extended [*history history-size*]

no processes cpu extended

Syntax Description	history <i>history-size</i>	Specifies the size of the history (in 5 second increments) to be collected for extended CPU load. Valid values are from 2 to 720. The default <i>history-size</i> is 12, which is equivalent to a one minute history.
---------------------------	------------------------------------	--

Command Default	Enabled
------------------------	---------

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

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Examples The following example shows how to enable the collection of extended CPU load for a history size of 36 (which is equivalent to 3 minutes of history):

```
Router(config)# processes cpu extended history 36
```

Related Commands	Command	Description
	show processes cpu extended	Displays an extended CPU load report.

prompt

To customize the CLI prompt, use the **prompt** command in global configuration mode. To revert to the default prompt, use the **no** form of this command.

prompt *string*

no prompt [*string*]

Syntax Description

<i>string</i>	Text that will be displayed on screen as the CLI prompt, including any desired prompt variables.
---------------	--

Defaults

The default prompt is either `Router` or the name defined with the **hostname** global configuration command, followed by an angle bracket (>) for user EXEC mode or a pound sign (#) for privileged EXEC mode.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

You can include customized variables when specifying the prompt. All prompt variables are preceded by a percent sign (%). [Table 58](#) lists the available prompt variables.

Table 58 Custom Prompt Variables

Prompt Variable	Interpretation
%h	Host name. This is either <i>Router</i> or the name defined with the hostname global configuration command.
%n	Physical terminal line (tty) number of the EXEC user.
%p	Prompt character itself. It is either an angle bracket (>) for user EXEC mode or a pound sign (#) for privileged EXEC mode.
%s	Space.
%t	Tab.
%%	Percent sign (%)

Issuing the **prompt %h** command has the same effect as issuing the **no prompt** command.

Examples

The following example changes the EXEC prompt to include the tty number, followed by the name and a space:

```
Router(config)# prompt TTY%n@%h%s%p
```

The following are examples of user and privileged EXEC prompts that result from the previous command:

```
TTY17@Router1 > enable  
TTY17@Router1 #
```

Related Commands

Command	Description
hostname	Specifies or modifies the host name for the network server.

pwd

To show the current setting of the **cd** command, use the **pwd** command in user EXEC or privileged EXEC mode.

pwd

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **pwd** command to show which directory or file system is specified as the default by the **cd** command. For all EXEC commands that have an optional *filesystem* argument, the system uses the file system specified by the **cd** command when you omit the optional *filesystem* argument.

For example, the **dir** command contains an optional *filesystem* argument and displays a list of files on a particular file system. When you omit this *filesystem* argument, the system shows a list of the files on the file system specified by the **cd** command.

Examples

The following example shows that the present working file system specified by the **cd** command is slot 0:

```
Router> pwd
slot0:/
```

The following example uses the **cd** command to change the present file system to slot 1 and then uses the **pwd** command to display that present working file system:

```
Router> cd slot1:
Router> pwd
slot1:/
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.

redistribute (IP)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in router configuration mode. To disable redistribution, use the **no** form of this command.

```
redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [as-number] [metric {metric-value | transparent}] [metric-type type-value] [match {internal | external 1 | external 2}] [tag tag-value] [route-map map-tag] [subnets]
```

```
no redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [as-number] [metric {metric-value | transparent}] [metric-type type-value] [match {internal | external 1 | external 2}] [tag tag-value] [route-map map-tag] [subnets]
```

Syntax Description	
<i>protocol</i>	<p>Source protocol from which routes are being redistributed. It can be one of the following keywords: bgp, connected, eigrp, isis, mobile, ospf, static [ip], or rip.</p> <p>The static [ip] keyword is used to redistribute IP static routes. The optional ip keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol.</p> <p>The connected keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes will be redistributed as external to the autonomous system.</p>
<i>process-id</i>	<p>(Optional) For the bgp or eigrp keyword, this is an autonomous system number, which is a 16-bit decimal number.</p> <p>For the isis keyword, this is an optional <i>tag</i> value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing.</p> <p>For the ospf keyword, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number.</p> <p>For the rip keyword, no <i>process-id</i> value is needed.</p>
level-1	Specifies that for IS-IS Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that for IS-IS both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that for IS-IS Level 2 routes are redistributed into other IP routing protocols independently.
<i>as-number</i>	(Optional) Autonomous system number for the redistributed route.
metric <i>metric-value</i>	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.

transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.
metric-type <i>type-value</i>	<p>(Optional) For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values:</p> <ul style="list-style-type: none"> • 1—Type 1 external route • 2—Type 2 external route <p>If a metric-type is not specified, the Cisco IOS software adopts a Type 2 external route.</p> <p>For IS-IS, it can be one of two values:</p> <ul style="list-style-type: none"> • internal—IS-IS metric that is < 63. • external—IS-IS metric that is > 64 < 128. <p>The default is internal.</p>
match { internal external 1 external 2 }	<p>(Optional) For the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following:</p> <ul style="list-style-type: none"> • internal—Routes that are internal to a specific autonomous system. • external 1—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route. • external 2—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.
tag <i>tag-value</i>	(Optional) 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
<i>map-tag</i>	(Optional) Identifier of a configured route map.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Command Default

Route redistribution is disabled.
protocol: No source protocol is defined.
process-id: No process ID is defined.
metric *metric-value*: 0
metric-type *type-value*: Type 2 external route
match **internal** | **external**: Internal, external 1, external 2
external: Internal
tag *tag-value*: If no value is specified, the remote autonomous system number is used for routes from

BGP and EGP; for other protocols, the default is 0.

route-map *map-tag*: If the **route-map** keyword is not entered, all routes are redistributed; if no *map-tag* value is entered, no routes are imported.

subnets: No subnets are defined.

Command Modes

Router configuration
Address family configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Address family configuration mode was added.
12.0(22)S	Address family support under EIGRP was added in Cisco IOS Release 12.0(22)S.
12.2(15)T	Address family support under EIGRP was added in Cisco IOS Release 12.2(15)T.
12.2(18)S	Address family support under EIGRP was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Routes learned from IP routing protocols can be redistributed at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Redistributed routing information must be filtered by the **distribute-list out** router configuration command. This guideline ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

When routes are redistributed into OSPF from protocols other than OSPF or BGP, and no metric has been specified with the **metric-type** keyword and *type-value* argument, OSPF will use 20 as the default metric. When routes are redistributed into OSPF from BGP, OSPF will use 1 as the default metric. When routes are redistributed from one OSPF process to another OSPF process, Autonomous system (AS) external and not-so-stubby-area (NSSA) routes will use 20 as the default metric. When intra-area and inter-area routes are redistributed between OSPF processes, the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process. (This is the only case in which the routing table metric will be preserved when routes are redistributed into OSPF.)

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise **connected** routes.

**Note**

The **metric** value specified in the **redistribute** command supersedes the **metric** value specified using the **default-metric** command.

Default redistribution of IGP or EGP into BGP is not allowed unless the **default-information originate** router configuration command is specified.

Examples

The following example shows how OSPF routes are redistributed into a BGP domain:

```
router bgp 109
 redistribute ospf
```

The following example causes Enhanced Interior Gateway Routing Protocol (EIGRP) routes to be redistributed into an OSPF domain:

```
router ospf 110
 redistribute eigrp
```

The following example causes the specified EIGRP process routes to be redistributed into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
router ospf 109
 redistribute eigrp 108 metric 100 subnets
 redistribute rip metric 200 subnets
```

The following example configures BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
router isis
 redistribute bgp 120 metric 5 metric-type external
```

In the following example, network 172.16.0.0 will appear as an external link-state advertisement (LSA) in OSPF 1 with a cost of 100 (the cost is preserved):

```
interface ethernet 0
 ip address 172.16.0.1 255.0.0.0
 ip ospf cost 100
interface ethernet 1
 ip address 10.0.0.1 255.0.0.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 redistribute ospf 2 subnet
router ospf 2
 network 172.16.0.0 0.255.255.255 area 0
```

Related Commands	Command	Description
	address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
	address-family vpv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
	default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
	default-information originate (IS-IS)	Generates a default route into an IS-IS routing domain.
	default-information originate (OSPF)	Generates a default route into an OSPF routing domain.
	distribute-list out (IP)	Suppresses networks from being advertised in updates.
	route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
	show route-map	Displays all route maps configured or only the one specified.

refuse-message

To define and enable a line-in-use message, use the **refuse-message** command in line configuration mode. To disable the message, use the **no** form of this command.

refuse-message *d message d*

no refuse-message

Syntax Description

<i>d</i>	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the message.
<i>message</i>	Message text.

Defaults

Disabled (no line-in-use message is displayed).

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character. You cannot use the delimiting character within the text of the message.

When you define a message using this command, the Cisco IOS software performs the following steps:

1. Accepts the connection.
2. Prints the custom message.
3. Clears the connection.

Examples

In the following example, line 5 is configured with a line-in-use message, and the user is instructed to try again later:

```
line 5
refuse-message /The dial-out modem is currently in use.

Please try again later./
```

reload

To reload the operating system, use the **reload** command in privileged EXEC mode.

```
reload [/verify | /noverify] [warm [file url]] [in [hh:]mm | at hh:mm [month day | day month]]
[cancel] [text]
```

Syntax Description	
/verify	(Optional) Verifies the digital signature of the file that is going to be loaded onto the operating system.
/noverify	(Optional) Does not verify the digital signature of the file that is going to be loaded onto the operating system. Note This keyword is often issued if the file verify auto command is enabled, which automatically verifies the digital signature of all images that are copied.
warm	(Optional) Prevents the warm reboot functionality from being overridden when the router is reloaded.
warm file <i>url</i>	(Optional) Reloads the operating system with a new image whose location and name is specified by the <i>url</i> argument. The reload will be performed using the warm upgrade functionality.
in [<i>hh:</i>]<i>mm</i>	(Optional) Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.
at <i>hh:mm</i>	(Optional) Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days.
<i>month</i>	(Optional) Name of the month, represented by any number of characters in a unique string.
<i>day</i>	(Optional) Number of the day in the range from 1 to 31.
cancel	(Optional) Cancels a scheduled reload.
<i>text</i>	(Optional) Reason for the reload, 1 to 255 characters long.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.3(2)T	The warm keyword was added.
	12.2(18)S	The /verify and /noverify keywords were added.
	12.0(26)S	The /verify and /noverify keywords were integrated into Cisco IOS Release 12.0(26)S.

Release	Modification
12.3(4)T	The /verify and /noverify keywords were integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The file keyword and <i>url</i> argument were added.

Usage Guidelines

The **reload** command halts the system. If the system is set to restart on error, it reboots itself. Use the **reload** command after configuration information is entered into a file and saved to the startup configuration.

You cannot reload from a virtual terminal if the system is not set up for automatic booting. This restriction prevents the system from dropping to the ROM monitor (ROMMON) and thereby taking the system out of the remote user’s control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system prompts whether you want to proceed with the save if the CONFIG_FILE variable points to a startup configuration file that no longer exists. If you say “yes” in this situation, the system enters setup mode upon reload.

When you schedule a reload to occur at a later time, it must take place within approximately 24 days.

The **at** keyword can be used only if the system clock has been set on the router (either through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the router. To schedule reloads across several routers to occur simultaneously, the time on each router must be synchronized with NTP.

To display information about a scheduled reload, use the **show reload EXEC** command.

The /verify and /noverify Keywords

If the **/verify** keyword is specified, the integrity of the image will be verified before it is reloaded onto a router. If verification fails, the image reload will not occur. Image verification is important because it assures the user that the image is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

The **/noverify** keyword overrides any global automatic image verification that may be enabled via the **file verify auto** command.

The warm Keyword

If you issue the **reload** command after you have configured the **warm-reboot** global configuration command, a cold reboot will occur. Thus, if you wish to reload your system, but do not want to override the warm reboot functionality, you should specify the **warm** keyword with the **reload** command. The warm reboot functionality allows a Cisco IOS image to reload without ROMMON intervention. That is, read-write data is saved in RAM during a cold startup and restored during a warm reboot. Warm rebooting allows the router to reboot quicker than conventional rebooting (where control is transferred to ROMMON and back to the image) because nothing is copied from flash to RAM.

Examples

The following example shows how to immediately reloads the software on the router:

```
Router# reload
```

The following example shows how to reload the software on the router in 10 minutes:

```
Router# reload in 10
```

```
Router# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
```

```
Proceed with reload? [confirm]
Router#
```

The following example shows how to reload the software on the router at 1:00 p.m. today:

```
Router# reload at 13:00

Router# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
Router#
```

The following example shows how to reload the software on the router on April 20 at 2:00 a.m.:

```
Router# reload at 02:00 apr 20

Router# Reload scheduled for 02:00:00 PDT Sat Apr 20 1996 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
Router#
```

The following example shows how to cancel a pending reload:

```
Router# reload cancel

%Reload cancelled.
```

The following example shows how to perform a warm reboot at 4:00 today:

```
Router# reload warm at 4:00
```

The following example shows how to specify image verification via the **/verify** keyword before reloading an image onto the router:

```
Router# reload /verify

Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-mz
.....
.....Done!
Embedded Hash      MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash      MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash           MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified

Proceed with reload? [confirm]n
```

Related Commands

Command	Description
copy system:running-config nvram:startup-config	Copies any file from a source to a destination.
file verify auto	Enables automatic image verification.
show reload	Displays the reload status on the router.

rename

To rename a file in a Class C Flash file system, use the **rename** command in user EXEC or privileged EXEC mode.

rename *url1 url2*

Syntax Description

<i>url1</i>	The original path and filename.
<i>url2</i>	The new path and filename.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

In the following example, the file named Karen.1 is renamed test:

```
Router# dir

Directory of disk0:/Karen.dir/

 0 -rw-          0 Jan 21 1998 09:51:29 Karen.1
 0 -rw-          0 Jan 21 1998 09:51:29 Karen.2
 0 -rw-          0 Jan 21 1998 09:51:29 Karen.3
 0 -rw-          0 Jan 21 1998 09:51:31 Karen.4
243 -rw-        165 Jan 21 1998 09:53:17 Karen.cur

340492288 bytes total (328400896 bytes free)

Router# rename disk0:Karen.dir/Karen.1 disk0:Karen.dir/test
Router# dir

Directory of disk0:/Karen.dir/

 0 -rw-          0 Jan 21 1998 09:51:29 Karen.2
 0 -rw-          0 Jan 21 1998 09:51:29 Karen.3
 0 -rw-          0 Jan 21 1998 09:51:31 Karen.4
243 -rw-        165 Jan 21 1998 09:53:17 Karen.cur
 0 -rw-          0 Apr 24 1998 09:49:19 test

340492288 bytes total (328384512 bytes free)
```

request-data-size

To set the protocol data size in the payload of a Cisco IOS IP Service Level Agreements (SLAs) operation's request packet, use the **request-data-size** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

request-data-size *bytes*

no request-data-size

Syntax Description

<i>bytes</i>	Size of the protocol data in the payload of the request packet of the operation. Range is 0 to the maximum of the protocol.
--------------	---

Defaults

The default data size will vary depending on the type of IP SLAs operation you are configuring.

Command Modes

IP SLA Monitor Configuration

DLSw configuration (config-sla-monitor-dlsw)
 Frame Relay configuration (config-sla-monitor-frameRelay)
 ICMP echo configuration (config-sla-monitor-echo)
 ICMP path echo configuration (config-sla-monitor-pathEcho)
 ICMP path jitter configuration (config-sla-monitor-pathJitter)
 UDP echo configuration (config-sla-monitor-udp)
 UDP jitter configuration (config-sla-monitor-jitter)

RTR Configuration

DLSw configuration (config-rtr-dlsw)
 Frame Relay configuration (config-rtr-frameRelay)
 ICMP echo configuration (config-rtr-echo)
 ICMP path echo configuration (config-rtr-pathEcho)
 ICMP path jitter configuration (config-rtr-pathJitter)
 UDP echo configuration (config-rtr-udp)
 UDP jitter configuration (config-rtr-jitter)



Note

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the "Usage Guidelines" section for more information.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines**IP SLAs Operation Configuration Dependence on Cisco IOS Release**

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 59](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **request-data-size** command varies depending on the Cisco IOS release you are running (see [Table 59](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP echo operation type is configured, you would enter the **request-data-size** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

Table 59 *Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release*

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.3(14)T and 12.4	ip sla monitor	IP SLA monitor configuration
All other Cisco IOS releases	rtr	RTR configuration

Examples

The following examples show how to set the request packet size to 40 bytes for IP SLAs ICMP echo operation 3. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 59](#)).

IP SLA Monitor Configuration

```
ip sla monitor 3
  type echo protocol ipIcmpEcho 172.16.1.175
  request-data-size 40
!
ip sla monitor schedule 3 life forever start-time now
```

RTR Configuration

```
rtr 3
  type echo protocol ipIcmpEcho 172.16.1.175
  request-data-size 40
!
rtr schedule 3 life forever start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.

resource policy

To enter ERM configuration mode and configure an ERM policy, use the **resource policy** command in global configuration mode. To disable this function, use the **no** form of this command.

resource policy

no resource policy

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines This command enters into ERM configuration mode.

Examples The following example shows how to configure an ERM policy.

```
Router(config)# resource policy
```

Related Commands	Command	Description
	policy (ERM)	Configures an ERM resource policy.
	show resource all	Displays all the resource details.
	show resource all	Displays resource details for all RUs.
	show resource database	Displays the resource database details.
	show resource owner	Displays the RO details.
	show resource relationship	Displays the resource relationship details.
	slot (ERM policy)	Configures line cards.
	system (ERM policy)	Configures system level ROs.

response-data-size

To set the protocol data size in the payload of an Service Assurance Agent (SAA) operation's response packet, use the **response-data-size** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

response-data-size *bytes*

no response-data-size

Syntax Description	<i>bytes</i>	Size of the protocol data in the payload in the operation's response packet. For "appl" protocols, the default is 0 bytes. For all others, the default is the same value as the request-data-size .
---------------------------	--------------	--

Defaults	0 bytes
-----------------	---------

Command Modes	SAA RTR configuration
----------------------	-----------------------

Command History	Release	Modification
	11.2	This command was introduced.
	12.3(14)T	The Service Assurance Agent (SAA) feature is replaced by the Cisco IOS IP Service Level Agreements (IP SLAs) feature.

Usage Guidelines The **response-data-size** command is only applicable for the following operations:

- type echo protocol snaLU0EchoAppl
- type echo protocol snaLU2EchoAppl
- type pathEcho protocol snaLU0EchoAppl
- type pathEcho protocol snaLU2EchoAppl

Note that these protocols are defined with the **type** command that end in "appl" (for example, **snalu0echoappl**). When the protocol ends in "appl," the response data size is 12 bytes smaller than normal payload size.

Examples The following example configures the response packet size of snaLU0 Echo operation 3 to 1440 bytes:

```
Router(config)# rtr 3
Router(config-rtr)# type echo protocol snalu0echoappl cwbc0a
Router(config-rtr)# response-data-size 1440
```

Related Commands

Command	Description
request-data-size	Sets the protocol data size in the payload of the SAA operation's request packet.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

retain

To configure the retention interval for bulk statistics files, use the **retain** command in Bulk Statistics Transfer configuration mode. To remove a previously configured retention interval from the configuration, use the **no** form of this command.

retain *minutes*

no retain *minutes*

Syntax Description

<i>minutes</i>	Length of time, in minutes, that the local bulk statistics file should be kept in system memory (the retention interval). The valid range is 0 to 20000. The default is 0.
----------------	--

Defaults

The default bulk statistics file retention interval is 0.

Command Modes

Bulk Statistics Transfer configuration (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

This command specifies how long the bulk statistics file should be kept in system memory, in minutes, after the completion of the collection interval and a transmission attempt is made. The default value of zero (**0**) indicates that the file will be deleted immediately from local memory after a successful transfer.

If the **retry** command is used, you should configure a retention interval larger than 0. The interval between retries is the retention interval divided by the retry number. For example, if **retain 10** and **retry 2** are configured, retries will be attempted once every 5 minutes. Therefore, if the **retain** command is not configured (retain default is 0), no retries will be attempted.

Examples

In the following example, the bulk statistics transfer retention interval is set to 10 minutes:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswr@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
retry	Configures the number of retries that should be attempted for sending bulk statistics files.
snmp mib bulkstat transfer	Identifies the transfer configuration with a name and enters Bulk Statistics Transfer configuration mode.

retry (bulkstat)

To configure the number of retries that should be attempted for a bulk statistics file transfer, use the **retry** command in Bulk Statistics Transfer configuration mode. To return the number of bulk statistics retries to the default, use the **no** form of this command.

retry *number*

no *retry number*

Syntax Description	<i>number</i>	Specifies the number of transmission retries. The valid range is 0 to 100. The default is 0 (no retry attempts).
---------------------------	---------------	--

Defaults	No retry attempts.
-----------------	--------------------

Command Modes	Bulk Statistics Transfer configuration (config-bulk-tr)
----------------------	---

Command History	Release	Modification
	12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.	
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.	

Usage Guidelines

If an attempt to send the bulk statistics file fails, the system can be configured to attempt to send the file again using the **retry** command. One retry includes an attempt first to the primary destination then, if the transmission fails, to the secondary location; for example, if the retry value is 1, an attempt will be made first to the primary URL, then to the secondary URL, then to the primary URL again, then to the secondary URL again.

If the **retry** command is used, you should also use the **retain** command to configure a retention interval larger than 0. The interval between retries is the retention interval divided by the retry number. For example, if **retain 10** and **retry 2** are configured, retries will be attempted once every 5 minutes. Therefore, if the **retain** command is not configured (or the **retain 0** command is used) no retries will be attempted.

Examples

In the following example, the number of retries for the bulk statistics transfer is set to 2:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswr@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands	Command	Description
	retain	Configures the retention interval in local system memory (NVRAM) for bulk statistics files.
	snmp mib bulkstat transfer	Identifies the transfer configuration with a name and enters Bulk Statistics Transfer configuration mode.

rmdir

To remove an existing directory in a Class C Flash file system, use the **rmdir** command in user EXEC or privileged EXEC mode.

rmdir *directory*

Syntax Description

directory Directory to delete.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

The following example deletes the directory named newdir:

```
Router# dir
Directory of flash:
  2  drwx          0  Mar 13 1993 13:16:21  newdir

8128000 bytes total (8126976 bytes free)
Router# rmdir newdir
Rmdir file name [newdir]?
Delete flash:newdir? [confirm]
Removed dir flash:newdir
Router# dir
Directory of flash:

No files in directory

8128000 bytes total (8126976 bytes free)
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkdir	Creates a new directory in a Class C Flash file system.

rmon

To enable Remote Monitoring (RMON) on an Ethernet interface, use the **rmon** command in interface configuration mode. To disable RMON on the interface, use the **no** form of this command.

```
rmon { native | promiscuous }
```

```
no rmon
```

Syntax Description

native	Enables RMON on the Ethernet interface. In native mode, the router processes only packets destined for this interface.
promiscuous	Enables RMON on the Ethernet interface. In promiscuous mode, the router examines every packet.

Defaults

RMON is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command enables RMON on Ethernet interfaces. A generic RMON console application is recommended in order to use the RMON network management capabilities. SNMP must also be configured. RMON provides visibility of individual nodal activity and allows you to monitor all nodes and their interaction on a LAN segment. When the **rmon** command is issued, the router automatically installs an Ethernet statistics study for the associated interface.



Note

RMON can be very data and processor intensive. Users should measure usage effects to ensure that router performance is not degraded and to minimize excessive management traffic overhead. Native mode is less intensive than promiscuous mode.

All Cisco IOS software feature sets support RMON alarm and event groups. Additional RMON groups are supported in certain feature sets. Refer to the Release Notes for feature set descriptions. As a security precaution, support for the packet capture group allows capture of packet header information only; data payloads are not captured.

The RMON MIB is described in RFC 1757.

Examples

The following example enables RMON on Ethernet interface 0 and allows the router to examine only packets destined for the interface:

```
interface ethernet 0
 rmon native
```

Related Commands

Command	Description
rmon alarm	Sets an alarm on any MIB object.
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
rmon queuesize	Changes the size of the queue that holds packets for analysis by the RMON process.
show rmon	Displays the current RMON agent status on the router.

rmon alarm

To set an alarm on any MIB object, use the **rmon alarm** command in global configuration mode. To disable the alarm, use the **no** form of this command.

```
rmon alarm number variable interval {delta | absolute} rising-threshold value [event-number]
falling-threshold value [event-number] [owner string]
```

```
no rmon alarm number
```

Syntax Description		
<i>number</i>		Alarm number, which is identical to the <i>alarmIndex</i> in the alarmTable in the Remote Monitoring (RMON) MIB.
<i>variable</i>		MIB object to monitor, which translates into the <i>alarmVariable</i> used in the alarmTable of the RMON MIB.
<i>interval</i>		Time in seconds the alarm monitors the MIB variable, which is identical to the <i>alarmInterval</i> used in the alarmTable of the RMON MIB.
delta		Tests the change between MIB variables, which affects the <i>alarmSampleType</i> in the alarmTable of the RMON MIB.
absolute		Tests each MIB variable directly, which affects the <i>alarmSampleType</i> in the alarmTable of the RMON MIB.
rising-threshold <i>value</i>		Value at which the alarm is triggered.
<i>event-number</i>		(Optional) Event number to trigger when the rising or falling threshold exceeds its limit. This value is identical to the <i>alarmRisingEventIndex</i> or the <i>alarmFallingEventIndex</i> in the alarmTable of the RMON MIB.
falling-threshold <i>value</i>		Value at which the alarm is reset.
owner <i>string</i>		(Optional) Specifies an owner for the alarm, which is identical to the <i>alarmOwner</i> in the alarmTable of the RMON MIB.

Defaults No alarms configured

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines The MIB object must be specified as a dotted decimal value after the entry sequence (for example, ifEntry.10.1). You cannot specify the variable name and the instance (for example, ifInOctets.1) or the entire dotted decimal notation. The variable must be of the form *entry.integer.instance*.

To disable the RMON alarms, you must use the **no** form of the command on each configured alarm. For example, enter **no rmon alarm 1**, where the 1 identifies which alarm is to be removed.

See RFC 1757 for more information about the RMON alarm group.

Examples

The following example configures an RMON alarm using the **rmon alarm** command:

```
rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0
owner jjohnson
```

This example configures RMON alarm number 10. The alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled, and checks the change in the variable's rise or fall. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the **rmon event** command. Possible events include a log entry or a SNMP trap. If the *ifEntry.20.1* value changes by 0 (falling-threshold 0), the alarm is reset and can be triggered again.

Related Commands

Command	Description
rmon	Enables Remote Network Monitoring (RMON) on an Ethernet interface
rmon event	Adds or removes an event in the RMON event table that is associated with an RMON event number.
show rmon	Displays the current RMON agent status on the router.

rmon capture-userdata

To disable the packet zeroing feature that initializes the user payload portion of each Remote Monitoring (RMON) MIB packet, use the **rmon capture-userdata** command in global configuration mode. To enable packet zeroing, use the **no** form of this command.

rmon capture-userdata

no rmon capture-userdata

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Global configuration

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

Usage Guidelines Use the **show rmon matrix** command to display RMON statistics.

Examples The following command disables the packet zeroing feature:

```
Router(config)# rmon capture-userdata
```

Related Commands	Command	Description
	rmon collection matrix	Enables a RMON MIB matrix group of statistics on an interface.

rmon collection history

To enable Remote Monitoring (RMON) history gathering on an interface, use the **rmon collection history** command in interface configuration mode. To disable the history gathering on an interface, use the **no** form of this command.

