

ssg accounting interval

To specify the interval at which Service Selection Gateway (SSG) sends accounting updates to the accounting server, use the **ssg accounting interval** command in global configuration mode. To disable the accounting interval, use the **no** form of this command.

ssg accounting interval *seconds*

no ssg accounting interval *seconds*

Syntax Description	<i>seconds</i>	Number of seconds after which an accounting update will be sent to the accounting server. The range is from 60 to 2147483647 seconds, in increments of 60 seconds. The value entered will be rounded up to the next multiple of 60. Default is 600.
---------------------------	----------------	---

Defaults	600 seconds
-----------------	-------------

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

Command History	Release	Modification
	12.0(5)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines	Use this command to specify the interval at which accounting updates are sent to the accounting server.
-------------------------	---

Examples	The following example shows how to specify that SSG will send an accounting update to the accounting server every 60 seconds:
-----------------	---

```
Router(config)# ssg accounting interval 60
```

Related Commands	Command	Description
	ssg accounting	Enables SSG accounting.

ssg accounting

To enable Service Selection Gateway (SSG) accounting, use the **ssg accounting** command in global configuration mode. To disable the SSG accounting, use the **no** form of this command.

ssg accounting

no ssg accounting

Syntax Description This command has no arguments or keywords.

Defaults Accounting is enabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines The **ssg accounting** command enables the sending of start, stop, and interim accounting records for hosts and connections.

Examples The following example shows how to reenables SSG accounting if it has been disabled:

```
Router(config)# ssg accounting
```

Related Commands	Command	Description
	ssg accounting interval	Specifies the interval at which accounting updates are sent to the accounting server.

ssg auto-domain

To enable Service Selection Gateway (SSG) Autodomain, use the **ssg auto-domain** command in global configuration mode. To remove all Autodomain configuration from the running configuration and to prevent further activation of autodomains, use the **no** form of this command.

ssg auto-domain

no ssg auto-domain

Syntax Description This command has no arguments or keywords.

Defaults Autodomain is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines To enable SSG Autodomain, use this command in global configuration mode. SSG must be enabled before the **ssg auto-domain** command can be entered.



Note

The **ssg auto-domain** command enables basic Autodomain. In basic Autodomain, the profile downloaded from the AAA server for the Autodomain name is a service profile (either with or without SSG-specific attributes). By default, an attempt is made to find a valid service profile first based on Access Point Name (APN), then based on username. Use the **mode extended** command to configure Autodomain extended mode.

Use the **no ssg auto-domain** command to prevent further activations of autodomains and to remove all Autodomain configuration from the running-configuration. Subsequent reissuing of the **ssg auto-domain** command restores Autodomain to its former state.

Examples The following example enables basic SSG Autodomain:

```
ssg enable
ssg auto-domain
```

Related Commands	Command	Description
	download exclude-profile	Adds to the Autodomain download exclusion list.
	exclude	Configures the Autodomain exclusion list.

Command	Description
mode extended	Enables extended mode for SSG Autodomain.
nat user-address	Enables NAT on Autodomain tunnel service.
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg enable	Enables SSG functionality.

ssg auto-logoff arp

To configure Service Selection Gateway (SSG) to automatically log off hosts that have lost connectivity with SSG and to use the Address Resolution Protocol (ARP) ping mechanism to detect connectivity, use the **ssg auto-logoff arp** command in global configuration mode. To disable SSG autologoff, use the **no** form of this command.

ssg auto-logoff arp [*interval seconds*]

no auto-logoff arp

Syntax Description	interval <i>seconds</i>	(Optional) ARP ping interval, in seconds. The interval specified will be rounded to the nearest multiple of 30. An interval of less than 30 will be rounded up to 30 seconds. The default interval is 30 seconds.
---------------------------	--------------------------------	---

Defaults	SSG auto logoff is not enabled. Default interval is 30 seconds.
-----------------	--

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

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines	When the ssg auto-logoff arp command is configured, SSG will use the ARP ping mechanism to detect connectivity to hosts.
-------------------------	---



Note

ARP ping should be used only in deployment situations in which all hosts are directly connected to the SSG through a broadcast interface such as an Ethernet interface or a bridged interface such as a routed bridge encapsulation (RBE) or an integrated routing and bridging (IRB) interface.

ARP request packets are smaller than Internet Control Message Protocol (ICMP) ping packets, so it is recommended that you configure SSG auto logoff to use ARP ping in situation sin which hosts are directly connected.

ICMP ping can be used in all types of deployment situations. See the **ssg auto-logoff icmp** command page for more information about SSG auto logoff using ICMP ping.

ARP ping will work only on hosts that have a MAC address. So, for example, ARP ping will not work for PPP users because they do not have a MAC table entry.

ARP ping does not support overlapping IP addresses.

SSG autologoff that uses the ARP ping mechanism will not work for hosts with static ARP entries.

You can use only one method of SSG autologoff at a time: ARP ping or ICMP ping. If you configure SSG to use ARP ping after ICMP ping has been configured, the ICMP ping function will become disabled.

