

type dhcp

To configure a Dynamic Host Configuration Protocol Service Assurance Agent (SAA) operation, use the **type dhcp** command in SAA RTR configuration mode. To disable a DHCP SAA operation, use the **no** form of this command.

```
type dhcp [source-ipaddr source-ip-address] [dest-ipaddr dest-ip-address] [option
decimal-option] [circuit-id circuit-id] [remote-id remote-id] [subnet-mask subnet-mask]
```

```
no type dhcp
```

Syntax Description

source-ipaddr <i>source-ip-address</i>	(Optional) Source name or IP address.
dest-ipaddr <i>dest-ip-address</i>	(Optional) Destination name or IP address.
option <i>decimal-option</i>	(Optional) Option number. The only currently valid value is 82. DHCP option 82 allows you to specify the circuit-id, remote-id, and/or the subnet-mask for the destination DHCP server.
circuit-id <i>circuit-id</i>	(Optional) Circuit ID in hexadecimal.
remote-id <i>remote-id</i>	(Optional) Remote ID in hexadecimal.
subnet-mask <i>subnet-mask</i>	(Optional) Subnet mask IP address. The default value is 255.255.255.0.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	The following keywords were added: <ul style="list-style-type: none"> source-ipaddr dest-ipaddr option 82

Usage Guidelines

You must configure the type of operation before you can configure any of the other characteristics of the operation.

If the source IP address is configured, then packets will be sent with that source address.

You may configure the **ip dhcp-server** command to identify the DHCP server that the DHCP operation will measure.

If the target IP address is configured, then only that device will be measured.

If the **ip dhcp-server** command is not configured and the target IP address is not configured, then DHCP discover packets will be sent on every available IP interface.

Option 82 is called the Relay Agent Information option and is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies. The DHCP Server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

The Relay Agent Information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. The initial sub-options are defined for a relay agent that is co-located in a public circuit access unit. These suboptions are as follows: a **circuit-id** for the incoming circuit, a **remote-id** which provides a trusted identifier for the remote high-speed modem, and a **subnet-mask** designation for the logical IP subnet from which the relay agent received the client DHCP packet.

If an odd number of characters are specified for the **circuit-id**, a zero will be added to the end of the string.

Examples

In the following example, SAA operation number 4 is configured as a DHCP operation enabled for DHCP server 172.16.20.3:

```
Router(config)# rtr 4
Router(config-rtr)# type dhcp option 82 circuit-id 10005A6F1234
Router(config-rtr)# exit
Router(config)# ip dhcp-server 172.16.20.3
```

Related Commands

Command	Description
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

type dlsw

To configure a data-link switching (DLSw) Service Assurance Agent (SAA) operation, use the **type dlsw** command in SAA RTR configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

```
type dlsw peer-ipaddr ip-address
```

```
no type dlsw peer-ipaddr ip-address
```

Syntax Description

peer-ipaddr	Peer destination.
<i>ip-address</i>	IP address.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

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

Usage Guidelines

In order to configure a DLSw operation, the DLSw feature must be configured on the local and target routers.

You must configure the type of operation before you can configure any of the other characteristics of the operation.

The default for the optional characteristic **request-data-size** for a DLSw SAA operation is 0 bytes.

The default for the optional characteristic **timeout** for a DLSw SAA operation is 30 seconds.

Examples

In the following example, SAA operation number 4 is configured as a DLSw operation enabled for remote peer IP address 172.21.27.11. The data size is 15 bytes.

```
Router(config)# rtr 4
Router(config-rtr)# type dlsw peer-ipaddr 172.21.27.11
Router(config-rtr)# request-data-size 15
```

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.
show dlsw peers	Displays DLSw peer information.

type dns

To configure a Domain Name System (DNS) Service Assurance Agent (SAA) operation, use the **type dns** command in SAA RTR configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

type dns target-addr {*ip-address* | *hostname*} **name-server** *ip-address*

no type dns target-addr {*ip-address* | *hostname*} **name-server** *ip-address*

Syntax Description	target-addr { <i>ip-address</i> <i>hostname</i> }	Target (destination) IP address or hostname.
	name-server <i>ip-address</i>	IP address of the Domain Name Server.

Defaults No SAA operation type is associated with the operation number being configured.

Command Modes SAA RTR configuration

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

Usage Guidelines You must configure the type of operation before you can configure any of the other characteristics of the operation.

Examples In the following example, SAA operation 7 is created and configured as a DNS operation using the target IP address 172.20.2.132:

```
Router(config)# rtr 7
Router(config-rtr)# type dns target-addr lethe name-server 172.20.2.132
```

Related Commands	Command	Description
	rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

type echo

To configure an Service Assurance Agent (SAA) end-to-end echo response time probe operation, use the **type echo** command in SAA RTR configuration mode. To remove the operation from the configuration, use the **no** form of this command.

```
type echo protocol protocol-type target [source-ipaddr ip-address]
```

```
no type echo protocol protocol-type target [source-ipaddr ip-address]
```

Syntax Description

protocol <i>protocol-type target</i>	Protocol used by the operation. The <i>protocol-type target</i> argument combination must take one of the following forms: <ul style="list-style-type: none"> • ipIcmpEcho {<i>ip-address</i> <i>hostname</i>}—IP/ICMP Echo. Requires a destination IP address or IP host name. • snaRUEcho <i>sna-hostname</i>—SNA's SSCP Native Echo. Requires the host name defined for the SNA's PU connection to VTAM. • snaLU0EchoAppl <i>sna-hostname</i> [<i>sna-application</i>] [<i>sna-mode</i>]—SNA LU type 0 connection to Cisco's NSPECHO host application that requires the host name defined for the SNA's PU connection to VTAM. Optionally, specify the host application name (the default is NSPECHO) and SNA mode to access the application. • snaLU2EchoAppl <i>sna-hostname</i> [<i>sna-application</i>] [<i>sna-mode</i>]—SNA LU type 2 connection to Cisco's NSPECHO host application that requires the host name defined for the SNA's PU connection to VTAM. Optionally, specify the host application name (the default is NSPECHO) and SNA mode to access the application.
source-ipaddr <i>ipaddr</i>	(Optional) Specifies an IP address as the source for the operation.

Defaults

The default SNA host *sna-application* name for an SNA LU type echo is NSPEcho. The default data size for a IP/ICMP echo operation is 28 bytes.

Command Modes

SAA RTR configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The source-ipaddr <i>ip-address</i> keyword/argument combination was added to support the specification of an IP source for the operation.

Usage Guidelines

Support of echo to a protocol and pathEcho to a protocol is dependent on the protocol type and implementation. In general most protocols support echo and few protocols support pathEcho.

**Note**

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

Prior to sending a operation packet to the responder, the SAA sends a control message to the Responder to enable the destination port.

The default for the optional characteristic **request-data-size** for a ipIcmpEcho operation is 28 bytes. This is the payload portion of the Icmp packet, which makes a 64 byte IP packet.