```
rmon collection history controlEntry integer [owner ownername] [buckets bucket-number]
[interval seconds]
```

```
no rmon collection history controlEntry integer [owner ownername] [buckets bucket-number]
[interval seconds]
```

Syntax Description

controlEntry	Specifies the RMON group of statistics using a value.
<i>integer</i>	A value from 1 to 65535 that identifies the RMON group of statistics and matches the index value returned for Simple Network Management Protocol (SNMP) requests.
owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
<i>ownername</i>	(Optional) Records the name of the owner of the RMON group of statistics.
buckets <i>bucket-number</i>	(Optional) Specifies the maximum number of buckets desired for the RMON collection history group of statistics.
interval <i>seconds</i>	(Optional) Specifies the number of seconds history should be gathered in a single bucket. When the interval ends, history is collected into a new bucket.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use the **show rmon capture** and **show rmon matrix** commands to display RMON statistics.

Examples

The following command enables an RMON MIB collection history group of statistics with an ID number of 20 and an owner as john:

```
Router(config-if)# rmon collection history controlEntry 20 owner john
```

Related Commands

Command	Description
show rmon capture	Displays the contents of the RMON history table.
show rmon matrix	Displays the RMON MIB matrix table.

rmon collection host

To enable a Remote Monitoring (RMON) MIB host collection group of statistics on the interface, use the **rmon collection host** command in interface configuration mode. To remove the specified RMON host collection, use the **no** form of the command.

rmon collection host controlEntry *integer* [**owner** *ownername*]

no rmon collection host controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry <i>integer</i>	Specifies an identification number for the RMON group of statistics. The integer can be any number in the range from 1 to 65535.
owner <i>ownername</i>	(Optional) Specifies the name of the owner of the RMON group of statistics.

Defaults

No RMON host collection is specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use the **show rmon hosts** and **show rmon matrix** commands to display RMON statistics.

Examples

The following command enables an RMON collection host group of statistics with an ID number of 20, and specifies john as the owner:

```
Router(config-if)# rmon collection host controlEntry 20 owner john
```

Related Commands

Command	Description
show rmon hosts	Displays the RMON MIB hosts table.
show rmon matrix	Displays the RMON MIB matrix table.

rmon collection matrix

To enable a Remote Monitoring (RMON) MIB matrix group of statistics on an interface, use the **rmon collection matrix** command in interface configuration mode. To remove a specified RMON matrix group of statistics, use the **no** form of the command.

rmon collection matrix controlEntry *integer* [**owner** *ownername*]

no rmon collection matrix controlEntry *integer* [**owner** *ownername*]

Syntax Description	controlEntry <i>integer</i>	Specifies an identification number for the RMON matrix group of statistics. The integer can be any number in the range from 1 to 65535.
	owner <i>ownername</i>	(Optional) Specifies the name of the owner of the RMON matrix group of statistics.

Defaults No RMON matrix group of statistics is specified.

Command Modes Interface configuration

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

Usage Guidelines Use the **show rmon matrix** command to display RMON statistics.

Examples The following command enables the RMON collection matrix group of statistics with an ID number of 25, and specifies john as the owner:

```
Router(config-if)# rmon collection matrix controlEntry 25 owner john
```

Related Commands	Command	Description
	show rmon matrix	Displays the RMON MIB matrix table.

rmon collection rmon1

To enable all possible autoconfigurable Remote Monitoring (RMON) MIB statistic collections on the interface, use the **rmon collection rmon1** command in interface configuration mode. To disable these statistic collections on the interface, use the **no** form of the command.

rmon collection rmon1 controlEntry *integer* [**owner** *ownername*]

no rmon collection rmon1 controlEntry *integer* [**owner** *ownername*]

Syntax Description

controlEntry <i>integer</i>	Specifies an identification number for the RMON group of statistics. The integer can be any number in the range from 1 to 65535.
owner <i>ownername</i>	(Optional) Specifies the name of the owner of the RMON group of statistics.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use the **show rmon matrix** command to display RMON statistics.

Examples

The following command enables the RMON collection rmon1 group of statistics with an ID number of 30, and specifies “john” as the owner:

```
Router(config-if)# rmon collection rmon1 controlEntry 30 owner john
```

Related Commands

Command	Description
show rmon matrix	Displays the RMON MIB matrix table.

rmon event

To add or remove an event in the RMON event table that is associated with an RMON event number, use the **rmon event** command in global configuration mode. To disable RMON on the interface, use the **no** form of this command.

```
rmon event number [log] [trap community] [description string] [owner string]
```

```
no rmon event number
```

Syntax Description		
<i>number</i>		Assigned event number, which is identical to the <i>eventIndex</i> in the eventTable in the RMON MIB.
log		(Optional) Generates an RMON log entry when the event is triggered and sets the <i>eventType</i> in the RMON MIB to <i>log</i> or <i>log-and-trap</i> .
trap <i>community</i>		(Optional) SNMP community string used for this trap. Configures the setting of the <i>eventType</i> in the RMON MIB for this row as either <i>snmp-trap</i> or <i>log-and-trap</i> . This value is identical to the <i>eventCommunityValue</i> in the eventTable in the RMON MIB.
description <i>string</i>		(Optional) Specifies a description of the event, which is identical to the event description in the eventTable of the RMON MIB.
owner <i>string</i>		(Optional) Owner of this event, which is identical to the <i>eventOwner</i> in the eventTable of the RMON MIB.

Defaults No events are configured.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines This command applies only to the Cisco 2500 series and Cisco AS5200 series. See RFC 1757 for more information about the RMON MIB.

Examples The following example enables the **rmon event** command:

```
rmon event 1 log trap eventtrap description "High ifOutErrors" owner sdurham
```

This example configuration creates RMON event number 1, which is defined as High ifOutErrors, and generates a log entry when the event is triggered by an alarm. The user sdurham owns the row that is created in the event table by this command. This configuration also generates a Simple Network Management Protocol (SNMP) trap when the event is triggered.

Related Commands

Command	Description
rmon	Enables RMON on an Ethernet interface.
show rmon	Displays the current RMON agent status on the router.

rmon queue-size

To change the size of the queue that holds packets for analysis by the Remote Monitoring (RMON) process, use the **rmon queue-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

rmon queue-size *size*

no rmon queue-size

Syntax Description	<i>size</i>	Number of packets allowed in the queue awaiting RMON analysis. Default queue size is 64 packets.
---------------------------	-------------	--

Defaults	64 packets
-----------------	------------

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

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	<p>This command applies to the RMON function, which is available on Ethernet interfaces of Cisco 2500 series and Cisco AS5200 series routers only.</p> <p>You might want to increase the queue size if the RMON function indicates it is dropping packets. You can determine this from the output of the show rmon command or from the etherStatsDropEvents object in the etherStats table. A feasible maximum queue size depends on the amount of memory available in the router and the configuration of the buffer pool.</p>
-------------------------	--

Examples	The following example configures the RMON queue size to be 128 packets:
-----------------	---

```
Router(config)# rmon queue-size 128
```

Related Commands	Command	Description
	show rmon	Displays the current RMON agent status on the router.

rommon-pref

To select a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR router or Cisco 7301 router when you are in ROMmon, use the **rommon-pref** command in ROMmon mode.

rommon-pref [readonly | upgrade]

Syntax Description

readonly	Selects the ReadOnly ROMmon image to be booted on the next reload.
upgrade	Selects the Upgrade, second ROMmon image to be booted on the next reload.

Defaults

No default behavior or values

Command Modes

ROMmon

Command History

Release	Modification
12.0(28)S	This command was introduced on the Cisco 7200 VXR router. It was introduced in ROMmon version 12.3(4r)T1 for the Cisco 7200 VXR router.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router. It was introduced in ROMmon version 12.3(4r)T2 for the Cisco 7301 router.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.

Usage Guidelines

You might select the ReadOnly ROMmon image to be booted on the next reload because the Upgrade image has features or side effects you do not like.

When you are in ROMmon, there is no descriptive output to inform you whether the ReadOnly ROMmon image was reloaded. To confirm the reload, use the **showmon** command after entering the **rommon-pref readonly** command.

Use this command when you are in ROMmon mode. Use the **upgrade rom-monitor preference** command when you are in Cisco IOS.

Examples

The following example, applicable to both the Cisco 7200 VXR and Cisco 7301 routers, shows how to select the ReadOnly ROMmon image to be booted on the next reload of the router when you are already in ROMmon mode:

```
rommon 2 > rommon-pref readonly
```

Related Commands

Command	Description
showmon	Shows both the ReadOnly and the Upgrade ROMmon image versions when you are in ROMmon mode, as well as which ROMmon image is running.

rsh

To execute a command remotely on a remote shell protocol (rsh) host, use the **rsh** command in privileged EXEC mode.

```
rsh {ip-address | host} [/user username] remote-command
```

Syntax Description

<i>ip-address</i>	IP address of the remote host on which to execute the rsh command. Either the IP address or the host name is required.
<i>host</i>	Name of the remote host on which to execute the command. Either the host name or the IP address is required.
/user <i>username</i>	(Optional) Remote username.
<i>remote-command</i>	Command to be executed remotely.

Defaults

If you do not specify the **/user** *username* keyword and argument, the Cisco IOS software sends a default remote username. As the default value of the remote username, the software sends the username associated with the current tty process, if that name is valid. For example, if the user is connected to the router through Telnet and the user was authenticated through the **username** command, then the software sends that username as the remote username. If the tty username is invalid, the software uses the host name as the both the remote and local usernames.



Note

For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are sometimes called tty devices (tty stands for teletype, the original UNIX terminal).

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **rsh** command to execute commands remotely. The host on which you remotely execute the command must support the rsh protocol, and the *.rhosts* files on the rsh host must include an entry that permits you to remotely execute commands on that host.

For security reasons, the software does not default to a remote login if no command is specified, as does UNIX. Instead, the router provides Telnet and connect services that you can use rather than rsh.

Examples

The following command specifies that the user named sharon attempts to remotely execute the UNIX **ls** command with the **-a** argument on the remote host named *mysys.cisco.com*. The command output resulting from the remote execution follows the command example:

```
Router1# rsh mysys.cisco.com /user sharon ls -a
```

```
.  
.br/>.br/>.alias  
.cshrc  
.emacs  
.exrc  
.history  
.login  
.mailrc  
.newsrc  
.oldnewsrc  
.rhosts  
.twmrc  
.xsession  
jazz
```

rtr



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr** command is replaced by the **ip sla monitor** command. See the **ip sla monitor** command for more information.

To begin configuration for a Cisco IOS IP Service Level Agreements (IP SLAs) operation and enter RTR configuration mode, use the **rtr** command in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the **no** form of this command.

rtr *operation-number*

no rtr *operation-number*

Syntax Description

<i>operation-number</i>	Operation number used for the identification of the IP SLAs operation you wish to configure.
-------------------------	--

Defaults

No IP SLAs operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(11)T	The maximum number of operations was increased from 500 to 2000 (SAA Engine II).
12.3(14)T	This command was replaced by the ip sla monitor command.

Usage Guidelines

The **rtr** command is used to configure Cisco IOS IP Service Level Agreements (IP SLAs) operations. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, you will enter the RTR configuration mode.

IP SLAs allows a maximum of 2000 operations.

Debugging is supported only on the first 32 operation numbers.

After you configure a operation, you must schedule the operation. For information on scheduling a operation, refer to the **rtr schedule** and **rtr group schedule** global configuration commands. You can also optionally set reaction triggers for the operation. For information on reaction triggers, refer to the **rtr reaction-configuration** and **rtr reaction-trigger** global configuration commands.



Note

After you schedule an operation, you cannot modify the configuration of the operation. To modify the configuration of the operation after it is scheduled, you must first delete the IP SLAs operation (using the **no rtr** command) and then reconfigure the operation with the new operation parameters.

To display the current configuration settings of the operation, use the **show rtr configuration EXEC** command.

Examples

In the following example, operation 1 is configured to perform end-to-end IP SLAs operations using an SNA LU Type 0 connection with the host name cwbc0a. Only the **type** RTR configuration command is required; all others are optional.

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol snalu0echoappl cwbc0a
Router(config-rtr)# request-data-size 40
Router(config-rtr)# response-data-size 1440
Router(config-rtr)# exit
```



Note

If operation 1 already existed and it has not been scheduled, you are placed into RTR configuration mode. If the operation already exists and has been scheduled, this command will fail.