Examples

The following example shows how to enable SSG autologoff. SSG will use ARP ping to detect connectivity to hosts.

```
Router(config)# ssg auto-logoff arp interval 60
```

Related Commands

Command	Description
ssg auto-logoff icmp	Configures the SSG to automatically log off hosts that have lost connectivity with SSG and to use the ICMP ping mechanism to detect connectivity.

ssg auto-logoff icmp

To configure Service Selection Gateway (SSG) to automatically log off hosts that have lost connectivity with SSG and to use the Internet Control Message Protocol (ICMP) ping mechanism to detect connectivity, use the **ssg auto-logoff icmp** command in global configuration mode. To disable SSG autologoff, use the **no** form of this command.

ssg auto-logoff icmp [*timeout milliseconds*] [*packets number*] [*interval seconds*]

no auto-logoff icmp

Syntax Description		
timeout <i>milliseconds</i>	(Optional) ICMP ping response timeout. The default is 500 milliseconds.	
packets <i>number</i>	(Optional) Number of ICMP ping packets that will be sent after a ping packet indicates that a host is unreachable. The default is 2 packets.	
interval <i>seconds</i>	(Optional) ICMP ping interval, in seconds. The interval specified will be rounded to the nearest multiple of 30. An interval less than 30 will be rounded up to 30 seconds. The default interval is 30 seconds.	

Defaults	
	SSG autologoff is not enabled.
	Interval: 30 seconds
	Timeout: 500 milliseconds
	Number of packets: 2 packets

Command Modes	
	Global configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines	
	When the ssg auto-logoff icmp command is specified, SSG will use the ICMP ping mechanism to detect connectivity to hosts.



Note

ICMP ping may be used in all types of deployment situations.

ICMP ping supports overlapping IP addresses.

If a user is not reachable, a configured number of packets (p) will be sent, and each packet will be timed out (t). The user will be logged off in $p * t$ milliseconds after the first pinging attempt. If $p * t$ milliseconds is greater than the configured pinging interval, then the time taken to log off the host after connectivity is lost will be greater than the configured autologoff interval. If parameters are configured this way, the following warning will be issued: "Hosts will be auto-logged off ($p * t$) msec after connectivity is lost." When the pinging interval is less than $p * t$, the timeout process for a host that has

become unreachable will be invoked when the pinging to that host is still occurring. However, because the timeout process will check the status of the host object and find that it is in a pinging state, the host will not be pinged again.

You can use only one method of SSG autologoff at a time: Address Resolution Protocol (ARP) ping or ICMP ping. If you configure SSG to use ARP ping after ICMP ping has been configured, the ICMP ping function will become disabled.

Default values will be applied if a value of zero is configured for any parameters.

The **ssg auto-logoff arp** command will configure SSG to use the ARP ping mechanism to detect connectivity to hosts. ARP ping should be used only in deployment situations in which all hosts are directly connected to the SSG through a broadcast interface such as an Ethernet interface or a bridged interface such as a routed bridge encapsulation or an integrated routing and bridging interface.

ARP request packets are smaller than ICMP ping packets, so it is recommended that you configure SSG autologoff to use ARP ping in situations in which hosts are directly connected. For more information about SSG autologoff that uses ARP ping, see the **ssg auto-logoff arp** command reference page.

Examples

The following example shows how to enable SSG autologoff. SSG will use ICMP ping to detect connectivity to hosts.

```
Router(config)# ssg auto-logoff icmp interval 60 timeout 300 packets 3
```

Related Commands

Command	Description
ssg auto-logoff arp	Configures the SSG to automatically log off hosts that have lost connectivity with SSG and to use the ARP ping mechanism to detect connectivity.

ssg bind direction

To specify an interface as a downlink or uplink interface, use the **ssg bind direction** command in global configuration mode. To disable the directional specification for the interface, use the **no** form of this command.

ssg bind direction {**downlink** | **uplink**} {**ATM** *atm-interface* | **Async** *async-interface* | **BVI** *bvi-interface* | **Dialer** *dialer-interface* | **Ethernet** *ethernet-interface* | **FastEthernet** *fastethernet-interface* | **Group-Async** *group-async-interface* | **Lex** *lex-interface* | **Loopback** *loopback-interface* | **Multilink** *multilink-interface* | **Null** *null-interface* | **Port-channel** *port-channel-interface* | **Tunnel** *tunnel-interface* | **Virtual-Access** *virtual-access-interface* | **Virtual-Template** *virtual-template-interface* | **Virtual-TokenRing** *virtual-tokenring-interface*}

no ssg bind direction {**downlink** | **uplink**} {**ATM** *atm-interface* | **Async** *async-interface* | **BVI** *bvi-interface* | **Dialer** *dialer-interface* | **Ethernet** *ethernet-interface* | **FastEthernet** *fastethernet-interface* | **Group-Async** *group-async-interface* | **Lex** *lex-interface* | **Loopback** *loopback-interface* | **Multilink** *multilink-interface* | **Null** *null-interface* | **Port-channel** *port-channel-interface* | **Tunnel** *tunnel-interface* | **Virtual-Access** *virtual-access-interface* | **Virtual-Template** *virtual-template-interface* | **Virtual-TokenRing** *virtual-tokenring-interface*}

Syntax Description		
downlink		Specifies interface direction as downlink.
uplink		Specifies interface direction as uplink.
ATM		Indicates that the interface is ATM.
<i>atm-interface</i>		ATM interface.
Async		Indicates that the interface is Async.
<i>async-interface</i>		Async interface.
BVI		Indicates that the interface is BVI.
<i>bvi-interface</i>		Bridge-Group Virtual Interface.
Dialer		Indicates that the interface is Dialer.
<i>dialer-interface</i>		Dialer interface.
Ethernet		Indicates that the interface is Ethernet.
<i>ethernet-interface</i>		IEEE 802.3.
FastEthernet		Indicates that the interface is Fast Ethernet.
<i>fastethernet-interface</i>		Fast Ethernet IEEE 802.3.
Group-Async		Indicates that the interface is Group Async.
<i>group-async-interface</i>		Group async interface.
Lex		Indicates that the interface is Lex.
<i>lex-interface</i>		Lex interface.
Loopback		Indicates that the interface is Loopback.
<i>loopback-interface</i>		Loopback interface.
Multilink		Indicates that the interface is Multilink.
<i>multilink-interface</i>		Multilink interface.
Null		Indicates that the interface is Null.

