

Global Configuration Mode Commands

Global configuration mode commands allow a privileged EXEC user to do the following tasks:

- Configure global GSS parameters.
- Access lower-level configuration modes on the GSS. These lower-level configuration modes are interface configuration mode and global server load-balancing configuration mode (and the configuration modes that you access from global server load-balancing configuration mode).

To access global configuration mode, use the **configure** command in privileged EXEC mode. The CLI prompt changes to (config) as follows:

```
gssm1.example.com# config  
gssm1.example.com(config)#
```

This section describes the commands in global configuration mode. For more information about commands for the lower-level configuration modes, see their sections later in this chapter.

For a list of commands that you can use in user EXEC and privileged EXEC modes, see the [“General Commands”](#) section.

aaa

To enable Terminal Access Controller Access Control System Plus (TACACS+) authentication, authorization, and accounting (AAA), use the **aaa** command. To disable a specific TACACS+ function, use the **no** form of this command.

```
aaa {authentication {ftp | gui | login | ssh} [local] | authorization
commands | accounting {commands | gui} }
```

```
no aaa {authentication {ftp | gui | login | ssh} [local] | authorization
commands | accounting {commands | gui} }
```

Syntax Description

authentication	Enables TACACS+ authentication for the specific access method. Choose from the various remote GSS authentication methods including a direct console connection, Telnet, Secure Shell (SSH), File Transfer Protocol (FTP), or primary GSSM graphical-user interface (GUI). You can also select the option to have the GSS fall back to local authentication through either the console port or a Telnet connection if the GSS cannot remotely contact another specified TACACS+ server.
ftp	Enables the TACACS+ authentication service for a FTP remote access connection.
gui	Enables the TACACS+ authentication service for a primary GSSM GUI connection.
login	Enables the TACACS+ authentication service for the login service using either a direct connection to the GSS console port or through a Telnet remote access connection.
ssh	Enables the TACACS+ authentication service for a SSH remote access connection.
local	(Optional) Used when you want the GSS to fall back to local authentication if TACACS+ authentication fails. The local option is always enabled for the login (console port or Telnet) access method.

authorization commands	Enables you to set parameters that restrict user access to specific GSS CLI commands as defined by the TACACS+ server. Use the aaa authorization commands command to enable the TACACS+ authorization service to limit a user's access to specific GSS CLI commands. The aaa authorization commands command applies to the user-level and privileged-level EXEC mode commands entered on the GSS. The command authorizes all attempts to use user-level and privileged-level EXEC mode commands including global configuration and interface configuration commands.
accounting	Enables the TACACS+ accounting service. AAA accounting enables you to monitor GSS CLI commands or primary GSSM GUI pages and user actions executed in the GSS. The information is contained in an accounting record and is transmitted from the GSS to the TACACS+ server. Each record can include a number of fields such as the username, the executed CLI command, the accessed primary GSSM GUI page and the performed action, and the time of execution.
commands	Enables the TACACS+ accounting service for monitoring the use of GSS CLI commands. The commands option applies to the user-level and privileged-level EXEC mode commands that a user enters. Command accounting generates accounting records for all user-level and privileged-level EXEC mode commands including global configuration and interface configuration commands.
gui	Enables the TACACS+ accounting service for monitoring access to the primary GSSM GUI pages and the actions performed on those pages.

Command Modes

Global configuration

Usage Guidelines

Ensure that you enable remote access on the GSS device (SSH, Telnet, or FTP) before you enable TACACS+ authentication for the specific GSS access method. See the *Cisco Global Site Selector Getting Started Guide* for details. Only one access list can be assigned to an interface at a time.

Before you enable the TACACS+ accounting service, ensure that you enable logging for accounting reports on the TACACS+ server and that you select the attributes that you want to log. For general guidelines on the recommended setup of a TACACS+ server for accounting, see the *Cisco Global Site Selector Administration Guide*, Chapter 4, Managing GSS Accounts Through a TACACS+ Server.

Examples

The following example shows how to enable TACACS+ authentication for an SSH remote access connection with a fallback to local authentication:

```
gss1.example.com(config)# aaa authentication ssh local
```

The following example shows how to enable TACACS+ authorization for the GSS CLI:

```
gss1.example.com(config)# aaa authorization commands
```

The following example shows how to enable TACACS+ accounting for the GSS CLI:

```
gss1.example.com(config)# aaa accounting commands
```

Related Commands

[show tacacs](#)
[tacacs-server host](#)
[tacacs-server keepalive-enable](#)
[tacacs-server timeout](#)

access-group

To assign a preexisting access list to an interface on your GSS, use the **access-group** command. To disassociate access lists from an interface, use the **no** form of this command.

```
access-group name interface {eth0 | eth1}
```

```
no access-group
```

Syntax Description

<i>name</i>	Name of a preexisting access list.
interface	Specifies an interface on the GSS to which the access list will be assigned.
eth0	Identifies the first Ethernet interface on the GSS device.
eth1	Identifies the second Ethernet interface on the GSS device.

Command Modes

Global configuration

Usage Guidelines

To assign an access list to a GSS interface, use the **access-group** command. An access list is a set of rules used to filter traffic to the GSS. If no access list is assigned to an interface, that interface will permit all packets to pass to the GSS.

Only one access list can be assigned to an interface at a time.

Examples

The following example shows how to assign a preexisting access list to an interface on your GSS:

```
gss1.example.com(config)# access-group icmp-rule eth0
```

Related Commands

[access-list](#)
[interface ethernet](#)

access-list

To configure access lists on the GSS that allow you to permit or deny packets access based on criteria that you establish such as the protocol type, the source address, or the destination port, use the **access-list** command. To modify or delete access lists from your GSS, use the **no** form of this command.

```
access-list name { permit | deny } protocol [source-address source-netmask |
host source-address | any] operator port [port] [destination-port
operator port [port]]
```

```
no access-list name { permit | deny } protocol [source-address
source-netmask | host source-address | any] operator port [port]
[destination-port operator port [port]]
```

Syntax Description

<i>name</i>	Alphanumeric name used to identify the access list that you are creating.
permit	When attached to an access condition, allows a connection when a packet matches the condition. All provisions of the condition must be met to make a match.
deny	When attached to an access condition, prevents a connection when a packet matches the condition. All provisions of the condition must be met to make a match.
<i>protocol</i>	Protocol for the traffic type. Recognized IP protocols are as follows: <ul style="list-style-type: none"> • tcp—Transmission Control Protocol • udp—User Datagram Protocol • icmp—Internet Control Message Protocol
<i>source-address</i>	(Optional) Network IP address from which the packet originated. The software uses the <i>source-address</i> and <i>source-netmask</i> arguments to match the incoming packet to a source network.

<i>source-netmask</i>	(Optional) Subnet mask for the network from which the packet originated. The software uses the <i>source-address</i> and <i>source-netmask</i> arguments to match the incoming packet to a source network.
host	(Optional) Host machine that is the source of the packet.
<i>source-address</i>	(Optional) IP address of the device that is the source of the packet.
<i>any</i>	(Optional) Wildcard value for the packet source. With <i>any</i> used in place of either the <i>source-address</i> , <i>source-netmask</i> , or host <i>source-address</i> values, packets from all incoming sources will match.
<i>operator</i>	Compares arbitrary bytes within the packet. Can be one of the following values: <ul style="list-style-type: none"> • eq—equal • neq—not equal • range—range
<i>port</i>	Source or destination port of the packet.
destination-port	(Optional) Compares the destination port of the packet with the access condition.

Command Modes

Global configuration

Usage Guidelines

To accept or deny packets arriving at the GSS based on criteria, such as the transfer protocol used and the packet source address, use the **access-list** command. An access list is a set of rules used to filter traffic to the GSS device. Rules can be used to either permit or deny packets and are associated with a particular interface. Each access list consists of one or more conditions. The GSS examines each packet to determine whether to forward or drop the packet based on the criteria that you specified within the access lists.