Examples

In the following example, operation 10 is created and configured as an echo probe using the IP/ICMP Echo protocol and the destination IP address 172.16.1.175:

```
Router(config)# rtr 10
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.175
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
show rtr configuration	Displays configuration values for RTR operations.

type frame-relay

To measure response time, frame loss, or data corruption across a Frame Relay permanent virtual circuit (PVC) using the Service Assurance Agent (SAA), use the **type frame-relay** command in global configuration mode. To delete a preconfigured frame-relay operation, use the **no** form of this command.

type frame-relay interface *interface-id* **dcli** *dcli-number*

no type frame-relay interface *interface-id* **dcli** *dcli-number*

Syntax Description

interface <i>interface-id</i>	Specifies the Frame Relay interface from which the operation will be sent. The <i>interface-id</i> argument should consist of the interface type and identification number (for example, serial 1/0).
dcli <i>dcli-number</i>	Specifies the Frame Relay PVC subinterface link that is assigned to the interface.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

RTR Entry configuration mode

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The SAA Responder must be enabled on the target router before this command is used. Use the **rtr responder type frame-relay all** global configuration command or the **rtr responder** global configuration command on the target router to enable the responder.

If the first measurement does not have the correct values for frames sent and frames lost, the Frame Relay monitoring operation cannot work properly. There need to be at least two successful measurements for the frames sent and frames lost to be correct.

If the encapsulation on the target interface is not Frame Relay (for example, if the encapsulation is changed), the Frame Relay operation will be removed automatically from the configuration.

Examples

In the following example, a Frame Relay monitoring operation is configured to be sent from serial interface 0/1 using DLCI subinterface 22:

```
Router(config)# rtr 1
Router(config-rtr)# type frame-Relay interface Serial10 dcli 22
```

Related Commands

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

type ftp

To configure an FTP operation, use the **type ftp** command in SAA RTR configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

type ftp operation get url *url* [**source-ipaddr** *source-ip-address*] [**mode** {**passive** | **active**}]

no type ftp operation get url *url* [**source-ipaddr** *source-ip-address*] [**mode** {**passive** | **active**}]

Syntax Description

operation get	Specifies an FTP GET operation. (Support for other FTP operation types may be added in future releases.)
url <i>url</i>	Location information for the file to retrieve.
source-ipaddr <i>source-ip-address</i>	(Optional) Source address of the operation.
mode	(Optional) Specifies the transfer mode, either active or passive.
passive	FTP passive transfer mode. This is the default.
active	FTP active transfer mode.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

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

Usage Guidelines

GET is the only valid operation value. The URL must be in one of the following formats:

- ftp://user:password@host/filename
- ftp://host/filename

If the user and password keywords are not specified, the defaults are anonymous and test, respectively.

Examples

In the following example, an FTP operation is configured. Joe is the user and Young is the password. zxq is the host and test is the file name.

```
Router(config)# rtr 3
Router(config-rtr)# type ftp operation get ftp://joe:young@zxq/test
```

Related Commands

Command	Description
show rtr collection-statistics	Displays statistical errors for all SAA operations or the specified operation.
show rtr operational-state	Displays the operational state of all SAA operations or the specified operation.

type http

To configure a Hypertext Transfer Protocol (HTTP) Service Assurance Agent (SAA) operation, use the **type http** command in SAA RTR configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

```
type http operation { get | raw } url url [name-server ip-address] [version version-number]
    [source-ipaddr { name | ip-address }] [source-port port-number] [cache { enable | disable }]
    [proxy proxy-url]
```

```
no type http operation { get | raw } url url [name-server ip-address] [version version-number]
    [source-ipaddr { name | ip-address }] [source-port port-number] [cache { enable | disable }]
    [proxy proxy-url]
```

Syntax Description

operation get	Specifies an HTTP GET operation.
operation raw	Specifies an HTTP RAW operation.
url <i>url</i>	Specifies the URL of destination HTTP server.
name-server	(Optional) Specifies name of destination Domain Name Server.
<i>ip-address</i>	(Optional) IP address of Domain Name Server.
version	(Optional) Specifies version number.
<i>version-number</i>	(Optional) Version number.
source-ipaddr	(Optional) Specifies source name or IP address.
<i>name</i>	Source name.
<i>ip-address</i>	Source IP address.
source-port	(Optional) Specifies source port.
<i>port-number</i>	(Optional) Source port number.
cache	(Optional) Enables or disables download of cached HTTP page.
enable	Enables downloads of cached HTTP page.
disable	Disables download of cached HTTP page.
proxy	(Optional) Proxy information.
<i>proxy-url</i>	(Optional) Proxy information or URL.

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

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

Usage Guidelines

You must configure the type of operation before you can configure any of the other characteristics of the operation.

Examples**HTTP GET operation**

In this example operation 5 is created and configured as an HTTP GET operation. The destination URL is `http://www.cisco.com`.

```
Router(config)# rtr 5
Router(config-rtr)# type http operation get url http://www.cisco.com
Router(config-rtr)# exit
Router(config)# rtr schedule 5 start-time now
```

HTTP RAW operation using RAW submode

In this example operation 6 is created and configured as an HTTP RAW operation. To use the raw request commands, HTTP-RAW submode is entered using the `http-raw-request` command. The RTR HTTP-RAW submode is indicated by the `(config-rtr-http)` router prompt.

```
Router(config)# rtr 6
Router(config-rtr)# type http operation raw url http://www.cisco.com
Router(config-rtr)# http-raw-request
Router(config-rtr-http)# GET /index.html HTTP/1.0\r\n
Router(config-rtr-http)# \r\n
Router(config-rtr-http)# exit
Router(config)# rtr schedule 6 start-time now
```

HTTP RAW operation through a Proxy Server

In this example `http://www.proxy.cisco.com` is the proxy server and `http://www.yahoo.com` is the HTTP Server:

```
Router(config)# rtr 6
Router(config-rtr)# type http operation raw url http://www.proxy.cisco.com
Router(config-rtr)# http-raw-request
Router(config-rtr-http)# GET http://www.example.com HTTP/1.0\r\n
Router(config-rtr-http)# \r\n
Router(config-rtr-http)# exit
Router(config)# rtr schedule 6 start-time now
```

Related Commands

Command	Description
<code>rtr</code>	Specifies an SAA operation and enters SAA RTR configuration mode.

type jitter

To configure a jitter Service Assurance Agent (SAA) operation, use the **type jitter** command in SAA RTR configuration mode. To disable a jitter operation, use the **no** form of this command.

```
type jitter dest-ipaddr {name | ip-address} dest-port port-number [source-ipaddr {name | ip-address}] [source-port port-number] [control {enable | disable}] [num-packets number-of-packets] [interval inter-packet-interval]
```

```
no type jitter dest-ipaddr {name | ip-address} dest-port port-number [source-ipaddr {name | ip-address}] [source-port port-number] [control {enable | disable}] [num-packets number-of-packets] [interval inter-packet-interval]
```

Syntax Description

dest-ipaddr	Destination for the operation.
<i>name</i>	Destination IP host name.
<i>ip-address</i>	Destination IP address.
dest-port	Destination port.
<i>port-number</i>	Port number of the destination port.
source-ipaddr	(Optional) Source IP address.
<i>name</i>	IP host name.
<i>ip-address</i>	IP address.
source-port	(Optional) Source port.
<i>port-number</i>	Port number of the source.
control	(Optional) Combined with the enable or disable keyword, enables or disables sending a control message to the destination port.
enable	Enables the SAA to send a control message to the destination port prior to sending a probe packet. This is the default value.
disable	Disables sending of control messages to the responder prior to sending a probe packet.
num-packets	(Optional) Number of packets, as specified by the number argument. The default value is 10.
<i>number-of-packets</i>	
interval	(Optional) Interpacket interval in milliseconds. The default value of the <i>inter-packet-interval</i> argument is 20 ms.
<i>inter-packet-interval</i>	

Defaults

No SAA operation type is associated with the operation number being configured.

The default for the optional characteristic **request-data-size** for a SAA Jitter operation is 32 bytes of UDP data.

Command Modes

SAA RTR configuration

Command History

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

Usage Guidelines

The **type jitter** command configures a UDP Plus SAA operation. The UDP Plus operation is a superset of the UDP echo operation. In addition to measuring UDP round trip time, the UDP Plus operation measures per-direction packet-loss and jitter (inter-packet delay variance). Packet loss is a critical element in SLAs, and Jitter statistics are useful for analyzing traffic in a VoIP network.

You must enable the SAA RTR Responder on the target router (using the `rtr responder` command) before you can configure a Jitter operation. Prior to sending a operation packet to the responder, the SAA sends a control message to the SAA RTR Responder to enable the destination port.

You must configure the type of operation before you can configure any of the other characteristics of the operation.

Examples

In the following example, operation 6 is created and configured as a Jitter operation using the destination IP address 172.30.125.15, the destination port number 2000, 20 packets, and an interval of 20:

```
Router(config)# rtr 6
Router(config-rtr)# type jitter dest-ip 172.30.125.15 dest-port 2000 num-packets 20 interval 20
```

Related Commands

Command	Description
request-data-size	Sets the payload size for SAA operation requests.
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

type pathEcho

To configure an Internet Protocol/Internet Control Message Protocol (IP/ICMP) Path Echo Service Assurance Agent (SAA) operation, use the **type pathEcho** command in SAA RTR configuration mode. To remove the operation from the configuration, use the **no** form of this command.

type pathEcho protocol ipIcmpEcho { *ip-address* | *ip-hostname* }

no type pathEcho protocol ipIcmpEcho { *ip-address* | *ip-hostname* }

Syntax Description	protocol ipIcmpEcho	Specifies an IP/ICMP Echo operation. This is currently the only protocol type supported for the SAA Path Echo operation.
	<i>ip-address</i>	Specifies the IP address of the target device.
	<i>ip-hostname</i>	Specifies the designated IP name of the target device.

Defaults No SAA operation type is associated with the operation number being configured.

Command Modes SAA RTR configuration

Command History	Release	Modification
	11.2	This command was introduced.

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

Examples In the following example, SAA operation 10 is created and configured as pathEcho probe using the IP/ICMP Echo protocol and the destination IP address 172.16.1.175:

```
Router(config)# rtr 10
Router(config-rtr)# type pathEcho protocol ipIcmpEcho 172.16.1.175
```

Related Commands	Command	Description
		rtr
	show rtr configuration	Displays configuration values for RTR operations (probes).

type pathJitter

To configure an Service Assurance Agent (SAA) Path Jitter monitoring operation, use the **type pathJitter** command in RTR Entry configuration mode. To remove an inactive Path Jitter entry from the RTR configuration, use the **no** form of this command.

```
type pathJitter dest-ipaddress ip-address [source-ipaddress source-ip] [num-packets
packet-number] [interval time-ms] [targetOnly]
```

```
no type pathJitter dest-ipaddress ip-address [source-ipaddress source-ip] [num-packets
packet-number] [interval time-ms] [targetOnly]
```

Syntax Description		
dest-ipaddress <i>ip-address</i>	Specifies the destination (target) IP address or host name.	
source-ipaddress <i>source-ip</i>	(Optional) Specifies the source IP address that will be used for the operational probe packets.	
num-packets <i>packet-number</i>	(Optional) The number of packets to be transmitted in each operation. The default value is 10.	
interval <i>time-ms</i>	(Optional) Time interval between packets (in milliseconds). The default value is 20 ms.	
targetOnly	(Optional) Sends test packets to the destination only (path is not traced).	

Defaults

No SAA operation type is associated with the operation number being configured.

Command Modes

SAA RTR configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The Path Jitter SAA operation traces a specified IP path from the source to the destination and then sends a specified number of packets to each hop along the traced path. Optionally, the time interval between each test packet can be specified.

If the number of packets and the time interval are not specified, the path jitter operation will use the default values.

If the **targetOnly** keyword is not used, the path jitter operation will trace the “hop-by-hop” IP path from the source to the destination and send the specified number of test packets to each hop along the trace path, using the specified time interval between each test packet.

If the **targetOnly** keyword is used, the command will cause the pathJitter operation to send echos to the destination only (the path from the source to the destination is not traced).

Examples

The following example enables the Path Jitter operation to trace the IP path to the destination 172.69.1.129 and send ten test packets to each hop with an interval of 20 ms between each test packet:

```
Router# config terminal  
Router(config)# rtr 1  
Router(config-rtr)# type pathJitter dest-ipaddr 172.69.1.129
```

The following example enables the Path Jitter operation to send 50 test packets to 172.69.5.6 with an interval of 30 ms between each test packet:

```
Router# config terminal  
Router(config)# rtr 2  
Router(config-rtr)# type pathJitter 172.69.5.6 num-packets 50 interval 30 targetOnly
```

type slm controller

To configure a Service Assurance Agent (SAA) operation as an SLM interface operation, and to specify the interface that the operation should be run on, use the **type slm controller** command in SAA RTR configuration mode. To remove or replace a previously configured SAA operation, use the **no rtr operation-number** global configuration command.

type slm controller *controller-id*

Syntax Description	<i>controller-id</i>	The controller type and slot/port number. Valid controller types include E1 , E3 , T1 , and T3 .
---------------------------	----------------------	--

Defaults	No SAA operation type is associated with the operation number being configured.
-----------------	---

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

Command History	Release	Modification
	12.2(15)T	This command was introduced for T3 and E3 controllers using ATM. This command replaces the type t1-slm command.
	12.3(1)	Support for controllers configured for Frame Relay was added.

Usage Guidelines	This SAA RTR configuration command specifies that the operation is an SLM physical controller operation, which provides information about the data link layer connection, and specifies the controller that the operation should be run on.
-------------------------	---

Controllers that can be monitored using this operation include T1, E1, T3, and E3.

The specified controller should be configured for Frame Relay or ATM.

Examples	In the following example, SAA operation 1 is configured as an SLM controller operation:
-----------------	---

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line.
Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 1
Router(config-rtr)# type slm controller T1 0
Router(config-rtr-slm-if)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-if)# exit
Router(config)# rtr schedule 1 start-time now life forever
Router(config)# end
Router#
Router# show rtr configuration 1 | include Type
Type of operation to perform: slm controller
Reaction Type: None
Router#
```

Related Commands

Command	Description
rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.
show rtr enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.
type slm interface	Specifies that the SAA operation is an SLM interface operation, and specifies the interface that the operation should be run on.

type slm frame-relay interface

To configure a Service Assurance Agent (SAA) operation as an Service Level Management (SLM) Frame Relay (FR) interface operation, and to specify the interface that the operation should be run on, use the **type slm frame-relay interface** command in SAA RTR configuration mode. To remove or replace a previously configured SAA operation, use the **no rtr operation-number** global configuration command.

type slm frame-relay interface *interface-type interface-number*

Syntax Description	<i>interface-type</i> <i>interface-number</i>	The interface type (Serial) and number. An intervening space is not required.
---------------------------	--	--

Defaults	No SAA operation type is associated with the operation number being configured.
-----------------	---

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

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

Usage Guidelines

The SAA SLM FR interface operation provides Frame Relay link (Layer 2) layer data. The **type slm frame-relay interface** command specifies the operation type and the interface that the operation should be run on. The specified interface should be configured for Frame Relay.