<i>null-interface</i>	Null interface.
Port-channel	Indicates that the interface is Port Channel.
<i>port-channel-interface</i>	Port channel interface.
Tunnel	Indicates that the interface is Tunnel.
<i>tunnel-interface</i>	Tunnel interface.
Virtual-Access	Indicates that the interface is Virtual Access.
<i>virtual-access-interface</i>	Virtual access interface.
Virtual-Template	Indicates that the interface is Virtual Template.
<i>virtual-template-interface</i>	Virtual template interface.
Virtual-TokenRing	Indicates that the interface is Virtual Token Ring.
<i>virtual-tokenring-interface</i>	Virtual token ring interface.

Defaults

All interfaces are configured as uplink interfaces by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use this command to specify an interface as downlink or uplink. An uplink interface is an interface to services; a downlink interface is an interface to subscribers.

Examples

The following example shows how to specify an ATM interface as a downlink interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssg bind direction downlink ATM 0/0/0.10
```

Related Commands

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.

ssg bind service

To specify the interface for a service, use the **ssg bind service** command in global configuration mode. To unbind the service and the interface, use the **no** form of this command.

ssg bind service *service-name* { *ip-address* | **ATM** *atm-interface* | **Async** *async-interface* | **BVI** *bvi-interface* | **Dialer** *dialer-interface* | **Ethernet** *ethernet-interface* | **FastEthernet** *fastethernet-interface* | **Group-Async** *group-async-interface* | **Lex** *lex-interface* | **Loopback** *loopback-interface* | **Multilink** *multilink-interface* | **Null** *null-interface* | **Port-channel** *port-channel-interface* | **Tunnel** *tunnel-interface* | **Virtual-Access** *virtual-access-interface* | **Virtual-Template** *virtual-template-interface* | **Virtual-TokenRing** *virtual-tokenring-interface* }

no ssg bind service *service-name* { *ip-address* | **ATM** *atm-interface* | **Async** *async-interface* | **BVI** *bvi-interface* | **Dialer** *dialer-interface* | **Ethernet** *ethernet-interface* | **FastEthernet** *fastethernet-interface* | **Group-Async** *group-async-interface* | **Lex** *lex-interface* | **Loopback** *loopback-interface* | **Multilink** *multilink-interface* | **Null** *null-interface* | **Port-channel** *port-channel-interface* | **Tunnel** *tunnel-interface* | **Virtual-Access** *virtual-access-interface* | **Virtual-Template** *virtual-template-interface* | **Virtual-TokenRing** *virtual-tokenring-interface* }

Syntax Description

<i>service-name</i>	Service name.
<i>ip-address</i>	IP address of the next-hop router.
ATM	Indicates that the interface is ATM.
<i>atm-interface</i>	ATM interface.
Async	Indicates that the interface is Async.
<i>async-interface</i>	Async interface.
BVI	Indicates that the interface is BVI.
<i>bvi-interface</i>	Bridge-Group Virtual Interface.
Dialer	Indicates that the interface is Dialer.
<i>dialer-interface</i>	Dialer interface.
Ethernet	Indicates that the interface is Ethernet.
<i>ethernet-interface</i>	IEEE 802.3.
FastEthernet	Indicates that the interface is Fast Ethernet.
<i>fastethernet-interface</i>	Fast Ethernet IEEE 802.3.
Group-Async	Indicates that the interface is Group Async.
<i>group-async-interface</i>	Group async interface.
Lex	Indicates the interface is Lex.
<i>lex-interface</i>	Lex interface.
Loopback	Indicates that the interface is Loopback.
<i>loopback-interface</i>	Loopback interface.
Multilink	Indicates that the interface is Multilink.
<i>multilink-interface</i>	Multilink interface.
Null	Indicates that the interface is Null.
<i>null-interface</i>	Null interface.

Port-channel	Indicates that the interface is Port Channel.
<i>port-channel-interface</i>	Port channel interface.
Tunnel	Indicates that the interface is Tunnel.
<i>tunnel-interface</i>	Tunnel interface.
Virtual-Access	Indicates that the interface is Virtual Access.
<i>virtual-access-interface</i>	Virtual access interface.
Virtual-Template	Indicates that the interface is Virtual Template.
<i>virtual-template-interface</i>	Virtual template interface.
Virtual-TokenRing	Indicates that the interface is Virtual Token Ring.
<i>virtual-tokenring-interface</i>	Virtual token ring interface.

Defaults No default behavior or values.

Command Modes Global configuration

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines Use this command to bind a service to an interface.

Examples The following example shows the interface for the service defined as “MyService”:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssg bind service MyService ATM 0/0/0.10
```

Command	Description
clear ssg service	Removes a service.
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
show ssg service	Displays the information for a service.

ssg default-network

To specify the default network IP address or subnet and mask, use the **ssg default-network** command in global configuration mode. To disable the default network IP address and mask, use the **no** form of this command.

ssg default-network *ip-address mask*

no ssg default-network *ip-address mask*

Syntax Description	<i>ip-address</i>	Service Selection Gateway (SSG) default IP address or subnet.
	<i>mask</i>	SSG default network destination mask.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines Use this command to specify the first IP address or subnet that users will be able to access without authentication. This is the address where the Cisco Service Selection Dashboard (SSD) resides. After users enter the URL for the Cisco SSD, they will be prompted for a username and password. A mask provided with the IP address specifies the range of IP addresses that users will be able to access without authentication.