Each additional criteria statement that you enter is appended to the end of the access list statements. You cannot delete individual statements after they have been created. You can only delete an entire access list.

The order of access list statements is important. When the GSS is deciding whether to forward or block a packet, the software tests the packet against each criteria statement in the order that the statements were created. After a match is found, no more criteria statements are checked.

If you create a criteria statement that explicitly permits all traffic, no statements added later will ever be checked. If you need additional statements, you must delete the access list and retype it with the new entries.

Examples

The following example shows how to configure access lists on the GSS that allow you to permit or deny packets access based on criteria that you establish such as the protocol type, the source address, or the destination port:

```
gss1.example.com(config)# access-list rule1 1.2.3.4 255.255.255.240  
type redirect  
gss1.example.com(config)# access-list rule2 permit udp any  
destination-port eq 80  
gss1.example.com(config)# access-list rule3 permit tcp host 1.2.3.4  
gss1.example.com(config)# no access-list rule4 permit udp any  
destination-port eq 80
```

certificate set-attributes

To modify the attributes for the security certificate provided by Cisco Systems and installed on the primary Global Site Selector Manager (GSSM), use the **certificate set-attributes** command. To return the attributes for the security certificate to the default settings, use the **no** form of this command.

certificate set-attributes

no certificate set-attributes

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Usage Guidelines

You can customize the X.509 fields, extensions, and properties found on the security certificate entered by Cisco Systems. The attribute changes that you make affect the fields on the Details tab of the certificate.

When you enter the **certificate set-attributes** command, the GSS software displays a series of prompts related to the fields on the certificate. You must go through all of the prompts and make changes only to those fields that you want to modify. When completed, the software prompts you to save your changes. If you save your changes, a new certificate is generated. When you access the GSSM GUI, the Security Alert dialog box appears informing you that the certificate is invalid. At that point, you can either reinstall the updated certificate or close the dialog box and continue the GSSM GUI operation.

All fields displayed for each software prompt have a maximum character limit of 64, except for the country code, which has a maximum character limit of 2.

Modifications to the certificate cannot occur while the GUI is active on the GSSM. You must enter the **gss stop** command before executing the **certificate set-attributes** command.

Examples

The following example shows how to modify the attributes for the security certificate provided by Cisco Systems and installed on the primary GSSM:

```
gss1.example.com(config)# certificate set-attributes  
Country code (2 chars) [US]:  
State [California]: MA  
City [San Jose]: Boston  
Organization [Cisco Systems, Inc.]: New Organization  
Organization Unit [ISBU]:  
e-Mail Address [tac@cisco.com]: company@mycompany.com
```

```
US  
MA  
Boston  
New Organization  
ISBU  
company@mycompany.com  
  
Save these values? (y/n): y
```

Related Commands

[gss](#)

clock

To perform the following actions, use the **clock** command:

- Read the hardware calendar into the system clock
- Set the current time or time zone for a GSS device
- Set the daylight saving time to some predefined summer time
- Reset the GSS to synchronize log time stamps to a new time zone
- Update the hardware calendar from the system clock
- Set a user-defined daylight saving time
- Specify a user-defined time zone

```
clock {read-calendar | set hh:mm:ss MONTH DD YYYY | summer-time
timezone | timezone timezonename | update-calendar |
user-summer-time summer-time name | start time | start day |
start week | start month | end time | end day | end week | end month | offset
| user-timezone timezone name | hour_offset | minute_offset}
```

Syntax Description

read-calendar	Reads the hardware calendar into the system clock. You can use this command when the system clock is reset via NTP and you want to revert back to using the hardware clock.
set	Sets the device clock to the date and time provided.
<i>hh:mm:ss</i>	Current time to which the GSS device clock is being reset. Specify one or two digits for the hours, minutes, and seconds.

<i>MONTH DD YYYY</i>	<p>Current date to which the GSS device clock is being reset. Specify the full name of the month, one or two digits for the day, and four digits for the year. The following month names are recognized:</p> <ul style="list-style-type: none">• January• February• March• April• May• June• July• August• September• October• November• December
summer-time	<p>Sets the daylight saving time to some predefined summer times.</p>
<i>timezone</i>	<p>Name of the predefined time zone. The following time zones are recognized:</p> <ul style="list-style-type: none">• ADT (Atlantic Daylight Time)• AKDT (Alaska Standard Daylight Time)• CDT (Central Daylight Time)• EDT (Eastern Daylight Time)• MDT (Mountain Daylight Time)• PDT (Pacific Daylight Time)
timezone	<p>Resets the GSS to synchronize log time stamps to a new time zone.</p>

<i>timezonename</i>	Name of the time zone. Enter ? to list all supported time zones, countries, continents, and cities. These options are available to set the local time zone for your GSS: <ul style="list-style-type: none"> • Standard time zone (for example, GMT, EST, UTC). • Country or part of a continent (for example, America, Europe, Egypt) • Specific city (for example, New York, Paris)
update-calendar	Updates the hardware calendar from the system clock. You can use this command when the system clock is reset through NTP and you want to synchronize the system time with the hardware clock.
user-summer-time	Sets a user-defined daylight saving time.
<i>summer-time name</i>	Name of the user-defined summer time.
<i>start time</i>	Start time for the user-defined summer time in hours and minutes. Values from 0–23 are recognized.
<i>start day</i>	Start day for the user-defined summer time. The following days are recognized: <ul style="list-style-type: none"> • Friday • Saturday • Sunday • Monday • Tuesday • Wednesday • Thursday
<i>start week</i>	Start week for the user-defined summer time. Values from 1–5 are recognized.

<i>start month</i>	Start month for the user-defined summer time. The following month names are recognized: <ul style="list-style-type: none">• January• February• March• April• May• June• July• August• September• October• November• December
<i>end time</i>	End time for the user-defined summer time in hours and minutes. Values from 0–23 are recognized.
<i>end day</i>	End day for the user-defined summer time. The following days are recognized: <ul style="list-style-type: none">• Friday• Saturday• Sunday• Monday• Tuesday• Wednesday• Thursday
<i>end week</i>	End week for the user-defined summer time. Values from 1–5 are recognized.

<i>end month</i>	End month for the user-defined summer time. The following month names are recognized: <ul style="list-style-type: none"> • January • February • March • April • May • June • July • August • September • October • November • December
<i>offset</i>	Offset (in minutes) for the user-defined time zone. Values from 0–1440 are recognized.
user-timezone	Specifies a user-defined time zone.
<i>timezone name</i>	Name of the user-defined time zone.
<i>hour_offset</i>	Hour offset for the user-defined time zone. Values from –23 to +24 are recognized.
<i>minute_offset</i>	Minute offset for the user-defined time zone. Values from 0–59 are recognized.

**Note**

The **clock update-calendar** and **read-calendar** commands allow you to synchronize the hardware clock and system clock without reloading the GSS.

Command Modes

Privileged EXEC, global configuration, and interface configuration.

Usage Guidelines

If you previously enabled Network Time Protocol (NTP) on a GSS using the **ntp enable** command, the GSS prevents you from using the **clock set** command and displays an error message. If you want to manually set the clock for the GSS, first disable NTP by using the **no ntp enable** command before setting the clock.