Related Commands

Command	Description
rtr group schedule	Configures the group scheduling parameters for multiple IP SLAs operations.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action type options are defined with the ip sla monitor reaction-configuration command.
rtr schedule	Configures the scheduling parameters for a single IP SLAs operation.
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

rtr group schedule



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr group schedule** command is replaced by the **ip sla monitor group schedule** command. See the **ip sla monitor group schedule** command for more information.

To perform group scheduling for Cisco IOS IP Service Level Agreements (IP SLAs) operations, use the **rtr group schedule** command in global configuration mode. To stop the operation and place it in the default state of normal scheduling, use the **no** form of this command.

```
rtr group schedule group-operation-number operation-id-numbers schedule-period
schedule-period-range [ageout seconds] [frequency group-operation-frequency] [life {forever
| seconds}] [start-time {hh:mm[:ss] [month day | day month] | pending | now |
after hh:mm:ss}]
```

```
no rtr group schedule
```

Syntax Description

<i>group-operation-number</i>	Group configuration or group schedule number of the IP SLAs operation to be scheduled. <ul style="list-style-type: none"> Valid values range from 0 to 65535.
<i>operation-id-numbers</i>	The list of IP SLAs operation ID numbers in the scheduled operation group. Indicate ranges of operation ID numbers with a hyphen. Individual ID numbers and ranges of ID numbers are delimited by a comma. For example, enter a list of operation ID numbers in any of the following ways: <ul style="list-style-type: none"> 2, 3, 4, 9, 20 10-20, 30-35, 60-70 2, 3, 4, 90-100, 105-115 The <i>operation-id-numbers</i> argument can include a maximum of 125 characters.
schedule-period <i>schedule-period-range</i>	Time (in seconds) for which the IP SLAs operation group is scheduled. <ul style="list-style-type: none"> Valid values are from 1 to 604800 seconds.
ageout <i>seconds</i>	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out).
frequency <i>group-operation-frequency</i>	(Optional) Specifies the number of seconds after which each IP SLAs operation is restarted. If this keyword and argument are specified, the frequency of all operations belonging to the group will be overridden and set to the specified frequency. <p>Note If this keyword and argument are not specified, the frequency for each operation is set to the value specified for the schedule period.</p> <ul style="list-style-type: none"> Valid values are from 1 to 604800 seconds.

life forever	(Optional) Schedules the operation to run indefinitely.
life seconds	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	(Optional) Time when the operation starts collecting information. If the start-time is not specified, no information is collected until the start-time is configured or a trigger occurs that performs a start-time now .
<i>hh:mm[:ss]</i>	(Optional) Specifies an absolute start time using hours, minutes, and (optionally) seconds. Use the 24-hour clock notation. For example, start-time 01:02 means “start at 1:02 a.m.,” and start-time 13:01:30 means “start at 1:01 p.m. and 30 seconds.” The current day is implied unless you specify a <i>month</i> and <i>day</i> .
<i>month</i>	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified as well. You can specify the month by using either the full English name or the first three letters of the month.
<i>day</i>	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified as well.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after hh:mm:ss	(Optional) Indicates that the operation should start <i>hh</i> hours, <i>mm</i> minutes, and <i>ss</i> seconds after this command was entered.

Defaults

The operation is placed in a **pending** state (that is, the operation is enabled but is not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor group schedule command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

Though IP SLAs multiple operations scheduling functionality helps in scheduling thousands of operations, you should be cautious while specifying the number of operations, the schedule period, and the operation group frequency to avoid CPU hogging.

For example, consider a scenario where you are scheduling 1 to 780 operations at a schedule period of 60 seconds, the command would be as follows:

```
rtr group schedule 2 1-780 schedule-period 60 start-now
```

IP SLAs calculates how many operations it should start in each 1-second interval by dividing the number of operations by the schedule period (780 operations divided by 60 seconds, which is 13 operations per second). Operations 1 to 13 in operation group 2 start after 0 seconds, operations 14 to 26 start after 1 second, operations 27 to 40 start after 2 seconds, and the iteration continues until operations 768 to 780 start after 59 seconds. This high value of operations starting at every 1-second interval (especially for jitter operations) can load the CPU to very high values.

The maximum recommended value of operations per second is 6 or 7. This is approximately 350 to 400 operations per minute. This value of 6 or 7 operation per second will be the maximum that does not have any major performance (CPU) impact. However, this value varies from platform to platform. The above value is verified and tested on a Cisco 2600 router.

**Note**

No warning messages will be displayed if IP SLAs multiple operations scheduling leads to a high number of operations starting per second.

When you reboot the router, the IP SLAs multiple operations scheduling functionality schedules the operations in the same order as was done before the reboot. For example, assume the following operation had been scheduled:

rtr group schedule 2 1-20 schedule-period 40 start-time now

Over a range of 40 seconds, 20 operations have to be started (that is, one operation every 2 seconds). After the system reboot, operation 1 will start at t seconds and operation 2 starts at $t+2$ seconds, operation 3 starts at $t+4$ seconds, and so on.

The IP SLAs multiple operations scheduling functionality schedules the maximum number of operations possible without aborting. However, this functionality skips those IP SLAs operations that are already running or those that are not configured and hence do not exist. The total number of operations will be calculated based on the number of operations specified in the command, irrespective of the number of operations that are missing or already running. The IP SLAs multiple operations scheduling functionality displays a message showing the number of active and missing operations. However, these messages are displayed only if you schedule operations that are not configured or are already running.

Examples

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1:

```
Router(config)# rtr group schedule 1 3, 4, 6-10
```

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1, with a schedule period of 20 seconds:

```
Router(config)# rtr group schedule 1 3, 4, 6-10 schedule-period 20
```

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1, with a schedule period of 20 seconds with start time as now:

```
Router(config)# rtr group schedule 1 3, 4, 6-10 schedule-period 20 start-time now
```

Related Commands

Command	Description
rtr schedule	Enters rtr scheduling mode.
show rtr collection-statistics	Displays the collection details of the IP SLAs operation.

Command	Description
show rtr configuration	Displays the configuration details of the IP SLAs operation.
show rtr operation	Displays the operation details of the IP SLAs operation.

rtr key-chain



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr key-chain** command is replaced by the **ip sla monitor key-chain** command. See the **ip sla monitor key-chain** command for more information.

To enable Cisco IOS IP Service Level Agreements (IP SLAs) control message authentication and specify an MD5 key chain, use the **rtr key-chain** command in global configuration mode. To remove control message authentication, use the **no** form of this command.

rtr key-chain *name*

no rtr key-chain

Syntax Description

<i>name</i>	Name of MD5 key chain.
-------------	------------------------

Defaults

Control message authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor key-chain command.

Usage Guidelines

The authentication configuration on the IP SLAs collector and IP SLAs Responder must be the same. Both sides must configure the same key chain or both sides must not use authentication.

Examples

In the following example, the IP SLAs control message uses MD5 authentication, and the key chain name is CSAA:

```
Router(config)# rtr key-chain csaa
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.

rtr logging traps



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr logging traps** command is replaced by the **ip sla monitor logging traps** command. See the **ip sla monitor logging traps** command for more information.

To enable the generation of system logging SNMP notifications (traps) specific to IP SLAs thresholds, use the **rtr logging traps** command in global configuration mode. To disable IP SLAs system logging SNMP traps, use the **no** form of this command.

rtr logging traps

no rtr logging traps

Syntax Description

No arguments or keywords.

Defaults

Disabled (IP SLAs system logging traps are not generated).

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor logging traps command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

SNMP notifications (traps) for IP SLAs can be configured as a triggered action, to be sent when monitored values exceed an upper threshold or fall below a lower threshold, or when a set of defined conditions are met. For example, an SNMP trap can be triggered by 5 consecutive timeouts during an IP SLAs operation. The sending of SNMP traps is one of the options for triggered actions that can be configured for IP SLAs violations. The monitored values (also called monitored elements), the threshold type, and the triggered action are configured using the **rtr reaction-configuration** global configuration mode command.

SNMP traps for IP SLAs are handled through the system logging (syslog) process. This means that system logging messages for IP SLAs violations are generated when the specified conditions are met, then sent as SNMP traps using the CISCO-SYSLOG-MIB. The **rtr logging traps** command is used to enable the generation of these IP SLAs specific traps. The generation of IP SLAs specific logging messages is dependant on the configuration of the standard set of logging commands (for example, **logging on**). IP SLAs logging messages are generated as level 7 (debugging) messages.

Examples

The following example shows the configuration of IP SLAs traps to be triggered for round-trip-time (rtt) violations and VoIP mean opinion score (MOS) violations, and the necessary SNMP configuration for enabling these SNMP logging traps:

```
Router(config)# rtr 1
Router(config-rtr)# type jitter dest-ipaddr 209.165.200.225 dest-port 9234
Router(config-rtr)# exit
Router(config)# rtr schedule 1 start now life forever
Router(config)# rtr reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly
Router(config)# rtr reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly

Router(config)# rtr logging traps
Router(config)#
Router(config)# snmp-server community public RW
Router(config)# snmp-server enable traps syslog
Router(config)# snmp-server host 209.165.202.129 version 3 public syslog
Router(config)# logging trap debugging
Router(config)# logging host 209.165.202.129
```

Related Commands

Command	Description
logging on	Controls (enables or disables) system message logging globally.
rtr reation-configuration	Configures reactions, such as the generation of syslog traps, based on monitored IP SLAs elements.

rtr low-memory



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr low-memory** command is replaced by the **ip sla monitor low-memory** command. See the **ip sla monitor low-memory** command for more information.

To specify how much unused memory must be available to allow Cisco IOS IP Service Level Agreements (IP SLAs) configuration, use the **rtr low-memory** command in global configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

rtr low-memory *value*

no rtr low-memory

Syntax Description

<i>value</i>	Specifies amount of memory, in bytes, that must be available to configure IP SLAs. The range is from 0 to the maximum amount of free memory bytes available.
--------------	--

Defaults

The default *value* is 25 percent of the memory available on the system.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor low-memory command.

Usage Guidelines

The **rtr low-memory** command allows the user to specify the amount of memory that IP SLAs can use. If the amount of available free memory falls below the value specified in the **rtr low-memory** command, then you will not be allowed to configure new IP SLAs operations. If this command is not used, the default low-memory value is 25 percent. This means that if 75 percent of system memory has been utilized you will not be able to configure any IP SLAs characteristics.

The value of the **rtr low-memory** command should not exceed the amount of free memory available on the system. To determine the amount of free memory available on the system, use the **show memory EXEC** command.

Examples

In the following example, the router is configured so that no less than 2 MB of memory will be free for IP SLAs configuration:

```
Router(config)# rtr low-memory 2000000
```

Related Commands

Command	Description
rtr	Specifies an identification number for an IP SLAs operation and enters RTR configuration mode.
show memory	Displays statistics about memory, including memory-free pool statistics.

rtr reaction-configuration



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr reaction-configuration** command is replaced by the **ip sla monitor reaction-configuration** command. See the **ip sla monitor reaction-configuration** command for more information.

To configure certain actions to occur based on events under the control of Cisco IOS IP Service Level Agreements (IP SLAs), use the **rtr reaction-configuration** command in global configuration mode. To clear the reaction configuration for a specified IP SLAs operation, use the **no** form of this command.