Frame Relay interface link statistics are used to monitor the basic health of a Frame Relay interface. This information includes some traffic counters, assorted error counts, and some performance-related counters.

To view the gathered statistics, use the **show rtr enhanced-history distribution-statistics** command or the **show rtr enhanced-history collection-statistics** command. Statistics gathered with this operation can also be retrieved from external network monitoring applications via the CNS event gateway.

Examples

In the following example, SAA operation 2 is configured as an SLM Frame Relay Interface operation:

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line.
Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 2
Router(config-rtr)# type slm frame-relay interface Serial10:0
Router(config-rtr-slm-fr-if)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-fr-if)# exit
Router(config)# rtr schedule 2 start-time now life forever
Router(config)# end
Router#
Router# show rtr configuration 2 | include Type
```

Type of operation to perform: Slm Frame-relay Interface
 Reaction Type: None

Related Commands	Command	Description
	rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
	show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.
	show rtr enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.

type slm frame-relay pvc interface

To configure an Service Assurance Agent (SAA) operation as an Service Level Management (SLM)Frame Relay (FR) Circuit operation, and specify the interface that the operation should be run on, use the **type slm frame-relay pvc interface** command in SAA RTR configuration mode. To remove or replace a previously configured SAA operation, use the **no rtr operation-number** global configuration command.

type slm frame-relay pvc interface *interface-type interface-number dlci-number*

Syntax Description		
<i>interface-type</i>		The interface type (Serial) and number. An intervening space is not required.
<i>interface-number</i>		
<i>dlci-number</i>		Data link connection identifier (DLCI) of the permanent virtual circuit (PVC) to be monitored.

Defaults No SAA operation type is associated with the operation number being configured.

Command Modes SAA RTR configuration mode

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

Usage Guidelines This command specifies that the operation is an SAA SLM FR circuit operation, which provides data for the specified circuit. The specified interface should be configured with a permanent virtual circuit (PVC) connection.

The Frame Relay circuit statistics are used to monitor the basic health of a Frame Relay circuit. This information includes some traffic counters, assorted error counts, and some performance-related counters.

This command puts the CLI into SAA SLM FR Circuit configuration mode (config-rtr-slm-fr-dlci).

Examples In the following example, SAA operation 3 is configured as an SLM Frame Relay Circuit (or PVC) operation:

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line.
Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 3
Router(config-rtr)# type slm frame-relay pvc interface Serial0:0 111
Router(config-rtr-slm-fr-dlci)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-fr-dlci)# exit
Router(config)# rtr schedule 3 start-time now life forever
Router(config)# end
```

```
Router#
Router# show rtr configuration 3 | include Type
Type of operation to perform: Slm Frame-relay Pvc
Reaction Type: None
```

Related Commands

Command	Description
rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.
show rtr enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.

type slm interface

To configure a Service Assurance Agent (SAA) operation as an Service Level Management (SLM) interface operation, and to specify the interface that the operation should be run on, use the **type slm interface** command in SAA RTR configuration mode. To remove or replace a previously configured SAA operation, use the **no rtr operation-number** global configuration command.

type slm interface *type number*

Syntax Description	<i>type number</i>	The interface type and number. Interface types include Serial and FR-ATM . Alternatively, an Inverse Multiplexing over ATM (IMA) group number can be specified.
---------------------------	--------------------	---

Defaults No default behavior or values.

Command Modes SAA RTR configuration

Command History	Release	Modification
	12.2(11)T	This command was introduced to support ATM SLM operations.
	12.2(13)T	This command was updated to support T1 IMA (ATM) interfaces.
	12.3(1)	This command was updated to support FR SLM operations (Serial interfaces).

Usage Guidelines The **type slm interface** SAA RTR configuration command specifies that the operation is an SLM physical interface operation, which provides information about the data link layer connection. The specified interface should be configured for Frame Relay or ATM.

Interfaces that can be monitored using this operation include Serial or HSSI (high speed serial interface) for Frame Relay interfaces, and IMA for ATM interfaces. To specify an HSSI interface, use the **Serial** keyword as the *type*.

In order for this operation to work, either the **atm slm statistics** global configuration command or the **rtr slm frame-relay statistics** global configuration command must be enabled on the device.

This command puts the CLI into SAA SLM controller/interface configuration mode, in which you can configure optional characteristics for the operation. To view the available options, enter the **?** command at the (config-rtr-slm-if) prompt.

Examples In the following example, SAA operation 1 is configured as an SLM interface operation for a Frame Relay interface:

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line.
```

```

Router(config)# rtr slm frame-relay statistics
Router(config)# rtr 1
Router(config-rtr)# type slm interface Serial 0.1
Router(config-rtr-slm-if)# enhanced-history interval 900 buckets 100
Router(config-rtr-slm-if)# exit
Router(config)# rtr schedule 1 start-time now life forever
Router(config)# end
Router#
Router# show rtr configuration 1 | include Type
Type of operation to perform: slm interface
Reaction Type: None
Router#

```

Related Commands

Command	Description
rtr	Allows configuration of SAA operations by entering SAA RTR configuration mode for the specified operation number.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified SAA operation, with data for each bucket shown individually.
show rtr enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.
type slm controller	Specifies that the SAA operation is an SLM controller operation, and specifies the controller that the operation should be run on.

type tcpConnect

To define a tcpConnect probe, use the **type tcpConnect** command in Service Assurance Agent (SAA) RTR configuration mode. To remove the type configuration for the probe, use the **no** form of this command.

```
type tcpConnect dest-ipaddr {name | ip-address} dest-port port-number [source-ipaddr {name | ip-address} source-port port-number] [control {enable | disable}]
```

```
no type tcpConnect dest-ipaddr {name | ip-address} dest-port port-number
```

Syntax Description	
dest-ipaddr <i>name</i> <i>ip-address</i>	Destination of tcpConnect probe. <i>name</i> indicates IP host name. <i>ip-address</i> indicates IP address.
dest-port <i>port-number</i>	Destination port number.
source-ipaddr <i>name</i> <i>ip-address</i>	(Optional) Source IP host name or IP address.
source-port <i>port-number</i>	(Optional) Port number of the source. When a port number is not specified, SAA picks the best IP address (nearest to the target) and available User Datagram Protocol (UDP) port.
control	(Optional) Specifies that the SAA control protocol should be used when running this probe. The control protocol is required when the probe's target is a Cisco router that does not natively provide the service (TCP service in this case). Combined with the enable or disable keyword, enables or disables sending a control message to the destination port. The default is that the control protocol is enabled. When enabled, the SAA sends a control message to the SAA Responder (if available) to enable the destination port prior to sending a probe packet.
enable	Enables the SAA collector to send a control message to the destination port prior to sending a probe packet. This is the default.
disable	Disables the SAA from sending a control message to the target prior to sending a probe packet.

Defaults No SAA operation type is associated with the operation number being configured.

Command Modes SAA RTR configuration

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

Usage Guidelines You must configure an SAA operation type before you can configure any of the other characteristics of the operation.

The Transmission Control Protocol (TCP) Connection operation is used to discover the time it takes to connect to the target device. This operation can be used to test virtual circuit availability or application availability. If the target is a Cisco router, then SA Agent makes a TCP connection to any port number specified by the user. If the destination is a non-Cisco IP host, then the user must specify a known target port number (for example, 21 for FTP, 23 for Telnet, or 80 for HTTP Server). This operation is useful in testing Telnet or HTTP connection times.

Examples

In the following example, SAA operation 11 is created and configured as a tcpConnect probe using the destination IP address 172.16.1.175, and the destination port 2400:

```
Router(config)# rtr 11
Router(config-rtr)# type tcpConnect dest-ipaddr 172.16.1.175 dest-port 2400
```

Related Commands

Command	Description
rtr	Specifies an SAA operation begins configuration for that operation.
show rtr configuration	Displays configuration values for SAA operations.

type udpEcho

To define a udpEcho probe, use the **type udpEcho** command in Service Assurance Agent (SAA) RTR configuration mode. To remove the type configuration for the probe, use the **no** form of this command.