Examples

The following example shows how to set the GSS device time:

```
gss1.example.com# clock set 13:01:05 sept 15 2004
gss1.example.com# clock timezone GMT
```

The following example shows how to set the GSS time zone:

```
gss1.example.com# clock timezone europe paris
```

The following example shows how to set a user-defined time zone on the GSS:

```
gss1.example.com# clock user-timezone EST -5 0
Please restart the GSS (reload) to sync log timestamps to new
timezone.
```

The following example shows how to set the user-defined summer time on the GSS:

```
gss1.example.com# clock user-summertime EDT 2:00 Sunday 1 April 2:00
Sunday 5 October 60
Timezone set
Please restart the GSS (reload) to sync log timestamps to new
timezone.
```

The following example shows how to update the hardware calendar from the system clock:

```
gss1.example.com# clock update-calendar
```

The following example shows how to read the hardware calendar into the system clock:

```
gss1.example.com# clock read-calendar
```

cnr aslb enable

To enable Cisco Network Registrar (CNR) additional section load balancing (ASLB) on your GSS, use the **cnr aslb enable** command. To disable ASLB, use the **no** form of this command.

cnr aslb enable

no cnr aslb enable

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Usage Guidelines

You can enable or disable the additional section load balancing (ASLB) feature that enables the GSS to load balance the additional section records of a CNR response to a D-Proxy DNS query. You enable or disable ASLB on any GSS device in the GSS mesh that has CNR loaded and enabled.

When ASLB is enabled, the GSS analyzes a CNR response before sending the response to the D-Proxy. The GSS replaces any A-records in the additional section of the CNR response with answers that you have configured in global server load balancing for the corresponding domain. The GSS then sends the modified response to the D-Proxy. The GSS performs ASLB on all CNR responses except for zone transfers and responses that the CNR digitally signed. For these two exceptions, the GSS passes the CNR responses directly to the D-Proxy without any additional processing.



Note

As the number of devices in a GSS mesh increases to its maximum size of 16 devices, the potential for an increased number of records in the additional section also increases. As the number of records increase, the performance of a GSS with ASLB enabled may slow because of the increased time required to process the CNR responses.

When you disable ASLB, the GSS passes all CNR responses directly to the D-Proxy.

Examples

The following example shows how to enable ASLB:

```
gss.example.com# config  
gss.example.com(config)# cnr aslb enable
```

Related Commands

[show cnr aslb](#)

cnr enable

To enable Cisco Network Registrar (CNR) on your GSS, use the **cnr enable** command. To disable CNR, use the **no** form of this command.

cnr enable

no cnr enable

Syntax Description This command has no keywords or arguments.

Command Modes Global configuration

Usage Guidelines The enable operation fails if CNR is not already installed on the GSS.



Note

The CNR installation does not activate the CNR server agent. Instead, you must explicitly enable CNR in order to start processing requests.

Examples The following example shows how to enable CNR:

```
gssml.example.com# cnr enable  
# Starting Network Registrar Local Server Agent
```

Related Commands [cnr install/uninstall](#)

exec-timeout

To modify the length of time that must expire before a GSS device automatically logs off an inactive user, use the **exec-timeout** command. To remove the exec-timeout setting and restore the default timeout value of 150 minutes on the GSS device, use the **no** form of this command.

exec-timeout *minutes*

no exec-timeout

<i>minutes</i>	Length of time, in minutes, that accounts must be inactive before they are timed out (1–44,640 minutes).
----------------	--

Command Modes

Global configuration

Usage Guidelines

Use the **exec-timeout** command to lengthen or shorten the period for which a user logged on to a GSS device in EXEC-mode must be idle before the session is automatically terminated. Users logged on to GSS devices in the global configuration mode are not affected by the **exec-timeout** command setting.

The default timeout for a GSS device is 150 minutes.

Examples

The following example shows how to modify the length of time that must expire before a GSS device automatically logs off an inactive user:

```
gss1.example.com(config)# exec-timeout 10
```

ftp enable

To enable the File Transfer Protocol (FTP) or launch an FTP session on your GSS device, use the **ftp enable** command. To disable FTP on your GSS device or remove the IP address from the FTP server, use the **no** form of this command.

```
ftp enable | ip_or_host
```

```
no ftp enable | ip_or_host
```

Syntax Description

<i>ip_or_host</i>	IP address or hostname of the FTP server that you want to access. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic hostname (for example, myhost.mydomain.com).
-------------------	---

Command Modes

Global configuration

Usage Guidelines

Use the **ftp enable** command in global configuration mode to enable the FTP server on the selected device or launch an FTP client to transfer a file to and from remote machines.

FTP is disabled on your GSS device by default.

Examples

The following example shows how to enable FTP or launch an FTP session on your GSS device:

```
gss1.example.com(config)# ftp enable
gss1.example.com (config)# ftp 192.168.0.1
```

Related Commands

[ftp](#)
[show telnet](#)
[telnet](#)
[scp](#)

ftp-client enable

To enable access to the File Transfer Protocol (FTP) client for different types of users, use the **ftp-client enable** command.

```
ftp-client enable {admin | all}
```

```
no ftp-client enable {admin | all}
```

Syntax Description

admin	Enables FTP client access for administrative users only.
all	Enables FTP client access for all users.

Command Modes

Global configuration

Usage Guidelines

Use the **ftp-client enable** command in global configuration mode to enable FTP client access for different types of users.

The FTP client is disabled on your GSS device by default.

Examples

The following example shows how to enable access to the FTP client for different types of users:

```
gss1.example.com(config)# ftp-client enable admin  
gss1.example.com (config)# ftp-client enable all
```

Related Commands

[ftp](#)
[ftp enable](#)
[show telnet](#)
[telnet](#)
[scp](#)

gslb

To enter global server load-balancing configuration mode, use the **gslb** command.

```
gslb [answer {cra | ns | vip} | answer-group | dns rule | domain-list |
keepalive-properties {cra | http-head | icmp | kalap | ns | tcp} |
location | owner | proximity {assign | group} | proximity-properties |
region | script | shared-keepalive {http-head | icmp | kalap | tcp} |
show | source-address- list | sticky group | sticky-properties | zone]
```

Syntax Description

See the “[Global Server Load-Balancing Configuration Mode Commands](#)” section for detailed syntax descriptions of the **gslb** command options.

Command Modes

Global configuration

Usage Guidelines

In global configuration mode, you can also use the **gslb** command with an option to perform its corresponding global server load-balancing function. For example, use the **gslb** command with the **region** option to enter region parameters. When you execute an option with the **gslb** command, you remain in global configuration mode.

To exit global server load-balancing configuration mode, use the **exec-timeout** or **gslb** commands or press **Ctrl-Z**.

Examples

The following example shows how to enter global server load-balancing configuration mode:

```
gss1.example.com# configure
gss1.example.com(config)# gslb
gss1.example.com(config-gslb)#
```

Related Commands

[exec-timeout](#)
[gslb](#)

hostname

To configure the network name of the GSS device, use the **hostname** command. To reset the hostname to the default setting, use the **no** form of this command.

hostname *name*

no hostname *name*

Syntax Description

<i>name</i>	New hostname for the GSS device; the name is case sensitive (for example, hostname.foo.com). The name may be from 1–22 alphanumeric characters. See the “Usage Guidelines,” section for more information.
-------------	---

Command Modes

Global configuration

Usage Guidelines

The default hostname is localhost.localdomain.

Use this command to configure the hostname for the GSS device. The command requires a fully qualified hostname, which requires at least one period (.) in the name (for example, hostname.foo.com). The hostname is used for the command prompts and default configuration filenames. The **no** form of this command erases the configured hostname and restores the default value.

When you specify a hostname for a GSS (primary GSSM, standby GSSM, or GSS device) that is operating in a lab network environment, the top-level domain of the hostname cannot begin with a numerical value. For example, you cannot name a primary GSSM as gssm.1lab. If you attempt to create or change a hostname for a top-level domain to a name that begins with a number, the following message appears:

```
Top level domains of hostnames cannot begin with a number
```

For the GSS interdevice communications, you should configure the hostname on the same interface (eth0 or eth1) that is being used for GSS communications, which was set when you entered the **gss-communications** command.