```
rtr reaction-configuration operation-number [react monitored-element] [threshold-type { never
| immediate | consecutive [consecutive-occurrences ] | xofy [ x-value y-value ] | average
[number-of-measurements ] } ] [threshold-value upper-threshold lower-threshold]
[action-type { none | trapOnly | triggerOnly | trapAndTrigger } ]
```

```
no rtr reaction-configuration operation-number
```

Syntax Description

<i>operation-number</i>	Number of the IP SLAs operation to configure for which reactions are to be configured.
react <i>monitored-element</i>	<p>Specifies the element to be monitored for violations. Keyword options for the <i>monitored-element</i> are:</p> <p>connectionLoss—Specifies that a reaction should occur if there is a connection loss for the monitored operation. Thresholds do not apply to this monitored element.</p> <p>jitterAvg—Specifies that a reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold.</p> <p>jitterDSAvg—Specifies that a reaction should occur if the average destination-to-source (DS) jitter value violates the upper threshold or lower threshold.</p> <p>jitterSDAvg—Specifies that a reaction should occur if the average source-to-destination (SD) jitter value violates the upper threshold or lower threshold.</p> <p>mos—Specifies that a reaction should occur if the mean opinion score (MOS) value violates the upper threshold or lower threshold.</p>

react <i>monitored-element</i> (continued)	<p>PacketLossDS—Specifies that a reaction should occur if the destination-to-source packet loss value violates the upper threshold or lower threshold.</p> <p>PacketLossSD—Specifies that a reaction should occur if the source-to-destination packet loss value violates the upper threshold or lower threshold.</p> <p>rtt—Specifies that a reaction should occur if the mean opinion score (MOS) value violates the upper threshold or lower threshold.</p> <p>timeout—Specifies that a reaction should occur if there is a timeout for the monitored operation. Thresholds do not apply to this monitored element.</p> <p>verifyError—Specifies that a reaction should occur if there is an error verification violation. Thresholds do not apply to this monitored element.</p>
threshold-type never	Do not calculate threshold violations. This is the default threshold-type.
threshold-type immediate	When the reaction conditions (such as threshold violations) are met for the monitored element, immediately perform the action defined by action-type .
threshold-type consecutive [<i>occurrences</i>]	<p>When the reaction conditions (such as threshold violations) are met for the monitored element five times in a row, perform the action defined by action-type. The optional <i>occurrences</i> argument can be used to change the number of consecutive occurrences from the default of 5. The valid range is from 1 to 16.</p> <p>The <i>occurrences</i> value will appear in the output of the show rtr reaction-configuration command as the “Threshold Count:” value.</p>
threshold-type xofy [<i>x-value y-value</i>]	<p>When the reaction conditions (such as threshold violations) are met for the monitored element after some number (x) of violations within some other number (y) of measurements (“x of y”), perform the action defined by action-type. The default is 5 for both <i>x-value</i> and <i>y-value</i> (xofy 5 5). The valid range for each value is from 1 to 16.</p> <p>The <i>x-value</i> value will appear in the output of the show rtr reaction-configuration command as the “Threshold Count:” value, and the <i>y-value</i> will appear as the “Threshold Count2:” value.</p>
threshold-type average [<i>number-of-measurements</i>]	<p>When the average of the last five values for the monitored element exceeds the upper threshold or when the average of the last five values for the monitored element drops below the lower threshold, perform the action defined by action-type. For example, if the upper threshold for react rtt threshold-type average 3 is configured as 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be $6000 + 6000 + 5000 = 17000 / 3 = 5667$, thus violating the 5000-ms upper threshold.</p> <p>The default number of 5 averaged measurements can be changed using the optional <i>number-of-measurements</i> argument. The valid range from 1 to 16.</p> <p>This syntax is not available if connectionLoss, timeout, or verifyError is specified as the monitored element, as upper and lower thresholds do not apply to these options.</p>

[threshold-value <i>upper-threshold</i> <i>lower-threshold</i>]	<p>(Optional) Specifies the upper-threshold value and lower-threshold values, for jitterAvg, jitterDSAvg, jitterSDAvg, mos, PacketLossDS, PacketLossSD, and rtt.</p> <p>The default upper-threshold value for all monitored elements except mos is 4500, and the default lower-threshold value is 3000.</p> <p>For MOS threshold values (react mos), the number is expressed in 3 digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 3.20, enter 320. The valid range is from 100 (1.00) to 500 (5.00). The default upper-threshold for MOS is 300 (3.00) and the default lower-threshold is 200 (2.00).</p>
action-type <i>option</i>	<p>(Optional) Specify what action or combination of actions the operation performs when you configure connection-loss-enable or timeout-enable, or threshold events occur. For the action-type to occur for threshold events, the threshold-type must be defined to anything other than never. Option can be one of the following keywords:</p> <ul style="list-style-type: none"> • none—No action is taken. • trapOnly—Send an SNMP logging trap when the specified violation type occurs for the monitored element. IP SLAs logging traps are enabled using the rtr logging traps command. For SNMP logging traps to be sent, SNMP logging must be enabled using the appropriate SNMP commands, including the snmp-server enable traps syslog command. • triggerOnly—Have one or more target operation's operational state make the transition from "pending" to "active" when the violation conditions are met. The target operations to be triggered are specified using the rtr reaction-trigger command. A target operation will continue until its life expires, as specified by the target operation's configured lifetime value). A triggered target operation must finish its life before it can be triggered again. • trapAndTrigger—Trigger both an SNMP trap and start another IP SLAs operation when the violation conditions are met, as defined in the trapOnly and triggerOnly options above. <p>The following SNA NMVT action-type options appear in the command line help, but are no longer valid: nmvtOnly, trapAndNmvt, nmvtAndTrigger, trapNmvtAndTrigger. These SNA NMVT CLI options will be removed in an upcoming release.</p>

Defaults

No IP SLAs reactions are generated.

Error verification is disabled.

Connection loss and timeout logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The verify-error-enable optional keyword was added.
12.3(7)T	<p>This command was enhanced to provide new monitored elements and reaction options. The old syntax of</p> <pre>rtr reaction-configuration <i>operation-number</i> [verify-error-enable] [connection-loss-enable] [timeout-enable] [threshold-falling <i>milliseconds</i>] [threshold-type <i>option</i>] [action-type <i>option</i>]</pre> <p>was replaced by the syntax shown above.</p> <p>Note Configuration of IP SLAs reactions using the old syntax remains available in release 12.3(7)T for backwards compatibility, but support for the old syntax will be removed in an upcoming release.</p> <ul style="list-style-type: none"> • The functionality of the connection-loss-enable keyword was replaced by the react connectionLoss syntax. • The functionality of the timeout-enable keyword was replaced by the react timeout syntax. • The functionality of the verify-error-enable keyword was replaced by the react verifyError syntax. • The functionality of the threshold-falling <i>milliseconds</i> syntax (and the threshold RTR configuration command) was replaced by the threshold-value <i>upper-threshold lower-threshold</i> syntax.
12.3(14)T	This command was replaced by the ip sla monitor reaction-configuration command.

Usage Guidelines

You can configure the **rtr reaction-configuration** command multiple times so as to allow reactions for multiple monitored elements (for example, configuring thresholds for operation 1 for destination-to-source packet loss, and also configuring MOS thresholds for same operation). However, issuing the **no rtr reaction-configuration** *operation-number* will clear all reactions for the specified operation. In other words, disabling of granular reaction elements (**no rtr reaction-configuration** *operation-number* **react** *monitored-element*) is not currently supported, so as to provide backwards compatibility with the earlier version of this command.

You can check the configuration of the IP SLAs reaction configuration using the **show rtr reaction-configuration** command.

**Note**

Keywords are not case sensitive and are shown in mixed case for readability only.

Examples

In the following example, IP SLAs operation 10 (a Jitter operation) is configured to send an SNMP logging trap when the MOS value exceeds 4.9 (best quality) or falls below 2.5 (poor quality):

```
Router(config)# rtr reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

The following example shows the default settings for the **rtr reaction-configuration** command when none of the optional syntax is used:

```

Router# show rtr reaction-configuration 1

Entry number: 1
Reaction Configuration not configured

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# rtr reaction-configuration 1
Router(config)# do show rtr reaction-configuration 1

Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None

```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the rtr reaction-configuration global configuration command.
show rtr reaction-configuration	Displays the current configuration for IP SLAs reactions.
show rtr reaction-trigger	Displays the configured state of triggered IP SLAs operations.
timeout	Sets the amount of time the IP SLAs operation waits for a response from its request packet.

rtr reaction-trigger



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr reaction-trigger** command is replaced by the **ip sla monitor reaction-trigger** command. See the **ip sla monitor reaction-trigger** command for more information.

To define a second Cisco IOS IP Service Level Agreements (IP SLAs) operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the **rtr reaction-configuration** command, use the **rtr reaction-trigger** command in global configuration mode. To remove the trigger combination, use the **no** form of this command.

```
rtr reaction-trigger operation-number target-operation
```

```
no rtr reaction-trigger operation
```

Syntax Description

<i>operation-number</i>	Number of the operation in the active state that has the action-type set with the rtr reaction-configuration global configuration command.
<i>target-operation</i>	Number of the operation in the pending state that is waiting to be triggered with the rtr global configuration command.

Defaults

No trigger combination is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor reaction-trigger command.

Usage Guidelines

Triggers are usually used for diagnostics purposes and are not used in normal operation.

Examples

In the following example, the state of operation 1 is changed from pending state to active state when **action-type** of operation 2 occurs:

```
Router(config)# rtr reaction-trigger 2 1
```

Related Commands	Command	Description
	rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
	rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
	rtr schedule	Configures the scheduling parameters for an IP SLAs operation.

rtr reset



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr reset** command is replaced by the **ip sla monitor reset** command. See the **ip sla monitor reset** command for more information.

To perform a shutdown and restart of the Cisco IOS IP Service Level Agreements (SLAs) engine, use the **rtr reset** command in global configuration mode.

rtr reset

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor reset command.

Usage Guidelines

The **rtr reset** command stops all operations, clears IP SLAs configuration information, and returns the IP SLAs feature to the startup condition. This command does not reread the IP SLAs configuration stored in startup-config in NVRAM. You must retype the configuration or load a previously saved configuration file.



Note

The **rtr reset** command does not remove IP SLAs label switched path (LSP) Health Monitor configurations from the running configuration.



Caution

Use the **rtr reset** command only in extreme situations such as the incorrect configuration of a number of operations.

Examples

The following example resets IP SLAs, clearing all stored IP SLAs information and configuration:

```
Router(config)# rtr reset
```

Related Commands

Command	Description
rtr restart	Restarts a stopped IP SLAs operation.

rtr responder



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr responder** command is replaced by the **ip sla monitor responder** command. See the **ip sla monitor responder** command for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder on a destination (operational target) device, use the **rtr responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

rtr responder

no rtr responder

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor responder command.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable the sending of receiving of IP SLAs Control packets. Enabling the IP SLAs Responder allows the generation of monitoring statistics on the device sending IP SLAs operations.

Examples

The following example enables the IP SLAs Responder:

```
Router(config)# rtr responder
```

Related Commands

Command	Description
rtr responder type tcpConnect	Enables the IP SLAs Responder for TCP Connect operations.
rtr responder type udpEcho	Enables the IP SLAs Responder for UDP Echo and Jitter operations.

rtr responder type frame-relay



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr responder type frame-relay** command is replaced by the **ip sla monitor responder type frame-relay** command. See the **ip sla monitor responder type frame-relay** command for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder on the operational target device for Frame Relay operations, use the **rtr responder type frame-relay** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

```
rtr responder type frame-relay {all | interface {serial | fr-atm} interface-id dlc1 dlc1-number}
```

```
no rtr responder type frame-relay {all | interface {serial | fr-atm} interface-id dlc1 dlc1-number}
```

Syntax Description

all	Specifies that the IP SLAs Responder will respond to Frame Relay operations on every interface and DLCI.
interface serial	Specifies the serial interface over which to respond to Frame Relay operations.
interface fr-atm	Specifies the Frame Relay interface over which to respond to Frame Relay operations.
<i>interface-number</i>	Frame Relay or Serial interface number.
dlc1 dlc1-number	Specifies the Frame Relay PVC subinterface link (DLCI number) that is assigned to the interface.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor responder type frame-relay command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

This command allows the IP SLAs Responder to respond to Frame Relay operations without receiving IP SLAs Control Protocol packets.

Note that if you use this command, packet loss statistics will not be able to be generated for the operation because the Responder will not be able to determine the order of the received packets. To generate packet loss statistics, use the **rtr responder** command without specifying an operation type.

Examples

In the following example, the IP SLAs Responder is configured to respond to Frame Relay operations specifically on Serial interface 1/0, using DLCI number 16:

```
Router(config)# rtr responder type frame-relay interface serial1/0 dlc1 16
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.

rtr responder type tcpConnect



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr responder type tcpConnect** command is replaced by the **ip sla monitor responder type tcpConnect** command. See the **ip sla monitor responder type tcpConnect** command for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder for TCP Connect operations, use the **rtr responder type tcpConnect** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

```
rtr responder type tcpConnect ipaddress ip-address port port
```

```
no rtr responder type tcpConnect ipaddress ip-address port port
```

Syntax	Description
ipaddress <i>ip-address</i>	(Optional) Specifies the IP address that the operation will be received at.
port <i>port</i>	(Optional) Specifies the port number that the operation will be received on.

Defaults Disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.1(1)T	The ipaddr and port keywords were added.
	12.3(14)T	This command was replaced by the ip sla monitor responder type tcpConnect command.

Usage Guidelines This command is used on the destination device for IP SLAs operations to enable the acceptance and return of TCP Connect operation packets.

Related Commands	Command	Description
	rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
	rtr responder type frame-relay	Enables the IP SLAs Responder for Frame Relay operations.
	rtr responder type udpEcho	Enables the IP SLAs Responder for UDP Echo and Jitter operations.

rtr responder type udpEcho



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr responder type udpEcho** command is replaced by the **ip sla monitor responder type udpEcho** command. See the **ip sla monitor responder type udpEcho** command for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder for User Datagram Protocol (UDP) Echo or Jitter operations, use the **rtr responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

```
rtr responder type udpEcho ipaddress ip-address port port
```

```
no rtr responder type udpEcho ipaddress ip-address port port
```

Syntax Description		
ipaddress <i>ip-address</i>	Specifies the IP address that the operation will be received at.	
port <i>port</i>	Specifies the port number that the operation will be received on.	

Defaults Disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.3(14)T	This command was replaced by the ip sla monitor type udpEcho command.

Usage Guidelines This command is used on the destination device for IP SLAs operations to enable UPD Echo and Jitter (UDP+) operations on non-native interfaces.

Examples The following example enables the IP SLAs Responder for Jitter operations:

```
Router(config)# rtr responder type udpEcho ipaddress A.B.C.D port 1
```

Related Commands	Command	Description
	rtr responder	Enables the IP SLAs Responder for non-specific IP SLAs operations.
	rtr responder type frame-relay	Enables the IP SLAs Responder for Frame Relay operations.

rtr restart



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr restart** command is replaced by the **ip sla monitor restart** command. See the **ip sla monitor restart** command for more information.

To restart a Cisco IOS IP Service Level Agreements (IP SLAs) operation, use the **rtr restart** command in global configuration mode.