Examples The following example shows a default network IP address, 192.168.1.2, and mask 255.255.255.255:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssg default-network 192.168.1.2 255.255.255.255
```

ssg enable

To enable Service Selection Gateway (SSG), use the **ssg enable** command in global configuration mode. To disable SSG, use the **no** form of this command.

ssg enable

no ssg enable

Syntax Description This command has no arguments or keywords.

Defaults SSG is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7) DC	This command was introduced on the Cisco 6400.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Examples The following example shows how to enable SSG:

```
Router(config)# ssg enable
```

ssg local-forwarding

To enable Service Selection Gateway (SSG) to forward packets locally, use the **ssg local-forwarding** command in global configuration mode. To disable local forwarding, use the **no** form of this command.

ssg local-forwarding

no ssg local-forwarding

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	12.1(1) DC1	This command was introduced on the Cisco 6400 node route processor.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Examples The following example enables local forwarding:

```
Router(config)# ssg local-forwarding
```

ssg maxservice

To set the maximum number of services per user, use the **ssg maxservice** command in global configuration mode. To reset the maximum number of services per user to the default, use the **no** form of this command.

```
ssg maxservice number
```

```
no ssg maxservice
```

Syntax Description	<i>number</i>	Maximum number of services per user. The minimum value is 0; the maximum is 20.
---------------------------	---------------	---

Defaults The default maximum number of services per user is 20.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines Use this command to limit the number of services to which a user can be logged on simultaneously.

Examples The following example shows how to set the maximum number of services per user to 10:

```
Router# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# ssg maxservice 10
```

ssg next-hop download

To download the next-hop table from a RADIUS server, use the **ssg next-hop download** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

ssg next-hop download [*profile-name*] [*profile-password*]

no ssg next-hop download [*profile-name*] [*profile-password*]

Syntax Description

<i>profile-name</i>	(Optional) Profile name.
<i>profile-password</i>	(Optional) Profile password.

Defaults

If no profile name and password are provided, the previous profile specified with this command is downloaded. If no previous profile was specified, an error message is generated.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

When this command is used, an entry is made in the running configuration. When the configuration is reloaded, the next-hop table is automatically downloaded. If the **no** form of this command is used to remove the command from the running configuration, a next-hop table will not be automatically downloaded when the configuration is reloaded.

Examples

The following example shows how to download the next-hop table called “MyProfile” from a RADIUS server:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssg next-hop download MyProfile MyProfilePassword
```

Related Commands

Command	Description
clear ssg next-hop	Removes the next-hop table.
show ssg next-hop	Displays the next-hop table.

ssg open-garden

To designate a service as an open garden service, use the **ssg open-garden** command in global configuration mode. To remove a service from the open garden, use the **no** form of this command.

ssg open-garden *profile-name*

no ssg open-garden *profile-name*

Syntax Description	<i>profile-name</i>	Local service profile name.
--------------------	---------------------	-----------------------------

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

Command History	Release	Modification
	12.1(5)DC	This command was introduced on the Cisco 6400 series node route processor.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines	Use this command to designate a service, defined in a local service profile, as an open garden service.
------------------	---

Examples	In the following example, the service called “fictitiousname.com” is defined in a local service profile and added to the open garden:
----------	---

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 251 "Oopengarden1.com"
Router(config-prof)# attribute 26 9 251 "D10.13.1.5"
Router(config-prof)# attribute 26 9 251 "R10.1.1.0;255.255.255.0"
Router(config-prof)# exit
Router(config)# ssg open-garden fictitiousname.com
```

Related Commands	Command	Description
	clear ssg open-garden	Removes open garden configurations and all open garden service objects.
	clear ssg service	Removes an SSG service.
	local-profile	Configures a local service profile.
	show ssg open-garden	Displays all open garden services.
	ssg service-search-order	Specifies the order in which SSG searches for a service profile.

ssg pass-through

To enable transparent pass-through, use the **ssg pass-through** command in global configuration mode. To disable transparent pass-through, use the **no** form of this command

```
ssg pass-through [filter { ip-access-list | ip-extended-access-list | access-list-name } | download
[profile-name | profile-name profile-password]] [downlink | uplink]]
```

```
no ssg pass-through [filter { ip-access-list | ip-extended-access-list | access-list-name } | download
[profile-name | profile-name profile-password]] [downlink | uplink]]
```

Syntax Description		
filter		(Optional) Specify access control for packets.
<i>ip-access-list</i>		(Optional) IP access list (standard or extended).
<i>ip-extended-access-list</i>		(Optional) IP extended access list (standard or extended).
<i>access-list-name</i>		(Optional) Access list name.
download		(Optional) Load a service profile and use its filters as default filters.
<i>profile-name</i>		(Optional) Service profile name.
<i>profile-password</i>		(Optional) Service profile password.
downlink		(Optional) Apply filter to downlink packets.
uplink		(Optional) Apply filter to uplink packets.

Defaults Transparent pass-through is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines Use this command to enable transparent pass-through if you want to allow unauthenticated traffic to pass through the Service Selection Gateway (SSG) in either direction without modification. If you want all traffic to be authenticated by the SSG, use this command to disable transparent pass-through. You can use the filter option to prevent pass through traffic from accessing the specified IP address and subnet mask combinations.

Use the **no** form of this command to remove a transparent pass-through filter that was configured at the command line. This will also remove it from the running configuration.

Examples

The following example shows how to enable SSG transparent pass-through and download a pass-through filter from the AAA server called “filter01”:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z
Router(config)# ssg pass-through
Router(config)# ssg pass-through filter download filter01 cisco

Radius reply received:
    Created Upstream acl from it.
Loading default pass-through filter succeeded.
```