Examples

The following example shows how to change the hostname to gss1.cisco.com:

```
localhost.localdomain(config)# hostname gss1.cisco.com  
gss1.cisco.com(config)#
```

The following example shows how to remove the hostname:

```
gss1.cisco.com(config)# no hostname gss1.cisco.com  
localhost.localdomain(config)#
```

Related Commands

[gss tech-report](#)
[interface ethernet](#)
[ip](#)

interface ethernet

To configure a GSS Ethernet interface, use the **interface ethernet** command.

```
interface ethernet {0 | 1} {autosense | duplex {auto | full | half} | ip address
  {ip-address netmask} | no | gss-communications | gss-tcp-keepalives |
  shutdown | speed {mbits | auto}}
```

Syntax Description

ethernet	Specifies which of the GSS's two Ethernet interfaces is configured.
0	Specifies the first network Ethernet interface on the GSS.
1	Specifies the second network Ethernet interface on the GSS.
autosense	Sets the interface to automatically detect the network line speed (Fast Ethernet only) and duplex of incoming signals, and synchronizes those parameters during data transfer.
duplex	Configures an interface for autonegotiate, full-duplex, or half-duplex operation.
auto	Resets the Fast Ethernet and Gigabit Ethernet ports to automatically negotiate the port speed and the duplex of the incoming signals.
full	Configures an interface for full-duplex operation. Full duplex allows data to travel in both directions at the same time through an interface or a cable.
half	Configures an interface for half-duplex operation. A half-duplex setting ensures that data travels only in one direction at any given time.
ip address	Sets the IP address and subnet mask of the Ethernet interface.
<i>ip-address</i>	IP address of the Ethernet interface. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

<i>netmask</i>	Subnet mask of the interface. The subnet mask of the interface in dotted-decimal notation (for example, 255.255.255.0).
no	Negates the selected command or restores its default values.
gss-communications	Sets the current interface as the primary interface for the device, which is used for all GSS-related communications.
gss-tcp-keepalives	Designates the current interface as the interface that is used for the GSS keepalive communication.
shutdown	Shuts down the specified interface.
speed	Sets the bandwidth of the specified interface.
<i>mbits</i>	Bandwidth of the interface in megabits per second (10, 100, or 1000 Mbps).
auto	Enables the autonegotiate speed configuration.

Command Modes

Global configuration and interface configuration

Usage Guidelines

Use the **interface** command to configure your GSS device Ethernet interfaces (0 or 1). You can enter commands directly from global configuration mode, or you can use the **interface** command to enable interface configuration mode, which makes it easier to configure multiple interface parameters.

You cannot execute interface commands while the GSS is running (for example, serving Domain Name System (DNS) requests). You must enter the **gss stop** command before entering the **interface** command.

To display the interface identifiers (for example, interface Ethernet 0), use the **show running-config** or **show startup-config** commands. The **(config-eth) autosense**, **exec-timeout**, **ip**, **snmp**, and **(config-eth) speed** commands are listed separately in this command reference.

You cannot set the **exec-timeout** command for full duplex or half duplex until you specify an interface bandwidth speed (megabits per second) by using the **(config-eth) speed** command. If you enter the **exec-timeout** command (other than **auto**) without an explicit speed setting, the following error message appears:

```
Duplex will not be set until speed is set to a non-auto value.
```

Examples

The following example shows how to configure an attribute of GSS interface Ethernet 0 with a single CLI command:

```
gss1.example.com(config)# interface ethernet 0 speed auto
```

The following example shows that an interface can be configured in a sequence of CLI commands:

```
gss1.example.com(config)# interface ethernet 0  
gss1.example.com(config-eth0)# speed 100  
gss1.example.com(config-eth0)# duplex full  
gss1.example.com(config-eth0)# exit  
gss1.example.com(config)#
```

Related Commands

[show gslb-config](#)

[show running-config](#)

[show startup-config](#)

ip

To change the initial network device IP configuration settings, use the **ip** command. To delete or disable these settings, use the **no** form of this command.

ip { **anycast** *ip-address* | **default-gateway** *ip-address* | **name-server** *ip-addresses* | **route** *destination_address netmask gateway* }

no ip { **anycast** *ip-address* | **default-gateway** *ip-address* | **name-server** *ip-addresses* | **route** *destination_address netmask gateway* }

Syntax Description

anycast <i>ip-address</i>	Specifies the anycast IP address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
default-gateway <i>ip-address</i>	Specifies the default gateway IP address (if not routing IP). Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
name-server <i>ip-addresses</i>	Specifies the name server IP address. Enter each IP address in dotted-decimal notation.
route	Specifies the network route.
<i>destination_address</i>	Destination IP route address. Enter the IP address in dotted-decimal notation.
<i>netmask</i>	Subnet mask in dotted-decimal notation (for example, 255.255.255.0).
<i>gateway</i>	Gateway address. Enter the IP address in dotted-decimal notation.

Command Modes

Global configuration

Usage Guidelines

The guidelines for the **ip** commands are as follows:

- **ip anycast** command—Use this command to define an anycast IP address. The GSS always configures the netmask for the anycast IP address as 255.255.255.255. To delete the anycast IP address, use the **no** form of this command.

You cannot enter **ip anycast** when the GSS is running. You must first enter **gss stop** as shown in the following example:

```
gss1.example.com# gss stop
gss1.example.com(config)# ip anycast 16.2.2.2
```

The GSS loopback interface **lo:1** is configured with the anycast IP address in addition to the other interface configurations during system startup and also when you change the anycast IP address by entering the **ip anycast** command.

The anycast IP configuration is stored on the GSS in the platform.cfg file in the following format: `anycast.ip=<ipaddress>`

See the *Cisco Global Site Selector Administration Guide* for more information.

- **ip default-gateway** command—Use this command to define a default gateway. To delete the IP default gateway, use the **no** form of this command. The GSS uses the default gateway to route IP packets when it cannot find a specific route to the destination.
- **ip domain-name** command—Use this command to define a default domain name. To remove the IP default domain name, use the **no** form of this command. The GSS appends the configured domain name to any hostname that does not contain a domain name. The appended name is resolved by the Domain Name System (DNS) server and then added to the host table. The GSS must have at least one domain name server specified for the hostname resolution to work correctly.
- **ip name-server** command—Use this command to specify the address of one or more name servers to use for name and address resolution. You can specify up to eight name servers for the GSS device. To disable IP name servers, use the **no** form of this command.
- **ip route** command—Use this command to configure static IP routing. To disable an IP routing, use the **no** form of this command.

Use the **ip route** command to add a specific static route for a network host. Any IP packet designated for the specified host uses the configured route.

Examples

The following examples show how to change the initial network device IP configuration settings:

```
gss1.example.com(config)# ip default-gateway 192.168.7.18
```

Global Configuration Mode Commands

```
gss1.example.com(config)# no ip default-gateway
gss1.example.com(config)# ip route 172.16.227.128 172.16.227.250
gss1.example.com(config)# no ip route 172.16.227.128 172.16.227.250
gss1.example.com(config)# ip domain-name cisco.com
gss1.example.com(config)# no ip domain-name
gss1.example.com(config)# ip name-server 10.11.12.13
gss1.example.com(config)# no ip name-server 10.11.12.14
```

Related Commands [show ip routes](#)

logging

To configure system logging on your GSS device, use the **logging** command. To disable logging functions, use the **no** form of this command.

```
logging { disk { enable | priority loglevel | subsystem name priority
loglevel } | { facility type } | { host { enable | ip ip_addresses | priority
loglevel | subsystem name priority loglevel } }
```

```
no logging { disk { enable | priority loglevel | subsystem name priority
loglevel } | { facility type } | { host { enable | ip ip_addresses | priority
loglevel | subsystem name priority loglevel } }
```