```
type udpEcho dest-ipaddr {name | ip-address} dest-port port-number [source-ipaddr {name | ip-address} source-port port-number] [control {enable | disable}]
```

```
no type udpEcho dest-ipaddr {name | ip-address} dest-port port-number
```

Syntax Description		
dest-ipaddr name ip-address		Destination of the udpEcho probe. Use an IP host name or IP address.
dest-port port-number		Destination port number. The range of port numbers is from 1 to 65,535.
source-ipaddr name ip-address		(Optional) Source IP host name or IP address.
source-port port-number		(Optional) Port number of the source. When a port number is not specified, SAA picks the best IP address (nearest to the target) and available User Datagram Protocol (UDP) port.
control		(Optional) Specifies that the SAA RTR control protocol should be used when running this probe. The control protocol is required when the probe's target is a Cisco router that does not natively provide the service (UDP service in this case). Combined with the enable or disable keyword, enables or disables sending of a control message to the destination port. The default is that the control protocol is enabled.
enable		Enables the SAA collector to send a control message to the destination port prior to sending a probe packet. This is the default.
disable		Disables the SAA from sending a control message to the responder prior to sending a probe packet.

Defaults No SAA operation type is associated with the operation number being configured.

Command Modes SAA RTR configuration

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

Usage Guidelines You must configure an operation type before you can configure any of the other characteristics of the operation.

The source IP address and port number are optional. If they are not specified, SAA selects the IP address nearest to the target and an available UDP port.

Examples

In the following example, SAA operation 12 is created and configured as udpEcho probe using the destination IP address 172.16.1.175 and destination port 2400:

```
Router# configure terminal
Router(config)# rtr 12
Router(config-rtr)# type udpEcho dest-ipaddr 172.16.1.175 dest-port 2400
```

Related Commands

Command	Description
rtr	Specifies an SAA operation and enters SAA RTR configuration mode.
show rtr configuration	Displays configuration values for SAA operations.

undelete

To recover a file marked “deleted” on a Class A Flash file system, use the **undelete** command in EXEC mode.

```
undelete index [filesystem:]
```

Syntax Description	<i>index</i>	A number that indexes the file in the dir command output.
	<i>filesystem:</i>	(Optional) A file system containing the file to undelete, followed by a colon.

Defaults The default file system is the one specified by the **cd** command.

Command Modes EXEC

Command History	Release	Modification
	11.0	This command was introduced for Class A Flash File Systems (platforms include the Cisco 7500 series and Cisco 12000 series).

Usage Guidelines For Class A Flash file systems, when you delete a file, the Cisco IOS software simply marks the file as deleted, but it does not erase the file. This command allows you to recover a “deleted” file on a specified Flash memory device. You must undelete a file by its index because you could have multiple deleted files with the same name. For example, the “deleted” list could contain multiple configuration files with the name router-config. You undelete by index to indicate which of the many router-config files from the list to undelete. Use the **dir** command to learn the index number of the file you want to undelete.

You cannot undelete a file if a valid (undeleted) file with the same name exists. Instead, you first delete the existing file and then undelete the file you want. For example, if you had an undeleted version of the router-config file and you wanted to use a previous, deleted version instead, you could not simply undelete the previous version by index. You would first delete the existing router-config file and then undelete the previous router-config file by index. You can delete and undelete a file up to 15 times.

On Class A Flash file systems, if you try to recover the configuration file pointed to by the CONFIG_FILE environment variable, the system prompts you to confirm recovery of the file. This prompt reminds you that the CONFIG_FILE environment variable points to an undeleted file. To permanently delete all files marked “deleted” on a Flash memory device, use the **squeeze** EXEC command.

For further information on Flash File System types (classes), see <http://www.cisco.com/warp/public/63/pcmciatrix.html>.

Examples The following example recovers the deleted file whose index number is 1 to the Flash memory card inserted in slot 0:

```
Router# undelete 1 slot0:
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.

upgrade rom-monitor file

To reload the Upgrade ROMmon image on a Cisco 7200 VXR or Cisco 7301 router, use the **upgrade rom-monitor file** command in Privileged EXEC mode.

For the Cisco 7200 VXR router using the NPE-G1, the syntax is:

```
upgrade rom-monitor file { bootflash [file-path] | disk0 [file-path] | disk1 [file-path] | disk2 [file-path] | flash [file-path] | ftp [file-path] | slot0 [file-path] | slot1 [file-path] | tftp [file-path] }
```

For the Cisco 7301 router, the syntax is:

```
upgrade rom-monitor file { flash [file-path] | ftp [file-path] | disk0 [file-path] | tftp [file-path] }
```

Syntax Description		
<i>file-path</i>		Directory path name or filename where the Upgrade ROMmon image is located.
bootflash		Filename location of Upgrade ROMmon image in boot flash memory.
disk0		Disk 0 is only present on a Cisco 7200 VXR that has an I/O controller and is always present on the Cisco 7301 router. The filename location of the Upgrade ROMmon image in disk 0 of the router chassis.
disk1		Disk 1 is only present on a Cisco 7200 VXR that has an I/O controller. The filename location of the Upgrade ROMmon image in disk 1 of the router chassis.
disk2		Disk 2 is always present on a Cisco 7200 VXR. The filename location of the Upgrade ROMmon image in disk 2 of the router chassis.
flash		Filename location of Upgrade ROMmon image in Flash memory.
ftp		Filename location of the Upgrade ROMmon image using File Transfer Protocol (FTP).
slot0, slot1		Slot 0 and slot 1 are only present on a Cisco 7200 VXR that has an I/O controller. The filename location of the Upgrade ROMmon image in slot 0 and slot 1 of the router chassis.
tftp		Filename location of the Upgrade ROMmon image on the TFTP server.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(28)S	This command was introduced on 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.
	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

A Cisco 7200 VXR that has an I/O controller card installed has the following additional devices on its chassis: disk 0, disk 1, slot 0, and slot 1.

Examples

The following example of a Cisco 7200 VXR using an I/O controller loads the Upgrade ROMmon image from a disk 1 filename:

```
Router# upgrade rom-monitor file disk1:C7200_NPEG1_RMFUR.srec.123-4r.T1
This command will reload the router. Continue? [yes/no]:yes
ROMMON image upgrade in progress.

Erasing boot flash eeeeeeeeeeeeeeeeeee
Programming boot flash pppppp
Now Reloading via hard watchdog timeout
```

The following example on a Cisco 7301 router loads the Upgrade ROMmon image from a specified TFTP file location:

```
Router# upgrade rom-monitor file tftp://00.0.00.0/biff/C7301_RMFUR.srec
Loading biff/C7301_RMFUR.srec from 00.0.00.0 (via GigabitEthernet0/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 392348 bytes]
```

```
This command will reload the router. Continue? [yes/no]:yes
ROMMON image upgrade in progress.
Erasing boot flash eeeeeeeeeeeeeeeeeee
Programming boot flash ppppp
Now Reloading via hard watchdog timeout
```

```
Unexpected exception, CP
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by cisco Systems, Inc.
```

Running new upgrade for first time

```
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by cisco Systems, Inc.
```

```
ROM:Rebooted by watchdog hard reset
C7301 platform with 1048576 Kbytes of main memory
```

```
Upgrade ROMMON initialized
rommon 1 >
```

upgrade rom-monitor preference

To select a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR or Cisco 7301router, use the **upgrade rom-monitor preference** command in privileged EXEC mode.

upgrade rom-monitor preference [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 Privileged EXEC

Command History	Release	Modification
	12.0(28)S	This command was introduced on 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.
	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 After running the **upgrade rom-monitor preference** command, you must reload the router for the selected ROMmon image to take effect.