Related Commands

Command	Description
clear ssg pass-through-filter	Removes the downloaded filter for transparent pass-through.
show ssg pass-through-filter	Displays the downloaded filter for transparent pass-through.

ssg port-map destination access-list

To identify packets for port-mapping by specifying an access list to compare against the subscriber traffic, use the **ssg port-map destination access-list** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg port-map destination access list *access-list-number*

no ssg port-map destination access list *access-list-number*

Syntax Description	<i>access-list-number</i>	Integer from 100 to 199 that is the number or name of an extended access list.
---------------------------	---------------------------	--

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

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

Command History	Release	Modification
	12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.	
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.	

Usage Guidelines	When the ssg port-map destination access list command is configured, any traffic going to the default network and matching the access list will be port-mapped.
-------------------------	--



Note

A default network must be configured and routable from Service Selection Gateway (SSG) in order for this command to be effective.

You can use multiple entries of the **ssg port-map destination access-list** command. The access lists are checked against the subscriber traffic in the order in which they are defined.

Examples	In the following example, packets permitted by access list 100 will be port-mapped:
-----------------	---

```
ssg port-map enable
ssg port-map destination access-list 100
ssg port-map source ip Ethernet0/0/0
!
.
.
.
!
access-list 100 permit ip 10.0.0.0 0.255.255.255 host 10.13.6.100
access-list 100 deny ip any any
```

Related Commands

Command	Description
ssg port-map destination range	Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic.

ssg port-map destination range

To identify packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic, use the **ssg port-map destination range** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg port-map destination range from *port-number-1* **to** *port-number-2* [**ip** *ip-address*]

no ssg port-map destination range from *port-number-1* **to** *port-number-2* [**ip** *ip-address*]

Syntax Description

from	Specifies lower end of TCP port range.
<i>port-number-1</i>	Port number at lower end of TCP port range.
to	Specifies higher end of TCP port range.
<i>port-number-2</i>	Port number at higher end of TCP port range.
ip <i>ip-address</i>	(Optional) Destination IP address in the packets.

Defaults

If an IP address is not specified, Service Selection Gateway (SSG) will allow any destination IP address in the subscriber traffic to be port-mapped, as long as the packets match the specified port ranges.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

If the destination IP address is not configured, a default network must be configured and routable from SSG in order for this command to be effective.

If the destination IP address is not configured, any traffic going to the default network with the destination port will fall into the destination port range and will be port-mapped.

You can use multiple entries of the **ssg port-map destination range** command. The port ranges are checked against the subscriber traffic in the order in which they were defined.

Examples

In the following example, packets that are going to the default network and have a destination port within the range 8080 to 8081 will be port-mapped:

```
Router(config)# ssg port-map destination range from 8080 to 8081
```

Related Commands

Command	Description
ssg port-map destination access-list	Identifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.

ssg port-map enable

To enable the Service Selection Gateway (SSG) port-bundle host key, use the **ssg port-map enable** command in global configuration mode. To disable the SSG port-bundle host key, use the **no** form of this command.

ssg port-map enable

no ssg port-map enable

Syntax Description This command has no arguments or keywords.

Defaults SSG port-bundle host key is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(2)B	This command was introduced on the Cisco 6400 series.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines This command will not take effect until the router has been reloaded.

The SSG Port-Bundle Host Key feature requires Cisco Service Selection Dashboard (SSD) Release 3.0(1) or Cisco Subscriber Edge Services Manager (SESM) Release 3.1(1). If you are using an earlier release of SSD, use the **no ssg port-map enable command** to disable the SSG Port-Bundle Host Key feature.

Examples The following example shows how to enable the SSG port-bundle host key:

```
Router(config)# ssg port-map enable
```

Related Commands	Command	Description
	ssg port-map destination access-list	Identifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.
	ssg port-map destination range	Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic.
	ssg port-map source ip	Specifies SSG source IP addresses to which to map the destination IP addresses in subscriber traffic.

ssg port-map length

To modify the port-bundle length upon the next Service Selection Gateway (SSG) reload, use the **ssg port-map length** command in global configuration mode. To return the port-bundle length to the default value, use the **no** form of this command.

ssg port-map length *bits*

no ssg port-map length *bits*

Syntax Description	<i>bits</i>	Port-bundle length, in bits. The maximum port-bundle length is 10 bits.
---------------------------	-------------	---

Defaults	4 bits
-----------------	--------

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

Command History	Release	Modification
	12.2(2)B	This command was introduced on the Cisco 6400 series.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The port-bundle length is used to determine the number of bundles in one group and the number of ports in one bundle. By default, the port-bundle length is 4 bits. The maximum port-bundle length is 10 bits. See [Table 66](#) for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. Increasing the port-bundle length can be useful when you see frequent error messages about running out of ports in a port bundle, but note that the new value does not take effect until SSG next reloads and Cisco Service Selection Dashboard (SSD) restarts.



Note For each Cisco SSD server, all connected SSGs must have the same port-bundle length.