Syntax Description

disk	Sets the log to a disk file.
enable	Enables the log to a disk or a host.
priority	Sets which priority level messages to log.
<i>loglevel</i>	Threshold that system messages must meet to be logged. Messages with lower priorities than the specified log level cannot be logged. Use one of the following keywords when selecting the log level, listed in order of priority: <ul style="list-style-type: none"> • emergencies—System is unusable. Priority 0. • alerts—Immediate action needed. Priority 1. • critical—Immediate action needed. Priority 2. • errors—Error conditions. Priority 3. • warnings—Warning conditions. Priority 4. • notifications—Normal but significant conditions. Priority 5. • informational—Informational messages. Priority 6. • debugging—Debugging messages. Priority 7.

subsystem	Sets the log for a named GSS subsystem. Each subsystem can have a different log level applied for its messages.
<i>name</i>	<p>Name of the GSS subsystem. Use one of the following keywords:</p> <ul style="list-style-type: none"> • boomerang—Boomerang logging messages. • crm—GSSM logging messages. • crdirector—CrDirector logging messages. • ddos—Distributed Denial of Service (DDoS) prevention module logging messages • dnserver—Domain Name System (DNS) logging messages. • drpagent—Director Response Protocol (DRP) agent logging messages. • keepalive—KeepAlive Engine logging messages. • nodemgr—Node manager logging messages. • proximity—Proximity logging messages. • snmp—SNMP logging messages • sticky—Sticky manager logging message. • system—System logging messages. • tacacs—TACACS+ logging messages.

facility <i>type</i>	<p>Specifies the syslog facility type. Enter the <i>type</i> argument to specify the syslog facility type. The default facility type is local5. The GSS supports the following types:</p> <ul style="list-style-type: none"> • auth—Authorization system • daemon—System daemon • kernal—Kernel • local0—Reserved for locally defined messages • local1—Reserved for locally defined messages • local2—Reserved for locally defined messages • local3—Reserved for locally defined messages • local4—Reserved for locally defined messages • local5—Reserved for locally defined messages • local6—Reserved for locally defined messages • local7—Reserved for locally defined messages • mail—Mail system • news—USENET news • syslog—System log • user—User process • uucp—UNIX-to-UNIX copy system
host	Sets the log to a remote host machine.
ip	Sets the remote host or hosts that will receive the GSS log files.
<i>ip_addresses</i>	Address or addresses of the remote logging hosts.

Command Modes

Global configuration

Usage Guidelines

Use this command to set specific parameters of the system log file. You can make global decisions about which level of logging to use, or you can make decisions on a subsystem-by-subsystem basis. For example, you could configure the GSSM to log all error-level messages but configure the node manager (nodemgr) to log a larger set of all notice-level messages.

To configure the GSS to send varying levels of event messages to an external syslog host, use the **logging host subsystem** option. Logging can be configured to send various levels of messages to disk using the **logging disk subsystem** option.

The defaults for this command are as follows:

- Logging to disk: Enabled
- Priority of message for disk: 5
- Priority of message for host: 4
- Log filename: /state/gss.log
- Log file recycle size: 10 MB
- Maximum number of log files: 25

Examples

The following examples show how to configure system logging on your GSS device:

```
gss1.example.com(config)# logging disk priority error
gss1.example.com(config)# logging host 172.16.2.3 priority notice

gss1.example.com(config)# logging disk subsystem crdirector priority
information
gss1.example.com(config)# logging host subsystem kale priority error

gss1.example.com(config)# no logging disk priority error
```

Related Commands

[show logging](#)

no

To negate a CLI command or set it to its default settings, use the **no** command. Some GSS CLI commands do not have a **no** form.

no *command*

Syntax Description

aaa	Disables a specific Terminal Access Controller Access Control System Plus (TACACS+) function.
access-group	Disassociates access lists from a specified Ethernet interface.
access-list	Modifies or deletes access lists from the GSS.
certificate set-attributes	Returns the attributes for the security certificate to the default settings.
exec-timeout	Removes the exec-timeout setting and restores the default timeout value of 150 minutes on the GSS device.
gslb	Disables proximity static entries, proximity groups, and sticky groups.
hostname	Resets the hostname to the default setting.
interface ethernet	Disables a GSS Ethernet interface.
ip	Disables or deletes network device IP configuration settings.
logging	Disables system logging (syslog).
ntp enable	Disables the Network Time Protocol (NTP).
ntp-server	Disables the NTP source.
snmp	Disables Simple Network Management Protocol (SNMP) on a GSS device.
ssh	Disables Secure Shell (SSH) on the GSS device.
tacacs-server	Disables a specific TACACS+ server function.
terminal-length	Restores the default terminal length, which is 23 lines.
username	Disables username authentication on the GSS device.

Command Modes Interface configuration, global, and global server load-balancing configuration

Usage Guidelines Use the **no** command to disable functions or negate a command. If you need to negate a specific command, such as the default gateway IP address, you must include the specific string in your command, such as **no ip default-gateway *ip-address***.

Examples The following example shows how to negate a CLI command or set it to its default settings:

```
gss1.example.com(config)# no ip name-server 10.11.12.14
```

```
gss1.example.com(config)# no ntp-server 172.16.22.44
```

ntp enable

To enable the Network Time Protocol (NTP) service, use the **ntp enable** command. To disable NTP, use the **no** form of this command.

ntp enable

no ntp enable

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Usage Guidelines

Use this command with the **ntp-server** command to synchronize the GSS clock with the specified NTP server.

NTP is disabled on your GSS device by default.

Examples

The following example shows how to enable the NTP service:

```
gss1.example.com(config)# ntp enable
```

Related Commands

[clock](#)

[ntp-server](#)

[show ntp](#)

ntp-server

To configure the Network Time Protocol (NTP) and to allow the system clock to be synchronized by a time server, use the **ntp-server** command. To disable an NTP time server, use the **no** form of this command.

```
ntp-server {ip_or_host}
```

```
no ntp-server {ip_or_host}
```

Syntax Description

<i>ip_or_host</i>	IP address or hostname of the time server providing the clock synchronization (maximum of four IP addresses or hostnames). Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic hostname (for example, myhost.mydomain.com).
-------------------	---

Command Modes

Global configuration

Usage Guidelines

Use this command to synchronize the GSS clock with the specified NTP server. When specifying more than one server, use spaces to separate the NTP server addresses. The default NTP version number is 3. To disable NTP, you must unconfigure all NTP servers by using the **no ntp-server** {*ip_or_host*} command.

If you set the clock using the **clock set** command, this setting overrides the NTP clock adjustments made with the **ntp-server** command.

Examples

The following example shows how to configure NTP and to allow the system clock to be synchronized by a time server:

```
gss1.example.com(config)# ntp enable
gss1.example.com(config)# ntp-server 161.16.22.44 161.100.10.17
```

The following example shows how to disable an NTP time server:

```
gss1.example.com(config)# no ntp-server 161.16.22.44
```

Related Commands[clock](#)[ntp enable](#)[show clock](#)[show ntp](#)

snmp

To enable Simple Network Management Protocol (SNMP) on your GSS device, use the **snmp** command. To disable SNMP on the GSS, use the **no** form of this command.

```
snmp { community-string | contact | enable | location }
```

```
no snmp { community-string | contact | enable | location }
```

Syntax Description		
	community-string	Specifies the SNMP community name for this GSS device. Enter the snmp community-string command and press Return . The GSS software prompts you to enter a name. Enter an unquoted text string with no space and a maximum length of 32 characters. Use the no form of this command to remove the community name.
	contact	Specifies the name of the contact person for this GSS device. You can include information about how to contact the person, such as a phone number or e-mail address. Enter the snmp contact command and press Return . The GSS software prompts you to enter the contact information. Enter an unquoted text string with a maximum of 255 characters including spaces. Use the no form of this command to remove contact information.
	enable	Enables SNMP on the selected GSS device.
	location	Specifies the physical location of this GSS device. Enter the snmp location command and press Return . The GSS software prompts you to enter the physical location information. Enter an unquoted text string with a maximum length of 255 characters. Use the no form of this command to remove location information.