Use the **rommon-pref** command when you are in ROMmon mode.

Examples The following example applicable to both the Cisco 7200 VXR and Cisco 7301 routers selects the ReadOnly ROMmon image to be booted on the next reload of the router:

```
Router# upgrade rom-monitor preference readonly
You are about to mark ReadOnly region of ROMMON for the highest boot preference.
Proceed? [confirm]
Done! Router must be reloaded for this to take effect.
```

Related Commands	Command	Description
	rommon-pref	Selects a ReadOnly or Upgrade ROMmon image to be booted on the next reload when you are in ROMmon mode.

vacant-message

To display an idle terminal message, use the **vacant-message** command in line configuration mode. To remove the default vacant message or any other vacant message that may have been set, use the **no** form of this command.

vacant-message [*d message d*]

no vacant-message

Syntax Description

<i>d</i>	(Optional) Delimiting character that marks the beginning and end of the vacant-message. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), or tilde (~). ^C is reserved for special use and should not be used in the message.
<i>message</i>	(Optional) Vacant terminal message.

Defaults

The format of the default vacant message is as follows:

```
<blank lines>
hostname tty# is now available
<blank lines>
Press RETURN to get started.
```

This message is generated by the system.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command enables the banner to be displayed on the screen of an idle terminal. The **vacant-message** command without any arguments restores the default message.

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.



Note

For a rotary group, you need to define only the message for the first line in the group.

Examples

The following example turns on the system banner and displays this message:

```
line 0
vacant-message #
    Welcome to Cisco Systems, Inc.
    Press Return to get started.
```

verify

To verify the checksum of a file on a Flash memory file system, use the **verify** command in EXEC mode.

```
verify [/md5 [md5-value]] filesystem:[file-url]
```

Syntax Description		
/md5	(Optional) Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.	
<i>md5-value</i>	(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system will calculate the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.	
<i>filesystem:</i>	(Optional) File system or directory containing the files to list, followed by a colon. Standard file system keywords for this command are flash: and bootflash: .	
<i>file-url</i>	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.	

Defaults The current working device is the default device (file system).

Command Modes EXEC

Command History	Release	Modification
	11.0	This command was introduced.
	12.2(4)T	The /md5 keyword was added.

Usage Guidelines This command replaces the **copy verify** and **copy verify flash** commands.

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory; it is not displayed when the image file is copied from one disk to another.

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into Flash memory or onto a server. A variety of image information is available on Cisco.com. For example, you can get the Release, Feature Set, Size, BSD Checksum, Router Checksum, MD5, and Publication Date information by clicking on the image file name prior to downloading it from the Software Center on Cisco.com.

To display the contents of Flash memory, use the **show flash** command. The Flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into Flash memory, use the **verify** command. Note, however, that the **verify**

command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the router and saved in the file system without detection. If a corrupt image is transferred successfully to the router, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **/md5** option of the **verify** command allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

To perform the MD5 integrity check, execute the **verify** command using the **/md5** keyword. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /md5** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /md5 8b5f3062c4caeccae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Examples

In the following example, the **verify** command is used to check the integrity of the file c7200-js-mz on the Flash memory card inserted in slot 0:

```
Router# dir slot0:
Directory of slot0:/
 1 -rw-      4720148   Aug 29 1997 17:49:36 hampton/nitro/c7200-j-mz
 2 -rw-      4767328   Oct 01 1997 18:42:53 c7200-js-mz
 5 -rw-         639   Oct 02 1997 12:09:32 rally
 7 -rw-         639   Oct 02 1997 12:37:13 the_time

20578304 bytes total (3104544 bytes free)
Router# verify slot0:c7200-js-mz
Verified slot0:c7200-js-mz
```

In the following example, the **/md5** keyword is used to display the MD5 value for the image:

```
Router# verify /md5 disk1:
Verify filename []? c7200-js-mz
.....
.....
.....
.....
.....
.....Done!
verify /md5 (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

In the following example, the known MD5 value for the image (obtained from Cisco.com) is specified in the **verify** command, and the system checks the value against the stored value:

```
Router# verify /md5 disk1:c7200-js-mz ?
WORD Expected md5 signature
<cr>
router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3
.....
.....
```

```
.....  
.....  
.....  
.....Done!  
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the cd command.
show file systems	Lists available file systems.

verify-data

To cause the Service Assurance Agent (SAA) operation to check each response for corruption, use the **verify-data** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

verify-data

no verify-data

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes SAA RTR configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Only use the **verify-data** command when corruption may be an issue.



Caution

Do not enable this feature during normal operation because it causes unnecessary overhead.

Examples In the following example, operation 5 is configured to verify the data for each response:

```
Router(config)# rtr 5
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.174
Router(config-rtr)# response-data-size 2
Router(config-rtr)# verify-data
```

Related Commands	Command	Description
	rtr	Specifies an SAA operation and enters SAA RTR configuration mode.

vrf (SAA)

To allow monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using Service Assurance Agent (SAA) operations, use the **vrf** command in RTR Entry configuration mode.

```
vrf vrf-name
```

Syntax Description

<i>vrf-name</i>	Name of the VRF.
-----------------	------------------

Defaults

No default behavior or values.

Command Modes

SAA (RTR Entry) configuration mode

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

If the **vrf** command is configured for an SAA operation, the SAA uses *vrf-name* to identify the VRF for this operation. This command should only be used if it is necessary to measure the response time over the VPN tunnel.

Examples

The following examples illustrate how to set up different SAA operations that support MPLS VPNs. These examples show how test traffic can be sent in an already existing VPN tunnel between two endpoints. Only the following operations can measure response time of a VPN tunnel.

Note that for all of the following operation types, the source IP address is not specified. The SAA will automatically specify the correct source interface when the **vrfName** command is used.

Configuring an Echo Operation Example

```
rtr 1
  type echo protocol ipIcmpEcho 1.1.1.1
  vrf vpn1
end
rtr schedule 1 start now
```

Configuring a Path Echo Operation Example

```
rtr 1
  type pathEcho protocol ipIcmpEcho 1.1.1.1
  vrfName vpn1
rtr schedule 1 start now
```

Configuring a UDP Echo Operation Example

```
rtr 1
```

```
type udpEcho dest-ipaddr 1.1.1.1 dest-port 1213
vrf vpn1
rtr schedule 1 start now
```

Configuring a Jitter Operation Example

```
rtr 1
type jitter dest-ipaddr 1.1.1.1 dest-port 1213
vrf vpn1
rtr schedule 1 start now
```

Related Commands

Command	Description
type echo	Configures an SAA Echo operation.

where

To list the open sessions, use the **where** command in EXEC mode.

where

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.