```
rtr restart operation-number
```

Syntax Description	<i>operation-number</i>	Number of the IP SLAs operation to restart. IP SLAs allows a maximum of 2000 operations.
--------------------	-------------------------	--

Defaults	No default behavior or values.
----------	--------------------------------

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

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.2(11)T	The maximum number of operations was increased from 500 to 2000 (SAA Engine II).
	12.3(14)T	This command was replaced by the ip sla monitor restart command.

Usage Guidelines	To restart an operation, the operation should be in an “active” state (as defined in the rtr reaction-configuration command).
------------------	--

IP SLAs allows a maximum of 2000 operations.

This command does not have a **no** form.

Examples	The following example restarts operation 12:
----------	--

```
Router(config)# rtr restart 12
```

Related Commands	Command	Description
	rtr reset	Clears all current IP SLAs statistics and configuration information from the router and resets the IP SLAs engine.

rtr schedule



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr schedule** command is replaced by the **ip sla monitor schedule** command. See the **ip sla monitor schedule** command for more information.

To configure the scheduling parameters for a Cisco IOS IP Service Level Agreements (IP SLAs) single operation, use the **rtr schedule** command in global configuration mode. To stop the operation and place it in the default state (**pending**), use the **no** form of this command.

```
rtr schedule group-operation-number [life {forever | seconds}] [start-time {hh:mm[:ss]
  [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]
```

```
no rtr schedule group-operation-number
```

Syntax Description

<i>group-operation-number</i>	Group configuration or group schedule number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life <i>seconds</i>	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	Time when the operation starts.
<i>hh:mm[:ss]</i>	Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation. For example, start-time 01:02 means “start at 1:02 a.m.,” and start-time 13:01:30 means “start at 1:01 p.m. and 30 seconds.” The current day is implied unless you specify a <i>month</i> and <i>day</i> .
<i>month</i>	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified as well. You can specify the month by using either the full English name or the first three letters of the month.
<i>day</i>	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified as well.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after <i>hh:mm:ss</i>	(Optional) Indicates that the operation should start <i>hh</i> hours, <i>mm</i> minutes, and <i>ss</i> seconds after this command was entered.
ageout <i>seconds</i>	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out).
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.

Defaults

The operation is placed in a **pending** state (that is, the operation is enabled but not actively collecting information).

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.1(1)T	The after and forever keywords were added.
	12.3(8)T	The recurring keyword was added.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(27)SBC. This integration includes the addition of the recurring keyword.
	12.3(14)T	This command was replaced by the ip sla monitor schedule command.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC. This integration includes the addition of the recurring keyword.

Usage Guidelines

After you schedule the operation with the **rtr schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no** form of the **rtr** global configuration command and reenter the configuration information.

If the operation is in a pending state, you can define the conditions under which the operation makes the transition from pending to active with the **rtr reaction-trigger** and **rtr reaction-configuration** global configuration commands. When the operation is in an active state, it immediately begins collecting information.

The following time line shows the age-out process of the operation:

W-----X-----Y-----Z

where:

- W is the time the operation was configured with the **rtr** global configuration command.
- X is the start time or start of life of the operation (that is, when the operation became “active”).
- Y is the end of life as configured with the **rtr schedule** global configuration command (life seconds have counted down to zero).
- Z is the age out of the operation.

Age out starts counting down at W and Y, is suspended between X and Y, and is reset to its configured size at Y.

It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation’s configuration time and start time (X and W) must be less than the age-out seconds.



Note

The total RAM required to hold the history and statistics tables is allocated at the time of scheduling the IP SLAs operation. This prevents router memory problems when the router gets heavily loaded and lowers the amount of overhead an IP SLAs operation causes on a router when it is active.

For Service Level Monitoring (SLM) operations (**type slm**), the operation will always start at the nearest 15-minute interval since the router start time. For example, if the **rtr schedule 1 start-time now** command is used, the operation will not start until the next quarter-hour time increment.

The **recurring** keyword is only supported for scheduling single IP SLAs operations. You cannot schedule multiple IP SLAs operations using the **rtr schedule** command. The **life** value for a recurring IP SLAs operation should be less than one day. The **ageout** value for a recurring operation must be “never” (which is specified with the value 0), or the sum of the **life** and **ageout** values must be more than one day. If the **recurring** option is not specified, the operations are started in the existing normal scheduling mode.

Examples

In the following example, operation 25 begins actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished with its life. When this operation ages out, all configuration information for the operation is removed (that is, the configuration information is no longer in the running-config in RAM).

```
Router(config)# rtr schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

In the following example, operation 1 begins collecting data after a 5-minute delay:

```
Router(config)# rtr schedule 1 start after 00:05:00
```

In the following example, operation 3 begins collecting data immediately and is scheduled to run indefinitely:

```
Router(config)# rtr schedule 3 start-time now life forever
```

In the following example, operation 15 begins automatically collecting data every day at 1:30 a.m.:

```
Router(config)# rtr schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
rtr group schedule	Performs group scheduling for IP SLAs operations.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action-type options is defined with the rtr reaction-configuration global configuration command.
show rtr configuration	Displays the configuration details of the IP SLAs operation.

rtr slm frame-relay statistics



Note

Effective with Cisco IOS Release 12.3(14)T, the **rtr slm frame-relay statistics** command is replaced by the **ip sla monitor slm frame-relay statistics** command. See the **ip sla monitor slm frame-relay statistics** command for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) or Cisco Networking Services (CNS) to collect Frame Relay performance monitoring statistics, use the **rtr slm frame-relay statistics** command in global configuration mode. To disable the collection of Frame Relay performance monitoring statistics, use the **no** form of this command.

rtr slm frame-relay statistics

no rtr slm frame-relay statistics

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor slm frame-relay statistics command.

Usage Guidelines

The **rtr slm frame-relay statistics** command should be issued prior to configuring any of the Frame Relay IP SLAs operations (**type slm interface**, **type slm controller**, **type slm frame-relay** or **type slm frame-relay pvc**). Performance statistics are not retained for these operations until this command is issued.

This command does not affect the standard Frame Relay IP SLAs operation (**type frame-relay**).

Examples

In the following example the IP SLAs Frame Relay service level monitoring feature is enabled:

```
Router(config)# rtr slm frame-relay statistics
```

Related Commands

Command	Description
type slm controller	Specifies that the IP SLAs operation is an SLM controller operation, and specifies the controller that the operation should be run on.
type slm frame-relay interface	Specifies that the IP SLAs operation is an SLM FR interface operation, and specifies the interface that the operation should be run on.
type slm frame-relay pvc interface	Specifies that the IP SLAs operation is an SLM FR circuit operation, and specifies the interface and DLCI number that the operation should be run on.
type slm interface	Specifies that the IP SLAs operation is an SLM interface operation, and specifies the interface that the operation should be run on.

saa apm cache-size



Note

Effective with Cisco IOS Release 12.3(14)T, the **saa apm cache-size** command is replaced by the **ip sla monitor apm cache-size** command. See the **ip sla monitor apm cache-size** command for more information.

To set the size of the Cisco IOS IP Service Level Agreements (IP SLAs) Application Performance Monitor (APM) cache, use the **saa apm cache-size** command in global configuration mode. To reset the IP SLAs APM cache size to its default, use the **no** form of this command.

saa apm cache-size *bytes*

no saa apm cache-size *bytes*

Syntax Description

<i>bytes</i>	Number that specifies the size of the cache, in bytes. The default is 100000 bytes.
--------------	---

Defaults

The default APM cache size is 100000 bytes.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor apm cache-size command.

Usage Guidelines

The IP SLAs APM script and scheduler files are kept in an area of memory called the IP SLAs APM cache. The cache size is checked by the system before each attempt to copy a new file to the cache. If the file to be downloaded puts the cache over its size limit, a “cache trimming” operation is performed, and all files in the cache not tagged with a “sticky bit” (sticky=1) will be deleted.

Examples

In the following example, the IP SLAs APM cache is set to 80,000 bytes (approximately 78 kilobytes):

```
Router(config)# saa apm cache-size 80000
Router(config)# end
Router#
00:01:50: %SYS-5-CONFIG_I: Configured from console by console
Router# show saa apm cache

Cache Size (bytes): 80000
Cache used (bytes): 793

File Name                               TimeCreated TimeAccessed ref Type sticky
apm.cf.1234567                          00:02:50     00:00:00   1 CFG  0
```

apm/config/sntp-1000.cfg 00:02:50 00:00:00 1 CFG 0

Related Commands

Command	Description
show saa apm cache	Displays the amount of memory available in the IP SLAs APM cache and information about the files stored in the cache.

saa apm copy



Note

Effective with Cisco IOS Release 12.3(14)T, the **saa apm copy** command is replaced by the **ip sla monitor apm copy** command. See the **ip sla monitor apm copy** command for more information.

To copy script or scheduler files from an FTP server to the device that will initiate the Cisco IOS IP Service Level Agreements (IP SLAs) Application Performance Monitor (APM) operations, use the **saa apm copy** command in global configuration mode.

```
saa apm copy {script | scheduler} ftp://[username:password@]server-name/path-to-file/filename
[sticky]
```

Syntax Description

script	Specifies that the file to be copied is an APM script file (.scr).
scheduler	Specifies that the file to be copied is an APM scheduler file (.sch).
ftp://	Begins the URL that specifies the file to copy from a remote FTP server.
<i>username:password@</i>	(Optional) Specifies a username and password as part of the URL. Use these arguments only if they are required on the server.
<i>server-name</i>	The server-name component of the URL.
<i>path-to-file</i>	Folder-path component of the URL. A folder-path can contain multiple folder names. Each folder should be separated using a forward slash (/).
<i>filename</i>	Name of the file to be copied from the server.
sticky	(Optional) Indicates that the copied file should not be deleted from the local APM cache during a cache trimming operation.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor apm copy command.

Usage Guidelines

The **saa apm copy** command downloads an IP SLAs APM script or scheduler file from an FTP server to the local IP SLAs APM cache in NVRAM.

A file tagged as “sticky” will not be deleted from the local APM cache during a cache trimming operation. APM cache trimming operations are initiated when the **saa apm lowWaterMark** value is reached.

You can force a file tagged as “sticky” to be deleted using the **clear saa apm cache** command.

Examples

In the following example, a Frame Relay emulation script titled frm.scr is downloaded from the FTP server FTP101. The username joe and the password letmein are used to access the server:

```
Router(config)# saa apm copy script ftp://joe:letmein@FTP101/userbin/joefiles/frm.scr  
sticky
```

Related Commands

Command	Description
clear saa apm cache	Deletes files from the IP SLAs APM cache.
saa apm lowWaterMark	Specifies the lowest amount of free memory that must be available on the system to allow additional IP SLAs APM operations to be configured.

saa apm lowWaterMark



Note

Effective with Cisco IOS Release 12.3(14)T, the **saa apm lowWaterMark** command is replaced by the **ip sla monitor apm lowWaterMark** command. See the **ip sla monitor apm lowWaterMark** command for more information.

To specify the lowest amount of free memory that must be available on the system to allow additional Cisco IOS IP Service Level Agreements (IP SLAs) Application Performance Monitor (APM) operations to be configured, use the **saa apm lowWaterMark** command in global configuration mode. To restore the default low-memory-watermark value, use the **no** form of this command.

saa apm lowWaterMark *bytes*

no saa apm lowWaterMark

Syntax Description

bytes Number that specifies the size of the cache, in bytes.

Defaults

The default APM low-memory-watermark is 25 percent of free memory at startup.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor apm lowWaterMark command.

Usage Guidelines

The **saa apm lowWaterMark** global configuration command configures the lowest amount of free memory (low-memory-watermark) that must be available on the system. If the amount of available free memory falls below the value specified in the **saa apm lowWaterMark** command, then IP SLAs will not allow new APM operations to be configured. The default value is 25 percent of the memory available on the system at startup.



Note

The smaller the low-memory-watermark value is, the more APM operations can be configured. If the value is set to 0, then APM operations can be created until the system runs out of memory. However, you should be careful not to set the low-memory-watermark too low, as all additional router processes must be able to run with the amount of memory specified by the **saa apm lowWaterMark** and **rtr low-memory** commands. Setting the low-memory-watermark to 0 is discouraged, as other router processes may not be left with enough system memory to function.

For example, if there are 6 MB of free memory when the router starts up, and the default low-memory-watermark of 25 percent is used, then the IP SLAs APM can use up to 4.5 MB memory for creating operations. If the free memory drops below 1.5 MB, then new APM operations cannot be created.

The value of the **saa apm lowWaterMark** command should not exceed the amount of free memory available on the system. To determine the amount of free memory available on the system, use the **show memory EXEC** command.

The **show saa apm information EXEC** command will display the number of operations that can be configured on the device in the “Max Number of operations supported” field.

Examples

In the following example, the IP SLAs APM low-memory-watermark is set to 3,145,728 bytes (3 MB):

```
Router(config)# saa apm lowWaterMark 3145728
Router(config)# end
Router# show saa apm information
    Service Assurance Agent: Application Performance Monitor

    APM Engine Version: 1.0
Max Number of oper supported: 23
Number of configurable oper: 23
  Number of oper configured: 0
    Number of files in cache: 0
      Cache Size (bytes): 100000
      Cache used (bytes): 0
    APM low memory water-mark: 3,145,728
```

Related Commands

Command	Description
show saa apm information	Displays details about the IP SLAs APM.

saa apm operation



Note

Effective with Cisco IOS Release 12.3(14)T, the **saa apm operation** command is replaced by the **ip sla monitor apm operation** command. See the **ip sla monitor apm operation** command for more information.

To start or stop a Cisco IOS IP Service Level Agreements (IP SLAs) Application Performance Monitor (APM) operation, use the **saa apm operation** command in global configuration mode. To delete existing IP SLAs APM operations, use the **no** form of this command.