Command Modes Global configuration.

Usage Guidelines

When entering the **snmp community-string community, location, and snmp contact** command and keywords, you have two different options available on the GSS. You can use either the pre-v2.0 software CLI or the new v2.0 software CLI. See the “Examples” section for more details.

The pre-v2.0 CLI is being retained to allow backward compatibility. Although the resulting configuration is the same for both CLIs, the front-end interface and commands differ.



Note

Be aware that existing, pre-v2.0, SNMP community, contact, and location configurations are retained after a v2.0 software upgrade. For example, if you have configured a company contact in v1.3 and then upgrade to GSS v2.0, that contact will be retained after the v2.0 upgrade is completed.

Related **snmp-server** commands are as follows:

- **snmp-server**—Configures SNMP server information and the GSS location and name.
- **snmp-server cpu-rising-threshold**—Configures the CPU rising threshold value for monitoring CPU utilization.
- **snmp-server enable-traps**—Enables SNMP server notifications (informs and traps).
- **snmp-server host**—Specifies the recipient of an SNMP notification operation.
- **snmp-server trap-limit**—Configures the maximum rate at which SNMP traps are set on your GSS device.

Examples

The following example shows how to configure a contact using the pre-v2.0 CLI:

```
gss-pilot1.cisco.com#
gss-pilot1.cisco.com# conf
gss-pilot1.cisco.com(config)# snmp contact
Enter new Contact Info: CISCO
gss-pilot1.cisco.com(config)#
```

The following example shows how to configure a contact using the v2.0 CLI:

```
gss-pilot1.cisco.com#
gss-pilot1.cisco.com# conf
```

```
gss-pilot1.cisco.com(config)# snmp-server contact CISCO  
gss-pilot1.cisco.com(config)#
```

Related Commands[gslb](#)[ntp enable](#)[ssh enable](#)[telnet](#)

snmp-server

To configure the Simple Network Management Protocol (SNMP) server information, switch location, and switch names, use the **snmp-server** command. To disable this setting, use the **no** form of this command.

```
snmp-server { community-string community-string [ro | rw] contact
contact-string | location [location] }
```

```
no snmp-server { community community string [ro | rw] contact
contact-string | location [location] }
```

Syntax Description

community-string <i>community-string</i>	Specifies the SNMP community string. The maximum length is 32 characters.
ro	(Optional) Sets the read-only access with this community string.
rw	(Optional) Sets the read-write access with this community string.
contact <i>contact-string</i>	Configures a system contact. Name of the contact. The maximum length is 255 characters.
location <i>location</i>	Configures the system location. (Optional) System location. The maximum length is 255 characters.

Command Modes

Global configuration.

Examples

The following example shows how to configure SNMP server information and the switch location:

```
gss.cisco.com(config)# snmp enable
gss.cisco.com(config)# snmp-server location Bangalore
```

The following example shows how to disable this setting:

```
gss.cisco.com(config)# no snmp-server location Bangalore
```

Related Commands [snmp-server enable-traps](#)
 [snmp-server host](#)
 [ssh enable](#)

snmp-server cpu-falling-threshold

You can configure the CPU usage threshold value that determines when the GSS issues a CPU falling threshold crossing notification by using the **snmp-server cpu-falling-threshold** command in global configuration mode. You set the threshold value as a percentage of total CPU utilization. By default, the threshold value is set to 80% of total CPU utilization. Use the **no** form of the command to set the threshold to its default value.

When CPU utilization falls below the threshold value, the GSS issues a CPU falling threshold notification if you have this notification type enabled (see “[snmp-server enable-traps](#)”).

snmp-server cpu-falling-threshold *falling_threshold*

no snmp-server cpu-falling-threshold

Syntax Description

falling_threshold Specifies the CPU usage falling threshold value, which is a percentage of the maximum CPU utilization. Enter a value from 1 to 100.

Command Modes

Global configuration.

Examples

The following example shows how to configure the CPU falling threshold value to 75% of total CPU utilization:

```
gss.cisco.com(config)# snmp enable
gss.cisco.com(config)# snmp-server enable-traps performance
gss.cisco.com(config)# snmp-server cpu-falling-threshold 75
```

The following example shows how to set the threshold back to the default value of 80%:

```
gss.cisco.com(config)# no snmp-server cpu-falling-threshold
```

Related Commands

[snmp-server](#)

snmp-server cpu-rising-threshold

snmp-server enable-traps

snmp-server host

ssh enable

snmp-server cpu-rising-threshold

You can configure the CPU usage threshold value that determines when the GSS issues a CPU rising threshold crossing notification by using the **snmp-server cpu-rising-threshold** command in global configuration mode. You set the threshold value as a percentage of total CPU utilization. By default, the threshold value is set to 80% of total CPU utilization. Use the **no** form of the command to set the threshold to its default value.

When CPU utilization exceeds the threshold, the GSS issues a CPU rising threshold notification if you have this notification type enabled (see “[snmp-server enable-traps](#)”).

The GSS does not issue a second CPU threshold crossing notification if the CPU utilization remains above the threshold value for two consecutive monitoring intervals. The GSS issues another notification only after the CPU utilization has dropped below the specified threshold value and then exceeds the threshold during subsequent monitoring intervals.

snmp-server cpu-rising-threshold *rising_threshold*

no snmp-server cpu-rising-threshold

Syntax Description	<i>rising_threshold</i>	Specifies the CPU usage rising threshold value, which is a percentage of the maximum CPU utilization. Enter a value from 1 to 100.
---------------------------	-------------------------	--

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

Examples	The following example shows how to configure the CPU rising threshold value to 75% of total CPU utilization:
-----------------	--

```
gss.cisco.com(config)# snmp enable
gss.cisco.com(config)# snmp-server enable-traps performance
gss.cisco.com(config)# snmp-server cpu-rising-threshold 75
```

The following example shows how to set the threshold back to the default value of 80%:

```
gss.cisco.com(config)# no snmp-server cpu-rising-threshold
```

Related Commands

[snmp-server](#)

[snmp-server cpu-falling-threshold](#)

[snmp-server enable-traps](#)

[snmp-server host](#)

[ssh enable](#)

snmp-server enable-traps

To enable all traps, use the **snmp-server enable-traps** command. To disable all traps, use the **no** form of this command.

```
snmp-server enable-traps [core | gslb [ans | dns | kal | peer-status] |
  performance [cpu-falling-threshold | cpu-rising-threshold] | snmp
  [authentication | cold-start]]
```

```
no snmp-server enable-traps [core | gslb [ans | dns | kal | peer-status] |
  performance [cpu-falling-threshold | cpu-rising-threshold] | snmp
  [authentication | cold-start]]
```

Syntax	Description
core	Enables the SNMP core-file discovery notification. Note Enabling core notification sends traps to the NMS when a core file is discovered on the device.
gslb	Enables all Simple Network Management Protocol (SNMP) global server load-balancing (GSLB) notifications.
ans	(Optional) Enables only the SNMP Answer status change notification.
dns	(Optional) Enables only the SNMP Domain Name System (DNS) server notification.
kal	(Optional) Enables only the SNMP GSLB keepalive notification.
peer-status	(Optional) Enables the SNMP GSLB peer-status change notification. Note Enabling peer-status notification sends traps/informs to the Network Management Station (NMS), whenever the status of the peer GSS devices changes from <i>online</i> to <i>offline</i> and vice versa. This trap/inform can be sent only by the primary GSS device because only the primary contains all the information about its peer GSS devices.

performance	Enables the SNMP CPU usage rising and falling threshold notification for monitoring CPU utilization.
cpu-falling-threshold	(Optional) Enables only the SNMP CPU usage falling threshold notification for monitoring CPU utilization.
cpu-rising-threshold	(Optional) Enables only the SNMP CPU usage rising threshold notification for monitoring CPU utilization.
snmp	Enables all SNMP agent notifications.
authentication	(Optional) Enables only the SNMP agent authentication notification.
cold-start	(Optional) Enables only the SNMP agent cold start notification.