Table 66 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per SSG Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016

Table 66 *Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values*

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per SSG Source IP Address)
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

Examples

The following example results in 64 ports per bundle and 1008 bundles per group:

```
Router(config)# ssg port-map length 6
```

Related Commands

Command	Description
show ssg port-map status	Displays information on port bundles, including the port-bundle length.

ssg port-map source ip

To specify Service Selection Gateway (SSG) source IP addresses to which to map the destination IP addresses in subscriber traffic, use the **ssg port-map source ip** command in global configuration mode. To remove this specification, use the **no** form of this command.

```
ssg port-map source ip {ip-address | interface}
```

```
no ssg port-map source ip {ip-address | interface}
```

Syntax Description	<i>ip-address</i>	SSG source IP address.
	<i>interface</i>	Interface whose main IP address is used as the SSG source IP address.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.2(2)B	This command was introduced on the Cisco 6400 series.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines With the SSG Port-Bundle Host Key feature, SSG maps the destination IP addresses in subscriber traffic to specified SSG source IP addresses.

All SSG source IP addresses configured with the **ssg port-map source ip** command must be routable in the management network where the Cisco SSD resides.

If the interface for the source IP address is deleted, the port-map translations will not work correctly.

Because a subscriber can have several simultaneous TCP sessions when accessing a web page, SSG assigns a bundle of ports to each subscriber. Because the number of available port bundles is limited, you can assign multiple SSG source IP addresses (one for each group of port bundles). By default, each group has 4032 bundles, and each bundle has 16 ports. To modify the number of bundles per group and the number of ports per bundle, use the **ssg port-map length** global configuration command.

Examples The following example shows the SSG source specified with an IP address and with specific interfaces:

```
Router(config)# ssg port-map source ip 10.0.50.1
Router(config)# ssg port-map source ip Ethernet 0/0/0
Router(config)# ssg port-map source ip Loopback 1
```

■ ssg port-map source ip

Related Commands

Command	Description
ssg port-map length	Modifies the port-bundle length upon the next SSG reload.

ssg profile-cache

To enable caching of user profiles for non-PPP users, use the **ssg profile-cache** command in global configuration mode. To disable caching of user profiles, use the **no** form of this command.

ssg profile-cache

no ssg profile-cache

Syntax Description This command has no arguments or keywords.

Defaults User-profile caching is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(2)B	This command was introduced.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines The **ssg profile-cache** command allows Service Selection Gateway (SSG) to cache the user profiles of non-PPP users. User profiles of PPP and RADIUS proxy users are always cached by SSG by default. In situations in which the user profile is not available from other sources, SSG user-profile caching makes the user profile available for RADIUS status queries, providing support for single-sign-on functionality and for failover from one Subscriber Edge Services Manager (SESM) to another.

In order for a user profile to be cached, the **ssg profile-cache** command must be configured before account login occurs. Once the user authentication has been done (as part of the account login), the host object is created, and the user profile is cached.



Note

If you are using SSG with the SESM in Lightweight Directory Access Protocol (LDAP) mode, you may want to disable SSG user-profile caching in order to save memory and improve scalability. SSG user-profile caching is required only when SSG is used with the SESM in RADIUS mode.

Examples The following example shows how to enable user-profile caching:

```
Router(config)# ssg profile-cache
```

ssg qos police

To enable the limiting transmission rates for an Service Selection Gateway (SSG) subscriber or for a service being used by an SSG subscriber, use the **ssg qos police** command in global configuration mode. To disable the limiting of transmission rates, use the **no** form of this command.

ssg qos police [user | session]

no ssg qos police [user | session]

Syntax Description	user	(Optional) Specifies per-user policing. Per-user policing is used to police bandwidth allocations for separate subscribers of an SSG service.
	session	(Optional) Specifies per-session policing. Per-session policing is used to police the bandwidth used by one subscriber for multiple services.

Defaults Traffic is forwarded with no SSG policing restrictions if the **ssg qos police** command is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines This command enables the SSG Hierarchical Policing feature, which is used to limit the output transmission rate for a subscriber or for a specific SSG service used by a subscriber. The parameters used to police traffic (committed rate, normal burst, and excess burst) are configured in a RADIUS user profile (per-user policing) or a RADIUS service profile (per-session policing) by using the Q option.

Examples The following is an example of a user profile with the SSG Hierarchical Policing enabled for downstream traffic. In this example, an excess burst size is set at 0 so all dropped packets are tail-dropped. In this particular profile, only downstream traffic is policed (although it is important to note that an upstream token bucket algorithm would operate identically to the downstream policing algorithm).

```
user = johndoe
radius = 7200-SSG-v1.1
check_items= {
2 = cisco
}
reply_attributes={
9,250="Nproxy_ser"
9,250="Ntunnel_ser"
9,250="QD8000;2000;0"
```

Per-user policing must be enabled on the router before the traffic directed to the subscriber is policed. Per-user policing is enabled on the router by entering the following global configuration command:

```
Router(config)# ssg qos police user
```



Note

The following steps provide an example of how traffic going to the subscriber is treated in the example configuration. Because packet sizes are variable, the packet sizes used in this example are created for the sake of the example.

The token bucket starts at 1000 tokens. Although the committed rate is specified in bits per seconds, the token bucket operates based on bytes. 8000 bits is equal to 1000 bytes, so a full token bucket has 1000 tokens. The normal burst parameter is set at 2000. For the sake of the example, no actual debt has been accrued before the arrival of the first packet.

- The first packet is 500 bytes and arrives 3/4 second after the last packet.
 - The packet size is 500 bytes.
 - The time difference (td) is 3/4 of a second.
 - $\text{actual_debt} = \text{previous_actual_debt} + \text{packet_size} = 0 + 500 = 500$
 - $\text{tokens} = \text{committed_rate} * \text{td} = 1000 * 3/4 = 750$
 - $750 > 500$. Therefore, the tokens are greater than the actual debt.