Usage Guidelines The **where** command displays all open sessions associated with the current terminal line. The break (Ctrl-Shift-6, x), **where**, and **resume** commands are available with all supported connection protocols.

Examples The following is sample output from the **where** command:

```
Router# where
Conn Host          Address           Byte   Idle  Conn Name
  1 MATHOM          192.31.7.21      0      0    MATHOM
* 2 CHAFF          131.108.12.19   0      0    CHAFF
```

The asterisk (*) indicates the current terminal session.

[Table 135](#) describes the fields shown in the display.

Table 135 *where* Field Descriptions

Field	Description
Conn	Name or address of the remote host to which the connection is made.
Host	Remote host to which the router is connected through a Telnet session.
Address	IP address of the remote host.
Byte	Number of unread bytes for the user to see on the connection.
Idle	Interval (in minutes) since data was last sent on the line.
Conn Name	Assigned name of the connection.

Related Commands	Command	Description
	show line	Displays information about all lines on the system or the specified line.
	show sessions	Displays information about open LAT, Telnet, or rlogin connections.

width

To set the terminal screen width, use the **width** command in line configuration mode. To return to the default screen width, use the **no** form of this command.

width *characters*

no width

Syntax Description	<i>characters</i>	Number of character columns displayed on the terminal. The default is 80 characters.
--------------------	-------------------	--

Defaults	80 character columns
----------	----------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	By default, the route provides a screen display width of 80 characters. You can reset this value for the current session if it does not meet the needs of your terminal. The rlogin protocol uses the value of the <i>characters</i> argument to set up terminal parameters on a remote host.
------------------	--

Examples	In the following example the location for line 7 is defined as “console terminal” and the display is set to 132 columns wide:
----------	---

```
Router(config)# line 7
Router(config-line)# location console terminal
Router(config-line)# width 132
```

Related Commands	Command	Description
	terminal width	Sets the number of character columns on the terminal screen for the current session.

write core

To test the configuration of a core dump setup, use the **write core** command in privileged EXEC mode.

write core [*hostname* [LINE] | *destination-address* [LINE]]

Syntax Description

<i>hostname</i>	(Optional) Host name of the remote server where the core dump file is to be written.
<i>destination-address</i>	(Optional) IP address of the remote server where the core dump file is to be written.
LINE	(Optional) Assigns the name “LINE” to the core dump file.

Defaults

If the *hostname* or *destination* arguments are not specified, the core dump file is written to the IP address or hostname specified by the **exception dump** command.

If the **LINE** keyword is not specified, the name of the core dump file is assigned as the host name of the remote server followed by the word “-core.”

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

When a router reloads, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the reload. Core dumps are generally useful to your technical support representative. Not all types of router reloads will produce a core dump.

The **write core** command causes the router to generate a core dump without reloading, which may be useful if the router is malfunctioning but has not reloaded. The core dump files will be the size of the respective memory regions. It is important to remember that the entire memory region is dumped, not just the memory that is in use.



Caution

Use the **write core** command only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. When using this command, the router will not reload until the content of its memory is dumped. This event might take some time, depending on the amount of DRAM present on the router. Also, the resulting binary file, which is very large, must be transferred to a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel who have access to source code and detailed memory maps.

Depending on your TFTP server, you might need to create an empty target file to which the router can write the core dump.

Examples

The following example shows how to test the configuration of a core dump setup. In this example, the core dump file is written to the remote server with the host name test.

```
write core test
```

write erase

The **write erase** command is replaced by the **erase nvram:** command. See the description of the **erase** command for more information.

write memory

The **write memory** command has been replaced by the **copy system:running-config nvram:startup-config** command. See the description of the **copy** command for more information.

write mib-data

To save MIB Persistence configuration data to NVRAM, use the **write mib-data** command in EXEC mode.

write mib-data

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.2(4)T	This command was introduced.

Usage Guidelines Any modified MIB data must be written to NVRAM memory using the **write mib-data** command. If the **write mib-data** command is not used, modified MIB data is not saved automatically.

Examples The following example enables Event MIB Persistence and writes MIB data to NVRAM:

```
Router(config)# snmp mib persist event
Router(config)# end
Router# write mib-data
```

Related Commands	Command	Description
	snmp mib persist	Enables MIB persistence.

write network

The **write network** command is replaced by the **copy system:running-config *destination-url***. See the description of the **copy** command for more information.

write terminal

The **more system:running-config** command is replaced by the **write terminal** command. See the description of the **more** command for additional information.

xmodem

To copy a Cisco IOS image to a router using the ROM monitor and the Xmodem or Ymodem protocol, use the **xmodem** command in ROM monitor mode.

```
xmodem [-c] [-y] [-e] [-f] [-r] [-x] [-s data-rate] [filename]
```

Syntax Description	
-c	(Optional) CRC-16 checksumming, which is more sophisticated and thorough than standard checksumming.
-y	(Optional) Uses the Ymodem protocol for higher throughput.
-e	(Optional) Erases the first partition in Flash memory before starting the download. This option is only valid for the Cisco 1600 series.
-f	(Optional) Erases all of Flash memory before starting the download. This option is only valid for the Cisco 1600 series.
-r	(Optional) Downloads the file to DRAM. The default is Flash memory.
-x	(Optional) Do not execute Cisco IOS image on completion of the download.
-s <i>data-rate</i>	(Optional) Sets the console port's data rate during file transfer. Values are 1200 , 2400 , 4800 , 9600 , 19200 , 38400 , and 115200 bps . The default rate is specified in the configuration register. This option is only valid for the Cisco 1600 series.
<i>filename</i>	(Optional) Filename to copy. This argument is ignored when the -r keyword is specified, because only one file can be copied to DRAM. On the Cisco 1600 series routers, files are loaded to the ROM for execution.

Defaults Xmodem protocol with 8-bit CRC, file downloaded into Flash memory and executed on completion.

Command Modes ROM monitor

Command History	Release	Modification
	11.2 P	This command was introduced.

Usage Guidelines The Cisco 3600 series routers does not support XBOOT functionality. If your Cisco IOS image is erased or damaged, you cannot load a new image over the network.

Use the **xmodem** ROM monitor command to download a new system image to your router from a local personal computer (such as a PC, Mac, or UNIX workstation), or a remote computer over a modem connection, to the router's console port. The computer must have a terminal emulation application that supports these protocols.

Cisco 3600 Series Routers

Your router must have enough DRAM to hold the file being transferred, even if you are copying to Flash memory. The image is copied to the first file in internal Flash memory. Any existing files in Flash memory are erased. There is no support for partitions or copying as a second file.

Cisco 1600 Series Routers

If you include the **-r** option, your router must have enough DRAM to hold the file being transferred. To run from Flash, an image must be positioned as the first file in Flash memory. If you are copying a new image to boot from Flash, erase all existing files first.

**Caution**

A modem connection from the telephone network to your console port introduces security issues that you should consider before enabling the connection. For example, remote users can dial in to your modem and access the router's configuration settings.

**Note**

If the file to be downloaded is not a valid router image, the copy operation is automatically terminated.

Examples

The following example uses the **xmodem -c filename** ROM monitor command to copy the file named **new-ios-image** from a remote or local computer:

```
rommon > xmodem -c new-ios-image

Do not start the sending program yet...
      File size      Checksum   File name
1738244 bytes (0x1a8604)  0xdd25  george-admin/c3600-i-mz

WARNING: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: yes
Ready to receive file new-ios-image ...
```

Related Commands

Command	Description
copy xmodem:	Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Xmodem protocol.
copy ymodem:	Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Ymodem protocol.

xsm

To enable XML Subscription Manager (XSM) client access to the device, use the **xsm** command in global configuration mode. To disable XSM client access to the device, use the **no** form of this command.

xsm

no xsm

Syntax Description This command has no arguments or keywords.