Command Modes

Global configuration.

Examples

The following example shows how to enable all traps:

```
gss.cisco.com(config)# snmp enable
gss.cisco.com(config)# snmp-server enable-traps kal
```

The following example shows how to disable all traps:

```
gss.cisco.com(config)# no snmp-server enable-traps kal
```

Related Commands

[snmp-server](#)
[snmp-server cpu-falling-threshold](#)
[snmp-server cpu-rising-threshold](#)
[snmp-server host](#)
[ssh enable](#)

snmp-server host

To specify the recipient of an Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command. To disable this setting, use the **no** form of this command.

```
snmp-server host host-address community-string {traps} {version [1 | 2]}
[udp-port port]
```

```
no snmp-server host host-address community-string {traps} {version [1 |
2]} [udp-port port]
```

Syntax Description

<i>host-address</i>	Name or IP address of the host (the targeted recipient).
<i>community-string</i>	SNMP community string. The maximum length is 32 characters.
traps	Sends SNMP traps to this host Note You can configure a maximum of 10 hosts for trap notification.
version	Specifies the version of SNMP used to send the traps.
1	(Optional) Specifies SNMPv1 (the default).
2	(Optional) Specifies SNMPv2.
udp-port <i>port</i>	(Optional) Specifies the port UDP port of the host to use. The default is 162.

Command Modes

Global configuration.

Examples

The following example shows how to specify the recipient of an SNMP notification operation:

```
gss.cisco.com(config)# snmp enable
gss.cisco.com(config)# snmp-server host 1.1.1.1 public traps version 2
udp-port 162
```

The following example shows how to disable this setting:

```
gss.cisco.com(config)# no snmp-server host 1.1.1.1 public traps
version 2 udp-port 162
```

Related Commands

[snmp-server](#)

[snmp-server enable-traps](#)

[snmp-server host](#)

snmp-server trap-limit

To configure the maximum rate at which Simple Network Management Protocol (SNMP) traps are set on your GSS device, use the **snmp-server trap-limit** command. To disable this setting, use the **no** form of this command.

```
snmp-server trap-limit { answer-trap value | dns-clause-trap value | keepalive-trap value }
```

```
no snmp-server trap-limit { answer-trap value | dns-clause-trap value | keepalive-trap value }
```

Syntax	Description
answer-trap <i>value</i>	Configures a rate limit for the answer trap. Valid values are from 1–65535 traps per minute.
dns-clause-trap <i>value</i>	Configures the rate limit for Domain Name System (DNS) clause traps. Valid values are from 1–65535 traps per minute.
keepalive-trap <i>value</i>	Configures the rate limit for the keepalive trap. Valid values are from 1–65535 traps per minute.

Command Modes Global configuration.

Examples The following example shows how to configure the maximum rate at which SNMP traps are set on your GSS device:

```
gss.cisco.com(config)# snmp enable
gss.cisco.com(config)# snmp-server trap-limit answer trap 10
```

The following example shows how to disable this setting:

```
gss.cisco.com(config)# no snmp-server trap-limit answer trap
```

Related Commands [snmp-server ssh enable](#)

snmp-server trap-source ethernet

To specify the IP address associated with an Ethernet port to use in the agent address field of SNMP V1 notifications, use the **snmp-server trap-source ethernet** command. To disable the setting, use the **no** form of the command.

```
snmp-server trap-source ethernet {0 | 1}
```

```
snmp-server trap-source ethernet {0 | 1}
```

Syntax Description	0	1
	Specifies the IP address associated with Ethernet port 0.	Specifies the IP address associated with Ethernet port 1.

Command Modes Global configuration.

Examples The following example shows how to specify to use the IP address associated with Ethernet port 1 in the agent address field:

```
gss.cisco.com(config)# snmp enable
gss.cisco.com(config)# snmp-server trap-source ethernet 1
```

The following example shows how to disable this setting:

```
gss.cisco.com(config)# no snmp-server trap-source ethernet 1
```

Related Commands [snmp-server](#)
[ssh enable](#)

ssh enable

To enable or disable Secure Shell (SSH) on the GSS device, use the **ssh enable** command. To disable SSH, use the **no** form of this command.

ssh enable

no ssh enable

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Usage Guidelines

SSH on the GSS supports the SSH v2 and v1 protocols. For SSH v2, the software provides 128-bit AES, Blowfish, 3DES, CAST128, ARCfour, 192-bit AES, or 256-bit AES. For SSH v1, the software provides encrypted communication using ciphers such as 3DES or Blowfish.

By default, the GSS turns off SSH protocol v1 because it is considered to be cryptographically insecure. If your clients support both SSH protocol v2 and v1, you should configure the client to use SSH protocol v2 by default. If your remote SSH application cannot support SSH protocol v2 and requires SSH protocol v1, enter the **ssh protocol version 1** command.

Examples

The following example shows how to enable SSH on the GSS device:

```
gss1.example.com(config)# ssh enable
```

The following example shows how to disable SSH on the GSS device:

```
gss1.example.com(config)# no ssh enable
```

Related Commands

[gslb](#)
[ntp enable](#)
[snmp](#)
[ssh keys](#)

ssh protocol version 1
telnet

ssh keys

To globally enable remote access to the copied private and public keys on the GSS, use the **ssh keys** command. To disable authentication using Secure Shell (SSH) keys, use the **no** form of this command.

ssh keys

no ssh keys

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Usage Guidelines

The GSS disables SSH key support by default.

The GSS supports remote login to the GSS over an SSH session that uses private and public key pairs for authentication. With this method of remote connection, use a generated private and public key pair to participate in a secure communication by encrypting and decrypting messages. Use of a private and public key pair bypasses the normal username and password authentication process. This remote access method may be useful when running scripts that connect automatically to the GSS.

You generate the private key and the corresponding public key as a key pair on a server separate from the GSS and copy the public key to the GSS /home directory.

By default, the GSS disables SSH key support. As a one-time process, after you initially copy the private and public keys onto the GSS, you must enable global access to those keys to remotely log in to the GSS by using the **ssh keys** command.

Examples

The following example shows how to globally enable remote access to the copied private and public keys on the GSS:

```
gss1.example.com(config)# ssh keys
```

The following example shows how to disable authentication using SSH keys:

```
gss1.example.com(config)# no ssh keys
```

Related Commands

[ssh enable](#)
[ssh protocol version 1](#)

ssh protocol version 1

If your remote Secure Shell (SSH) application cannot support SSH protocol v2 and you require SSH protocol v1, use the **ssh protocol version 1** command. To disable SSH protocol version 1, use the **no** form of this command.

ssh protocol version 1

no ssh protocol version 1

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Usage Guidelines

The GSS turns off SSH protocol v1 by default.

SSH on the GSS supports the SSH v2 and v1 protocols. For SSH v2, the software provides 128-bit AES, Blowfish, 3DES, CAST128, ARCfour, 192-bit AES, or 256-bit AES. For SSH v1, the software provides encrypted communication using ciphers such as 3DES or Blowfish.

By default, the GSS turns off SSH protocol v1 because it is considered to be cryptographically insecure. If your clients support both SSH protocol v2 and v1, we recommend that you configure the client to use SSH protocol v2 by default. If your remote SSH application cannot support SSH protocol v2 and requires SSH protocol v1, enter the **ssh protocol version 1** command.