Because tokens are greater than the actual debt, the user has been idle for a sufficient amount of time and the packet is transmitted.
- The second packet is 1500 bytes and arrives 1/2 second after the previous packet.
 - The packet size is 1500 bytes.
 - The td is 1/2 of a second.
 - $\text{actual_debt} = 0 + 1500 = 1500$
 - $\text{tokens} = 1000 * 1/2 = 500$
 - $500 < 1500$. Therefore, the tokens are less than the actual debt. Because the tokens are less than the actual debt, an updated actual debt must be calculated and compared to the normal burst size.
 - $\text{New actual_debt} = \text{previous_actual_debt} - \text{tokens} = 1500 - 500 = 1000$
 - Normal burst is configured at 2000.
 - $1000 < 2000$. Because the actual debt is less than the normal burst size, the packet is forwarded.
- The next packet is 4000 bytes and it arrives 1/2 second later.
 - The packet size is 4000 bytes.
 - The td is 1/2 second.
 - $\text{actual_debt} = \text{previous_actual_debt} + \text{packet_size} = 1000 + 4000 = 5000$
 - $\text{tokens} = 1000 * 1/2 = 500$
 - $500 < 5000$. The tokens are less than the actual debt, so the new actual debt must be computed.
 - $\text{actual_debt} = \text{previous_actual_debt} - \text{tokens} = 5000 - 500 = 4500$
 - $4500 > 2000$. Because the actual debt is greater than the normal burst size, the packet is dropped.

Future packets will be policed similarly on the basis of this algorithm.

Related Commands	Command	Description
	attribute	Specifies the attributes of a service profile for SSG. The parameters that are used by the token bucket to police traffic are specified using the attribute command.
	show ssg host	Displays information about an SSG host, including whether policing is enabled or disabled and the policing configurations of a particular host.
	show ssg connection	Displays information about a particular SSG connection, including the policing parameters.

ssg radius-helper

To enable communications with the Cisco Service Selection Dashboard (SSD) and specify port numbers and secret keys for receiving packets, use the **ssg radius-helper** command in global configuration mode. To disable communications with the Cisco SSD, use the **no** form of this command.

ssg radius-helper [**acct-port** *port-number* | **auth-port** *port-number* | **key** *key*]

no ssg radius-helper [**acct-port** *port-number* | **auth-port** *port-number* | **key** *key*]

Syntax Description

acct-port <i>port-number</i>	(Optional) UDP ¹ destination port for RADIUS accounting requests; the host is not used for accounting if set to 0. The default is 1646.
auth-port <i>port-number</i>	(Optional) UDP destination port for RADIUS authentication requests; the host is not used for authentication if set to 0. The default is 1645.
key <i>key</i>	(Optional) Key shared with the RADIUS clients

1. UDP = User Datagram Protocol

Defaults

The default port number for **acct-port** is 1646.
The default port number for **auth-port** is 1645.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

You must use this command to specify a key so that SSG can communicate with the Cisco SSD.

Examples

The following example shows how to enable communication with the Cisco SSD:

```
Router# configure terminal
```

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

```
Router(config)# ssg radius-helper acct-port 1646 auth-port 1645
```

```
Router(config)# ssg radius-helper key MyKey
```

ssg radius-proxy

To enable SSG RADIUS Proxy, use the **ssg radius-proxy** command in global configuration mode. To prevent further connection of proxy users, use the **no** form of this command

ssg radius-proxy

no ssg radius-proxy

Syntax Description This command has no arguments or keywords.

Defaults SSG RADIUS Proxy is not enabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Use this command to enable SSG RADIUS Proxy.

This command also enables SSG-radius-proxy configuration mode. You must enable SSG with the **ssg enable** command before you can enter the **ssg radius-proxy** command. If you do not enter the **ssg radius-proxy** command, SSG continues to proxy RADIUS packets containing SSG vendor-specific attributes (VSAs) received from the Service Selection Dashboard (SSD), but does not act as a generic RADIUS proxy.

The **no ssg radius-proxy** command does not log off RADIUS client hosts that are already logged in.

If you configure the **no ssg radius-proxy** command, no further connections of proxy users are allowed, but hosts from already configured RADIUS clients remain connected. If you subsequently configure the **ssg radius-proxy** command, the previous RADIUS proxy configuration is restored.

Examples The following example enables SSG RADIUS Proxy:

```
ssg enable
ssg radius-proxy
```

Related Commands	Command	Description
	address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
	clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.

Command	Description
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
forward accounting-start-stop	Proxies accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.
idle-timeout (SSG)	Configures a host object timeout value.
server-port	Defines the ports for the SSG RADIUS proxy.
show ssg tcp-redirect group	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg enable	Enables SSG.

ssg service-password

To specify the password for downloading a service profile, use the **ssg service-password** command in global configuration mode. To disable the password, use the **no** form of this command.

ssg service-password *password*

no ssg service-password *password*

Syntax Description	<i>password</i> Service profile password.
---------------------------	---

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

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

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.	
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.	

Usage Guidelines	This command sets the password required to authenticate with the authentication, authorization, and accounting (AAA) server and download a service profile.
-------------------------	---

Examples	The following example shows how to set the password for downloading a service profile:
-----------------	--

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssg service-password MyPassword
```

ssg service-search-order

To specify the order in which Service Selection Gateway (SSG) searches for a service profile, use the **ssg service-search-order** command in global configuration mode. To disable the search order, use the **no** form of this command.