Defaults XSM client access to the device is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines This command requires that the **ip http server** command is enabled. Enabling the **xsm** command also enables the **xsm vdm** and **xsm edm** commands. This command must be enabled for the XSM client (such as VPN Device Manager [VDM]) to operate.

Examples In the following example, access by remote XSM clients to XSM data on the device is disabled:

```
Router# no xsm
```

Related Commands	Command	Description
	ip http server	Enables a device to be reconfigured through the Cisco browser interface.
	show xsm status	Displays information and status about clients subscribed to the XSM server.
	show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.
	xsm dvdm	Grants access to switch operations.
	xsm edm	Grants access to EDM monitoring and configuration data.
	xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm dvdm

To enable switch-specific configuration data (for example, configuring switch ports and VLANs) when running VPN Device Manager (VDM) on a switch, use the **xsm dvdm** command in global configuration mode. To disable switch-specific configuration data for VDM, use the **no** form of this command.

xsm dvdm

no xsm dvdm

Syntax Description This command has no arguments or keywords.

Defaults Access to switch-specific configuration data is enabled when XSM is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(9)YO1	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Access to switch-specific configuration data (dVDM) is enabled by default when XSM is enabled. The **no xsm dvdm** command allows you to disable only switch-specific XSM data. Note however that disabling dVDM will prevent the VDM application from communicating properly with the device (switch). There is minimal performance impact associated with leaving dVDM enabled.

Examples In the following example, access to switch-specific configuration data is disabled in XSM:

```
Router(config)# no xsm dvdm
```

Related Commands	Command	Description
	xsm	Enables XSM client access to the router.
	xsm edm	Grants access to EDM monitoring and configuration data.
	xsm history vdm	Enables specific VPN statistics collection on the XSM server.
	xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm edm

To grant access to Embedded Device Manager (EDM) monitoring and configuration data, use the **xsm edm** command in global configuration mode. To cancel access to EDM monitoring and configuration data, use the **no** form of this command.

xsm edm

no xsm edm

Syntax Description

This command has no arguments or keywords.

Defaults

Access to EDM monitoring and configuration data is granted by default if XSM is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command exists to allow you to disable EDM using the **no xsm edm** form of the command. EDM is enabled by default when XSM is enabled.

EDM provides the following generic information to the VPN Device Manager (VDM):

- Relevant interfaces
- IP routing
- Access-list details
- Basic device health

Note that disabling EDM prevents XSM clients (such as VDM) from working properly and also disables the **xsm history edm** command. There is minimal performance impact associated with leaving EDM enabled.

Examples

In the following example, access to EDM data is disabled:

```
Router(config)# xsm
Router(config)# no xsm edm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm dvdm	Grants access to switch operations.
xsm history edm	Enables statistics collection for the EDM on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm history edm

To enable statistics collection for the Embedded Device Manager (EDM) on the XML Subscription Manager (XSM) server, use the **xsm history edm** command in global configuration mode. To disable statistics collection for the EDM on the XSM server, use the **no** form of this command.

xsm history edm

no xsm history edm

Syntax Description This command has no arguments or keywords.

Defaults EDM statistics collection is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Use this command to save up to five days of data. Historical information on items such as RAM and CPU utilization is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data, as the XSM server does not save this data between reloads.

Examples In the following example, statistics collection for the EDM is enabled on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history edm
```

Related Commands	Command	Description
	xsm	Enables XSM client access to the router.
	xsm edm	Grants access to EDM monitoring and configuration data.
	xsm history vdm	Enables specific VPN statistics collection on the XSM server.

xsm history vdm

To enable specific VPN statistics collection on the XML Subscription Manager (XSM) server, use the **xsm history vdm** command in global configuration mode. To disable collection of specific selected VPN statistics on the XSM server, use the **no** form of this command.

xsm history vdm

no xsm history vdm

Syntax Description This command has no arguments or keywords.

Defaults VPN statistics collecting is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

With this command enabled, you can save up to five days of data. Historical information on items such as the number of active IKE tunnels, IPsec tunnels, total crypto throughput, and total throughput is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data. The XSM server does not save history data across reloads.

Examples

The following example shows how to enable specific VPN statistics collection on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history vdm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm history edm	Enables statistics collection for the EDM on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm privilege configuration level

To enable the XML Subscription Manager (XSM) configuration privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege configuration level** command in global configuration mode. To remove a previously configured XSM configuration privilege level, use the **no** form of this command.

xsm privilege configuration level *number*

no xsm privilege configuration level *number*

Syntax Description	<i>number</i>	Privilege level. Valid values are from 1 to 15. The default is 15.
---------------------------	---------------	--

Defaults	Level 15
-----------------	----------

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

Command History	Release	Modification
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The privilege level for the **xsm privilege configuration level** command must be greater than or equal to the privilege level for the **xsm privilege monitor level** command. For example, if the **xsm privilege configuration 7** command is enabled, you need a minimum privilege level of 7 to subscribe to configuration XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.



Note

The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

Examples

The following example shows how to set a configuration privilege level of 15, and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
xsm privilege configuration level 15
xsm privilege monitor level 11
```

Related Commands

Command	Description
privilege	Configures IOS privilege parameters.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

xsm privilege monitor level

To enable the XML Subscription Manager (XSM) monitoring privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege monitor level** command in global configuration mode. To remove a previously configured XSM monitoring privilege level, use the **no** form of this command.

xsm privilege monitor level *number*

no xsm privilege monitor level *number*

Syntax Description	<i>number</i>	Privilege level. Valid values are from 1 to 15. The default is 15.
---------------------------	---------------	--

Defaults	Level 1
-----------------	---------

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

Command History	Release	Modification
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The privilege level for the **xsm privilege monitor level** command must be less than or equal to the privilege level for the **xsm privilege configuration level** command. For example, if the **xsm privilege monitor 7** command is enabled, you need a minimum privilege level of 7 to subscribe to monitor XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.



Note

The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

Examples

The following example shows how to set a configuration privilege level of 15 and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
xsm privilege configuration level 15
xsm privilege monitor level 11
```

Related Commands	Command	Description
	privilege	Configures IOS privilege parameters.
	xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.

xsm vdm

To grant access to VPN-specific monitoring and configuration data for the VPN Device Manager (VDM), use the **xsm vdm** command in global configuration mode. To cancel access to VPN-specific monitoring and configuration data for VDM, use the **no** form of this command.

xsm vdm

no xsm vdm

Syntax Description This command has no arguments or keywords.

Defaults Enabled (Access to VPN-specific monitoring and configuration data for the VDM is granted when XSM is enabled.)

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines This command enables access to the following VPN-specific information:

- IPSec
- IKE
- Tunneling
- Encryption
- Keys and certificates

If XSM is enabled, this command is enabled by default. Access to VPN-specific monitoring and configuration data within XSM can be disabled by using the **no** form of the command. However, disabling this command will prevent VDM from working properly and will also disable the **xsm history vdm** command. Leaving this command enabled has minimal performance impact.

Examples In the following example, access to VPN-specific monitoring and configuration data is disabled:

```
Router(config)# xsm
Router(config)# no xsm vdm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm dvd	Grants access to switch operations.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.