Examples

The following example shows how to enable SSH protocol v1:

```
gss1.example.com(config)# ssh protocol version 1
```

The following example shows how to disable SSH protocol v1:

```
gss1.example.com(config)# no ssh protocol version 1
```

Related Commands

[ssh enable](#)
[ssh keys](#)

tacacs-server host

To specify the name of the IP hosts maintaining the Terminal Access Controller Access Control System Plus (TACACS+) server, use the **tacacs-server host** command. To delete a server from the running configuration, to delete a specified TCP port, or to delete an encryption key, use the **no** form of this command.

```
tacacs-server host ip_or_host [port port] [key encryption_key]
```

```
no tacacs-server host ip_or_host [port port] [key encryption_key]
```

Syntax Description

<i>ip_or_host</i>	IP address or hostname of the TACACS+ server that you want to access. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic hostname (for example, myhost.mydomain.com).
port <i>port</i>	(Optional) Specifies the TCP port of the TACACS+ server. The default port is 49. You can enter a port number from 1–65535.
key <i>encryption_key</i>	(Optional) Specifies the shared secret between the GSS and the TACACS+ server. You must define an encryption key to encrypt TACACS+ packet transactions between the GSS and the TACACS+ server. If you do not define an encryption key, the GSS does not encrypt packets transmitted to the TACACS+ server and they will be in clear text. The range for the encryption key is 1–100 alphanumeric characters.

Command Modes

Global configuration

Usage Guidelines

The TACACS+ server contains the TACACS+ authentication, authorization, and accounting relational databases. You can designate a maximum of three servers on the GSS. However, the GSS uses only one server at a time. To set up a list of preferred TACACS+ security daemons, use the **tacacs-server host** command.

The TACACS+ software searches for the server hosts in the order that you specify through the **tacacs-server host** command. The GSS periodically queries all configured TACACS+ servers with a TCP keepalive to ensure network connectivity and TACACS+ application operation. If the GSS determines that the first TACACS server is down, the GSS attempts to connect to the next server in the list of configured TACACS+ servers as the backup server. If a second (or third) TACACS+ server is available for use, the GSS selects that server as the active TACACS+ server.

The GSS uses TCP keepalives to monitor connectivity with the active TACACS+ server. If the TCP keepalives fail or if you disable the use of keepalives, you can use the **tacacs-server timeout** command to define a global TACACS+ timeout period that the GSS uses to wait for a response to a connection attempt from a TACACS+ server. The timeout value applies to all defined TACACS+ servers.

For recommended guidelines on setting up a TACACS+ server (the Cisco Secure ACS in this example), see the *Cisco Global Site Selector Administration Guide*, Chapter 4, Managing GSS Accounts Through a TACACS+ Server.

Examples

The following example shows how to configure three TACACS+ servers as 192.168.1.100:8877, 192.168.1.101:49 (using the default TCP port), and 192.168.1.102:9988 with different shared secrets:

```
gss1.example.com(config)# tacacs-server host 192.168.1.100 port 8877
key SECRET-123
gss1.example.com(config)# tacacs-server host 192.168.1.101 key
SECRET-456
gss1.example.com(config)# tacacs-server host 192.168.1.102 port 9988
key SECRET-789
```

Related Commands

[show statistics](#)
[show tacacs](#)
[tacacs-server keepalive-enable](#)
[tacacs-server timeout](#)

tacacs-server keepalive-enable

To disable or enable the use of TCP keepalives sent by the GSS to the active Terminal Access Controller Access Control System Plus (TACACS+) server, use the **tacacs-server keepalive-enable** command. To disable the use of TCP keepalives with the active TACACS+ server, use the **no** form of this command.

tacacs-server keepalive-enable

no tacacs-server keepalive-enable

Syntax Description This command has no keywords or arguments.

Command Modes Global configuration

Usage Guidelines By default, the GSS enables the automatic use of TCP keepalives to periodically query all online TACACS+ servers with a TCP keepalive to ensure network connectivity and TACACS+ application operation. If the GSS determines that the first TACACS server is down (offline), the GSS then attempts to connect to the next server in the list of configured TACACS+ servers as the backup server. If a second (or third) TACACS+ server is available for use, the GSS selects that server as the active TACACS+ server.

To disable the use of TCP keepalives with the active TACACS+ server, use the **no** form of the **tacacs-server keepalive-enable** command.

Examples The following example shows how to enable TCP keepalives:

```
gss1.example.com(config)# tacacs-server keepalive-enable
```

Related Commands

- [show statistics](#)
- [show tacacs](#)
- [tacacs-server host](#)

tacacs-server timeout

tacacs-server timeout

To define a global Terminal Access Controller Access Control System Plus (TACACS+) timeout period, in seconds, that specifies how long the GSS waits for a response to a connection attempt from a TACACS+ server, use the **tacacs-server timeout** command. To reset the timeout period to the default of 5 seconds, use the **no** form of this command.

```
tacacs-server timeout {seconds}
```

```
no tacacs-server timeout {seconds}
```

Syntax Description

seconds

Timeout value. Enter a number from 1–255 seconds. The default is 5 seconds. The GSS dynamically applies the modified timeout period and the new value takes effect automatically on the next TACACS+ connection.

Command Modes

Global configuration

Usage Guidelines

The timeout value applies to all defined TACACS+ servers.

If the TCP keepalives fail or if you disable the use of keepalives, you can use the **tacacs-server timeout** command to define a global TACACS+ timeout period, in seconds, that the GSS uses to wait for a response to a connection attempt from a TACACS+ server. The timeout value applies to all defined TACACS+ servers. The default timeout period is 5 seconds.

Examples

The following example shows how to set the timeout period to 60 seconds:

```
gss1.example.com(config)# tacacs-server timeout 60
```

Related Commands

[show statistics](#)

[show tacacs](#)

tacacs-server keepalive-enable

tacacs-server timeout

terminal-length

To adjust the amount of screen information that can be displayed at one time on your terminal, use the **terminal-length** command. To restore the default terminal length, which is 23 lines, use the **no** form of this command.

terminal-length *number*

no terminal-length

Syntax Description	<i>number</i>	Number of screen rows between 0–512. The default terminal length is 23 lines.
---------------------------	---------------	---

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

Usage Guidelines The **terminal-length** command allows you to adjust the number of rows of output that will be sent to your terminal screen at once by the GSS. The maximum number of rows is 512.

When set to 0, the GSS sends all of its data to the screen at once, without pausing (buffering the data).

Examples The following example shows how to adjust the amount of screen information that can be displayed at one time on your terminal:

```
gss1.example.com(config)# terminal-length 512
```

The following example shows how to restore the default terminal length:

```
gss1.example.com(config)# no terminal-length
```

Related Commands	show terminal-length
-------------------------	--------------------------------------

username

To establish the username authentication, use the **username** command.

```
username name { delete | password password privilege { user | admin } }
```

Syntax Description

<i>name</i>	Username that you want to assign or change. Enter an unquoted alphanumeric text string with no spaces and a maximum of 32 characters. Usernames may contain alpha characters (for example, A-Z or a-z) and/or numerals. Numerals may be present at any position in the name.
delete	Deletes the named user or administrative account.
password	Establishes the password.
<i>password</i>	Password that you want to assign or change. Enter an unquoted text string with no spaces and a maximum length of eight characters.
privilege	Sets the user privilege level.
user	Sets the user privilege to normal user.
admin	Sets the user privilege to administrative user.

Command Modes

Global configuration

Usage Guidelines

The **username** global configuration command is used to create users or administrative accounts, change the password and privilege level for existing user accounts, or delete existing accounts.

When specifying a username, enter an unquoted alphanumeric text string with no spaces and a maximum of 32 characters. Usernames may contain alpha characters (for example, A-Z or a-z) and/or numerals. Numerals may be present at any position in the name.

Examples

The following example shows how a new account can be set up or removed from a GSS device:

```
gss1.example.com(config)# username testuser password mypassword  
privilege user  
gss1.example.com(config)# exit  
gss1.example.com# show user username testuser  
testuser user  
  
gss1.example.com(config)# username testuser delete
```

Related Commands

[show user](#)

[show users](#)