```
saa apm operation operation-number {start
ftp://[user:password@]server-name/path-to-file/filename | stop}
```

```
no saa apm operation [operation-number]
```

Syntax Description

<i>operation-number</i>	A number which uniquely identifies the APM operation. In the no saa apm operation form of this command, this argument is optional. If an operation-number is not specified in the no form of this command, all APM operations are removed from the system configuration.
start	Starts the specified operation.
ftp://	Begins the URL that specifies the configuration file to use for the APM operation.
<i>user:password@</i>	(Optional) Allows you to specify a user-name and password as part of the URL if they are required on the server.
<i>server-name</i>	Server-name component of the URL.
<i>path-to-file</i>	Folder path component of the URL. Each folder should be separated using a forward slash (/).
<i>filename</i>	Name of the APM configuration (.cf) file to be used for the operation.
stop	Stops the specified operation.

Defaults

No IP SLAs APM operations exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor apm operation command.

Usage Guidelines

The following files are required to perform an IP SLAs APM operation:

- script file (.scr) available on the routing device running IP SLAs
- scheduler file (.sch) available on the routing device running IP SLAs
- configuration file (.cf) available on an FTP server
- data file (.dat) available on an FTP server

All filenames can have a maximum of 255 characters.

The **saa apm operation start** command points to the APM configuration file to be used for the operation. The APM configuration file specifies the location of the other files used in the operation, and the target IP address for the operation.

To download script, configuration, data, and scheduler template files used by the IP SLAs APM, and to download the documentation (“readme” files) for the scripts, go to the “Cisco IP SAA APM” page at <http://www.cisco.com/cgi-bin/tablebuild.pl/saa-apm>.

After an operation is started using the **saa apm operation start** command, the operation should be stopped using the **saa apm operation stop** command.

Examples

In the following example, an IP SLAs APM NNTP operation is started and stopped, and the operation is deleted from the configuration:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# saa apm operation 2 start
ftp://user:password@saa-nms/apm/config/nntp-20.cf
Router(config)#
1d09h: SAA-APM-1: downloading file (apm/config/nntp-20.cf) of size (532)
1d09h: SAA-APM-1: using cached file (apm/scheduler/master.sch)
1d09h: SAA-APM-1: using cached file (apm/scripts/nntp.scr)
1d09h: SAA-APM-1: sending APM_SCRIPT_DONE message
1d09h: SAA-APM-1: operation done
Router(config)# saa apm operation 2 stop
Router(config)# no saa apm operation 2
```

Related Commands

Command	Description
show saa apm results	Displays the data gathered using the IP SLAs Application Performance Monitor.

samples-of-history-kept

To set the number of entries kept in the history table per bucket for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **samples-of-history-kept** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

samples-of-history-kept *samples*

no samples-of-history-kept

Syntax Description	<i>samples</i>	Number of entries kept in the history table per bucket. The default is 16.
---------------------------	----------------	--

Defaults	16 entries
-----------------	------------

Command Modes	<p>IP SLA Monitor Configuration ICMP path echo configuration (config-sla-monitor-pathEcho)</p> <p>RTR Configuration ICMP path echo configuration (config-rtr-pathEcho)</p>
----------------------	--



Note

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.2</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.2	This command was introduced.
Release	Modification				
11.2	This command was introduced.				

Usage Guidelines	<p>An IP SLAs operation can collect history and capture statistics. By default, the history for an IP SLAs operation is not collected. If history is collected, each history bucket contains one or more history entries from the operation. When the operation type is ICMP path echo, an entry is created for each hop along the path that the operation takes to reach its destination. The type of entry stored in the history table is controlled by the filter-for-history command. The total number of entries stored in the history table is controlled by the combination of the samples-of-history-kept, buckets-of-history-kept, and lives-of-history-kept commands.</p>
-------------------------	---



Note

This command is supported by the IP SLAs ICMP path echo operation only.



Note

Collecting history increases the RAM usage. Collect history only when you think there is a problem in the network.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 60](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **samples-of-history-kept** command varies depending on the Cisco IOS release you are running (see [Table 60](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP path echo operation type is configured, you would enter the **samples-of-history-kept** command in ICMP path echo configuration mode (config-sla-monitor-pathEcho) within IP SLA monitor configuration mode.

Table 60 Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.3(14)T and 12.4	ip sla monitor	IP SLA monitor configuration
All other Cisco IOS releases	rtr	RTR configuration

Examples

In the following examples, ten entries are kept in the history table for each of the lives of IP SLAs ICMP path echo operation 1. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 60](#)).

IP SLA Monitor Configuration

```
ip sla monitor 1
  type pathecho protocol ipIcmpEcho 172.16.1.176
  lives-of-history-kept 3
  samples-of-history-kept 10
!
ip sla monitor schedule 1 life forever start-time now
```

RTR Configuration

```
rtr 1
  type pathecho protocol ipIcmpEcho 172.16.1.176
  lives-of-history-kept 3
  samples-of-history-kept 10
!
rtr schedule 1 life forever start-time now
```

Related Commands

Command	Description
buckets-of-history-kept	Sets the number of history buckets that are kept during the lifetime of the IP SLAs operation.
filter-for-history	Defines the type of information kept in the history table for the IP SLAs operation.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

Command	Description
lives-of-history-kept	Sets the number of lives maintained in the history table for the IP SLAs operation.
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.

scheduler allocate

To guarantee CPU time for processes, use the **scheduler allocate** command in global configuration mode. To restore the default, use the **no** form of this command.

scheduler allocate *interrupt-time process-time*

no scheduler allocate

Syntax Description

<i>interrupt-time</i>	Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network interrupt context. The range is from 400 to 60000 microseconds. The default is 4000 microseconds.
<i>process-time</i>	Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled. The range is from 100 to 4000 microseconds. The default is 200 microseconds.

Defaults

Approximately 5 percent of the CPU is available for process tasks.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command applies to the Cisco 7200 series and Cisco 7500 series routers.



Note

Changing settings associated with CPU processes can negatively impact system performance.

Examples

The following example makes 20 percent of the CPU available for process tasks:

```
Router (config)# scheduler allocate 2000 500
```

Related Commands

Command	Description
scheduler interval	Controls the maximum amount of time that can elapse without running system processes.

scheduler heapcheck process

To perform a “sanity check” for corruption in memory blocks when a process switch occurs, use the **scheduler heapcheck process** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
scheduler heapcheck process [memory [fast] [io] [multibus] [pci] [processor] [checktype {all | magic | pointer | refcount | lite-chunks}]]
```

```
no scheduler heapcheck process
```

Syntax Description	
memory	(Optional) Specifies checking all memory blocks and memory pools.
fast	(Optional) Specifies checking the fast memory block.
io	(Optional) Specifies checking the I/O memory block.
multibus	(Optional) Specifies checking the multibus memory block.
pci	(Optional) Specifies checking the process control information (PCI) memory block.
processor	(Optional) Specifies checking the processor memory block.
checktype	(Optional) Specifies checking specific memory pools.
all	(Optional) Specifies checking the value of the block magic, red zone, size, refcount, and pointers (next and previous).
magic	(Optional) Specifies checking the value of the block magic, red zone, and size.
pointer	(Optional) Specifies checking the value of the next and previous pointers.
refcount	(Optional) Specifies checking the value of the block magic and refcount.
lite-chunks	(Optional) Specifies checking the memory blocks allocated by the memory allocation lite (malloc_lite) feature.

Defaults This command is not enabled by default. If no keywords are specified, a sanity check will be performed on all the memory blocks and memory pools.

Command Modes Global configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.3(11)T	The lite-chunks keyword was added.

Usage Guidelines When configuring this command, you can choose none or all memory block keywords (**fast**, **io**, **multibus**, **pci**, **processor**, and **checktype**).

Enabling this command has a significant impact on router performance.

Examples

The following example shows how to sanity check for corruption in the I/O memory block when a process switch occurs. In this example, the values of only the block magic, red zone, and size will be checked.

```
scheduler heapcheck process memory io checktype magic
```

The following example shows how to sanity check for corruption in the processor memory block when a process switch occurs. In this example, the values of only the next and previous pointers will be checked.

```
scheduler heapcheck process memory processor checktype pointer
```

Related Commands

Command	Description
memory lite	Enables the malloc_lite feature.
memory sanity	Performs a “sanity check” for corruption in buffers and queues.

scheduler interval

To control the maximum amount of time that can elapse without running system processes, use the **scheduler interval** command in global configuration mode. To restore the default, use the **no** form of this command.

scheduler interval *milliseconds*

no scheduler interval

Syntax Description	<i>milliseconds</i>	Integer that specifies the interval (in milliseconds). The minimum interval that you can specify is 500 milliseconds; there is no maximum value.
---------------------------	---------------------	--

Defaults High-priority operations are allowed to use as much of the CPU as needed.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The normal operation of the network server allows the switching operations to use as much of the central processor as is required. If the network is running unusually heavy loads that do not allow the processor the time to handle the routing protocols, give priority to the system process scheduler. High-priority operations are allowed to use as much of the CPU as needed.



Note

Changing settings associated with CPU processes can negatively impact system performance.

On the Cisco 7200 series and Cisco 7500 series, use the **scheduler allocate** global configuration command instead of the **scheduler interval** command.

Examples The following example changes the low-priority process schedule to an interval of 750 milliseconds:

```
Router(config)# scheduler interval 750
```

Related Commands	Command	Description
	scheduler allocate	Guarantees CPU time for processes.

schema

To specify the bulk statistics schema to be used in a specific bulk statistics transfer configuration, use the **schema** command in Bulk Statistics Transfer configuration mode. To remove a previously configured schema from a specific bulk statistics transfer configuration, use the **no** form of this command.

schema *schema-name*

no schema *schema-name*

Syntax Description

<i>schema-name</i>	Name of a previously configured bulk statistics schema.
--------------------	---

Defaults

No bulk statistics schema is specified.

Command Modes

Bulk Statistics Transfer configuration (config-bulk-tr)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Repeat this command as desired for a specific bulk statistics transfer configuration. Multiple schemas can be associated with a single transfer configuration; all collected data will be in a single bulk statistics data file (VFile).

Examples

In the following example, the bulk statistics schemas ATM2/0-IFMIB and ATM2/0-CAR are associated with the bulk statistics transfer configuration called bulkstat1:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# schema ATM2/0-CAR
Router(config-bulk-tr)# url primary ftp://user:pswr@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

scripting tcl encdir

To specify the default location of external encoding files used by the Tool Command Language (Tcl) shell, use the **scripting tcl encdir** command in global configuration mode. To remove the default location, use the **no** form of this command.

```
scripting tcl encdir location-url
```

```
no scripting tcl encdir location-url
```

Syntax Description	<i>location-url</i>	The URL used to access external encoding files used by Tcl.
---------------------------	---------------------	---

Defaults	Tcl does not use external encoding files.
-----------------	---

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

Command History	Release	Modification
	12.3(2)T	This command was introduced.

Usage Guidelines

Character strings in Tcl are encoded using 16-bit Unicode characters. Different operating system interfaces or applications can generate character strings using other encoding methods. Use the **scripting tcl encdir** command to configure a location URL for the external Tcl character encoding files to support the Tcl **encoding** command.

Tcl contains only a few character sets internally. Additional characters sets are loaded, as needed, from external files.

Examples

The following example shows how to specify a default location for external encoding files to be used by Tcl:

```
Router# config terminal
Router(config)# scripting tcl encdir tftp://10.18.117.23/file2/
```

Related Commands	Command	Description
	scripting tcl init	Specifies an initialization script for the Tcl shell.
	tclsh	Enables the Tcl shell and enters Tcl configuration mode.

scripting tcl init

To specify an initialization script for the Tool Command Language (Tcl) shell, use the **scripting tcl init** command in global configuration mode. To remove the initialization script, use the **no** form of this command.

scripting tcl init *init-url*

no scripting tcl init *init-url*

Syntax Description

<i>init-url</i>	The URL used to access the initialization script to be used by Tcl.
-----------------	---

Defaults

Tcl does not run an initialization script.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

Use the **scripting tcl init** command when you want to predefine Tcl procedures to run in an initialization script. The initialization script runs when the Tcl shell is entered and saves manual sourcing of the individual scripts.

Examples

The following example shows how to specify an initialization script to run when the Tcl shell is enabled:

```
Router# config terminal
Router(config)# scripting tcl init ftp://user:password@172.17.40.3/tclscript/initfile3.tcl
```

Related Commands

Command	Description
scripting tcl encdir	Specifies the default location of external encoding files used by the Tcl shell.
tclsh	Enables the Tcl shell and enters Tcl configuration mode.

send

To send messages to one or all terminal lines, use the **send** command in user EXEC or privileged EXEC mode.

```
send {line-number | * | aux number | console number | tty number | vty number}
```

Syntax Description

<i>line-number</i>	Line number to which the message will be sent.
*	Sends a message to all lines.
aux number	Sends a message to the specified AUX port.
console number	Sends a message to the specified console port.
tty number	Sends a message to the specified asynchronous line.
vty number	Sends a message to the specified virtual asynchronous line.

Defaults

No messages are sent.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

After entering this command, the system prompts for the message to be sent, which can be up to 500 characters long. Enter **Ctrl-Z** to end the message. Enter **Ctrl-C** to abort this command.



Caution

Be aware that in some circumstances text sent using the **send** command may be interpreted as an executable command by the receiving device. For example, if the receiving device is Unix workstation, and the receiving device is in a state (shell) where commands can be executed, the incoming text, if a properly formatted Unix command, will be accepted by the workstation as a command. For this reason, you should limit your exposure to potential messages from terminal servers or other Cisco IOS-based devices when running an interactive shell.

Examples

The following example sends a message to all lines:

```
2509# send *
Enter message, end with CTRL/Z; abort with CTRL/C:
The system 2509 will be shut down in 10 minutes for repairs.^Z
Send message? [confirm]
2509#
***
***
*** Message from tty0 to all terminals:
```

The system 2509 will be shut down in 10 minutes for repairs.

server (boomerang)

To configure the server address for a specified boomerang domain, use the **server** command in boomerang configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

server *server-ip-address*

no server *server-ip-address*

Syntax Description

<i>server-ip-address</i>	IP address of the specified server.
--------------------------	-------------------------------------

Defaults

No default behavior or values.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **server** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the Director Response Protocol (DRP) agent.

Use the **server** command to specify a server address that is to be associated with a given domain name. This configuration overrides the server-to-DRP agent association that is configured on DistributedDirector.

Examples

The following example configures the server for a domain named www.boom1.com. The server address for www.boom1.com is 172.16.101.101:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# server 172.16.101.101
```

```
Router# show running-config
.
.
.
ip drp domain www.boom1.com
content-server 172.16.101.101
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.

Command	Description
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttdns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttdns ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

service compress-config

To compress startup configuration files, use the **service compress-config** command in global configuration mode. To disable compression, use the **no** form of this command.

service compress-config

no service compress-config

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines After you configure the **service compress-config** command, the router will compress configuration files every time you save a configuration to the startup configuration. For example, when you enter the **copy system:running-config nvram:startup-config** command, the running configuration will be compressed before storage in NVRAM.

If the file compression succeeds, the following message is displayed:

```
Compressing configuration from configuration-size to compressed-size
[OK]
```

If the boot ROMs do not recognize a compressed configuration, the following message is displayed:

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

If the file compression fails, the following message is displayed:

```
Error trying to compress nvram
```

One way to determine whether a configuration file will be compressed enough to fit into NVRAM is to use a text editor to enter the configuration, then use the UNIX **compress** command to check the compressed size. To get a closer approximation of the compression ratio, use the UNIX **compress -b12** command.

Once the configuration file has been compressed, the router functions normally. At boot time, the system recognizes that the configuration file is compressed, uncompresses it, and proceeds normally. A **partition nvram:startup-config** command uncompresses the configuration before displaying it.

To disable compression of the configuration file, enter configuration mode and specify the **no service compress-config** command. Then, exit global configuration mode and enter the **copy system:running-config nvram:startup-config** command. The router displays an OK message if it is

able to write the uncompressed configuration to NVRAM. Otherwise, the router displays an error message indicating that the configuration is too large to store. If the configuration file is larger than the physical NVRAM, the following message is displayed:

```
##Configuration too large to fit uncompressed in NVRAM Truncate configuration? [confirm]
```

When the file is truncated, commands at the end of the file are erased. Therefore, you will lose part of your configuration. To truncate and save the configuration, type **Y**. To not truncate and not save the configuration, type **N**.

Examples

In the following example, the configuration file is compressed:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# service compress-config
Router(config)# end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# copy system:running-config nvram:startup-config
Building configuration...
Compressing configuration from 1179 bytes to 674 bytes
[OK]
```

Related Commands

Command	Description
partition nvram:startup-config	Separates Flash memory into partitions on Class B file system platforms.

service config

To enable autoloading of configuration files from a network server, use the **service config** command in global configuration mode. To restore the default, use the **no** form of this command.

service config

no service config

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled, except on systems without NVRAM or with invalid or incomplete information in NVRAM. In these cases, autoloading of configuration files from a network server is enabled automatically.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Usually, the **service config** command is used in conjunction with the **boot host** or **boot network** command. You must enter the **service config** command to enable the router to automatically configure the system from the file specified by the **boot host** or **boot network** command.

With IOS software versions 12.3(2)T, 12.3(1)B, and later, you no longer have to specify the **service config** command for the **boot host** or **boot network** command to be active.

If you specify both the **no service config** command and the **boot host** command, the router attempts to find the specified host configuration file. The **service config** command can also be used without the **boot host** or **boot network** command. If you do not specify host or network configuration filenames, the router uses the default configuration files. The default network configuration file is network-config. The default host configuration file is host-config, where host is the hostname of the router. If the Cisco IOS software cannot resolve its hostname, the default host configuration file is router-config.

Examples

In the following example, a router is configured to autoload the default network and host configuration files. Because no **boot host** or **boot network** commands are specified, the router uses the broadcast address to request the files from a TFTP server.

```
Router(config)# service config
```

The following example changes the network configuration filename to bridge_9.1, specifies that rcp is to be used as the transport mechanism, and gives 172.16.1.111 as the IP address of the server on which the network configuration file resides:

```
Router(config)# service config
Router(config)# boot network rcp://172.16.1.111/bridge_9.1
```

Related Commands

Command	Description
boot host	Changes the default name of the host configuration filename from which to load configuration commands.
boot network	Changes the default name of the network configuration file from which to load configuration commands.

service decimal-tty

To specify that line numbers be displayed and interpreted as octal numbers rather than decimal numbers, use the **no service decimal-tty** command in global configuration mode. To restore the default, use the **service decimal-tty** command.

service decimal-tty

no service decimal-tty

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled (line numbers displayed as decimal numbers)

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

In the following example, the router is configured to display decimal rather than octal line numbers:

```
Router(config)# service decimal-tty
```

service exec-wait

To delay the startup of the EXEC on noisy lines, use the **service exec-wait** command in global configuration mode. To disable the delay function, use the **no** form of this command.

service exec-wait

no service exec-wait

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command delays startup of the EXEC until the line has been idle (no traffic seen) for 3 seconds. The default is to enable the line immediately on modem activation.

This command is useful on noisy modem lines or when a modem attached to the line is configured to ignore MNP/V.42 negotiations, and MNP/V.42 modems may be dialing in. In these cases, noise or MNP/V.42 packets may be interpreted as usernames and passwords, causing authentication failure before the user has a chance to type a username or password. The command is not useful on nonmodem lines or lines without some kind of login configured.

Examples The following example delays the startup of the EXEC:

```
Router(config)# service exec-wait
```

service finger

The **service finger** command has been replaced by the **ip finger** command. However, the **service finger** and **no service finger** commands continue to function to maintain backward compatibility with older versions of Cisco IOS software. Support for this command may be removed in a future release. See the description of the **ip finger** command for more information.

service hide-telnet-address

To hide addresses while trying to establish a Telnet session, use the **service hide-telnet-address** command in global configuration mode. To disable this service, use the **no** form of this command.

service hide-telnet-address

no service hide-telnet-address

Syntax Description This command has no arguments or keywords.

Defaults Addresses are displayed.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines When you attempt to connect to a device, the router displays addresses and other messages (for example, “Trying router1 (171.69.1.154, 2008)...”). With the hide feature, the router suppresses the display of the address (for example, “Trying router1 address #1...”). The router continues to display all other messages that would normally be displayed during a connection attempt, such as detailed error messages if the connection was not successful.

The hide feature improves the functionality of the busy-message feature. When you configure only the **busy-message** command, the normal messages generated during a connection attempt are not displayed; only the busy-message is displayed. When you use the hide and busy features together you can customize the information displayed during Telnet connection attempts. When you configure the **service hide-telnet-address** command and the **busy-message** command, the router suppresses the address and displays the message specified with the **busy-message** command if the connection attempt is not successful.

Examples The following example hides Telnet addresses:

```
Router(config)# service hide-telnet-address
```

Related Commands	Command	Description
	busy-message	Creates a “host failed” message that is displayed when a connection fails.

service linenumber

To configure the Cisco IOS software to display line number information after the EXEC or incoming banner, use the **service linenumber** command in global configuration mode. To disable this function, use the **no** form of this command.

service linenumber

no service linenumber

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines With the **service linenumber** command, you can have the Cisco IOS software display the host name, line number, and location each time an EXEC process is started, or an incoming connection is made. The line number banner appears immediately after the EXEC banner or incoming banner. This feature is useful for tracking problems with modems, because the host and line for the modem connection are listed. Modem type information can also be included.

Examples In the following example, a user Telnets to Router2 before and after the **service linenumber** command is enabled. The second time, information about the line is displayed after the banner.

```
Router1> telnet Router2

Trying Router2 (172.30.162.131)... Open

Welcome to Router2.

User Access Verification

Password:
Router2> enable
Password:
Router2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)# service linenumber
Router2(config)# end
Router2# logout

[Connection to Router2 closed by foreign host]
Router1> telnet Router2
```

```
Trying Router2 (172.30.162.131)... Open  
Welcome to Router2.  
Router2 line 10  
  
User Access Verification  
  
Password:  
Router2>
```

Related Commands

Command	Description
show users	Displays information about the active lines on the router.

service nagle

To enable the Nagle congestion control algorithm, use the **service nagle** command in global configuration mode. To to disable the algorithm, use the **no** form of this command.

service nagle

no service nagle

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines When using a standard TCP implementation to send keystrokes between machines, TCP tends to send one packet for each keystroke typed. On larger networks, many small packets use up bandwidth and contribute to congestion.

The algorithm developed by John Nagle (RFC 896) helps alleviate the small-packet problem in TCP. In general, it works this way: The first character typed after connection establishment is sent in a single packet, but TCP holds any additional characters typed until the receiver acknowledges the previous packet. Then the second, larger packet is sent, and additional typed characters are saved until the acknowledgment comes back. The effect is to accumulate characters into larger chunks, and pace them out to the network at a rate matching the round-trip time of the given connection. This method is usually effective for all TCP-based traffic. However, do not use the **service nagle** command if you have XRemote users on X Window system sessions.

Examples The following example enables the Nagle algorithm:

```
Router(config)# service nagle
```

service prompt config

To display the configuration prompt (config), use the **service prompt config** command in global configuration mode. To remove the configuration prompt, use the **no** form of this command.

service prompt config

no service prompt config

Syntax Description This command has no arguments or keywords.

Defaults The configuration prompts appear in all configuration modes.

Command Modes Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Examples

In the following example, the **no service prompt config** command prevents the configuration prompt from being displayed. The prompt is still displayed in EXEC mode. When the **service prompt config** command is entered, the configuration mode prompt reappears.

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no service prompt config
hostname newname
end
newname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
service prompt config
newname(config)# hostname Router
Router(config)# end
Router#
```

Related Commands

Command	Description
hostname	Specifies or modifies the host name for the network server.
prompt	Customizes the prompt.

service sequence-numbers

To enable visible sequence numbering of system logging messages, use the **service sequence-numbers** command in global configuration mode. To disable visible sequence numbering of logging messages, use the **no** form of this command.

service sequence-numbers

no service sequence-numbers

Syntax Description This command has no arguments or keywords.

Defaults Disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0	This command was introduced.

Usage Guidelines Each system status messages logged in the system logging process have a sequence reference number applied. This command makes that number visible by displaying it with the message. The sequence number is displayed as the first part of the system status message. See the description of the **logging** commands for information on displaying logging messages.

Examples In the following example logging message sequence numbers are enabled:

```
.Mar 22 15:28:02 PST: %SYS-5-CONFIG_I: Configured from console by console
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# service sequence-numbers
Router(config)# end
Router#
000066: .Mar 22 15:35:57 PST: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands	Command	Description
	logging on	Enables system logging globally.
	service timestamps	Enables time-stamping of system logging messages or debugging messages.