```
ssg service-search-order {local | remote | local remote | remote local}
```

```
no ssg service-search-order {local | remote | local remote | remote local}
```

Syntax Description

local	Search for service profiles in local Flash memory.
remote	Search for service profiles on a RADIUS server.
local remote	Search for service profiles in local Flash memory, then on a RADIUS server.
remote local	Search for service profiles on a RADIUS server, then in local Flash memory.

Defaults

The default search order is **remote**; that is, SSG searches for service profiles on the RADIUS server.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

SSG can search for service profiles in local Flash memory, on a remote RADIUS server, or both. The possible search orders are:

- Local—search only in Flash memory
- Remote—search only on the RADIUS server
- Local remote—search in Flash memory first, then on the RADIUS server
- Remote local—search on the RADIUS server, then in Flash memory

Examples

The following example shows how to set the search order to local remote, so that SSG will always look for service in Flash memory first, then on the RADIUS server:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ssg service-search-order local remote
```

Related Commands	Command	Description
	show ssg binding	Configures a local RADIUS service profile.

ssg tcp-redirect

To enable SSG TCP redirection and SSG-redirect mode, use the **ssg tcp-redirect** command in global configuration mode. To disable SSG TCP redirection, use the **no** form of this command.

ssg tcp-redirect

no ssg tcp-redirect

Syntax Description SSG TCP redirect is not enabled.

Defaults This command has no default behavior.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced. This command replaces the ssg http-redirect group command.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines Use this command to enable SSG TCP redirection. This command also enables SSG-redirect mode. The **no ssg tcp-redirect** command disables SSG TCP Redirect and removes all configurations created in the SSG-redirect mode. You must enable SSG by issuing the **ssg enable** command before you can configure SSG TCP redirect.

Examples The following example shows how to select a captive portal group for redirection of traffic from unauthorized users. In the following example, traffic from unauthorized users is redirected to the captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
  redirect unauthenticated-user to RedirectServer
```

The following example shows how to define a port list named “WebPorts” and adds TCP ports 80 and 8080 to the port list. Port 8080 is configured to be redirected by the captive portal group named “Redirect Server”:

```
ssg enable
ssg tcp-redirect
  port-list WebPorts
    port 80
    port 8080
  exit
  redirect port 8080 to RedirectServer
```

Related Commands	Command	Description
	debug ssg tcp-redirect	Turns on debug information for the SSG TCP Redirect for Services feature.
	network (ssg-redirect)	Adds an IP address to a named network list.
	network-list	Defines a list of one or more IP networks that make up a named network list.
	port (ssg-redirect)	Adds a TCP port to a named port list.
	port-list	Defines a list of one or more TCP ports that make up a named port list and enters SSG-redirect-port configuration mode.
	redirect captivate advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
	redirect captivate initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
	redirect port to	Marks a TCP port or named TCP port list for SSG TCP redirection.
	redirect smtp group	Selects a captive portal group for redirection of SMTP traffic.
	redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.
	redirect unauthenticated-user to	Redirects traffic from authenticated users to a specified captive portal group.
	server (SSG)	Adds a server to a captive portal group.
	server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
	show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
	show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
	ssg enable	Enables SSG.
	ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

ssg vc-service-map

To map virtual circuits (VCs) to service names, use the **ssg vc-service-map** command in global configuration mode. To disable VC-to-service-name mapping, use the **no** form of this command.

```
ssg vc-service-map service-name [interface interface-number] start-vpi | start-vpilvci [end-vpi | end-vpilvci] exclusive | non-exclusive
```

```
no ssg vc-service-map service-name [interface slot-module-port] start-vpi | start-vpilvci [end-vpi | end-vpilvci] exclusive | non-exclusive
```

Syntax Description	
<i>service-name</i>	Service name.
interface	(Optional) Specifies a service name mapping for an interface.
<i>interface-number</i>	(Optional) Number of the interface (such as 1/0) through which SSG will access the mapped service.
<i>start-vpi</i>	Virtual path identifier (VPI) or start of a range of VPIs that will be mapped to the service. The range is from 0 to 255.
<i>start-vpilvci</i>	VPI/virtual channel identifier (VCI) or start of a range of VPI/VCIs that will be mapped to the service. The range is from 0 to 255.
<i>end-vpi</i>	(Optional) End of a range of VPIs that will be mapped to the service. The range is from 0 to 255.
<i>end-vpilvci</i>	(Optional) End of a range of VPI/VCIs that will be mapped to the service. The range is from 0 to 255.
exclusive	Users will be able to access only the mapped service.
non-exclusive	Users will be able to access the mapped service and any other services to which they are subscribed. Users can log in to the Service Selection Gateway (SSG) with a username and password, establishing a non-PPP Termination Aggregation (PTA) session, and a PTA session to the mapped service will be established by default. If non-exclusive is specified for the service mapping, users can also establish a PTA session to another service to which they are subscribed.

Defaults The service mapping is **non-exclusive** by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use this command to map VCs to service names. If you specify a VC-to-service-name mapping as exclusive, specifying a username will log you in to the mapped service. However, specifying username@service will not log you in. If you specify a mapping as nonexclusive, specifying a username will log you in to the mapped service. However, username@service1 will log you in to service1.

Examples

The following example shows how to map all users coming into SSG on VPI/VCI 3/33 to the service “Worldwide” exclusively:

```
Router# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# ssg vc-service-map Worldwide 3/33 exclusive
```

Related Commands

Command	Description
ssg vc-service-map	Displays VC-to-service-name mappings.

subscriber access

To configure a network access server (NAS) to enable Subscriber Service Switch (SSS) to preauthorize the NAS port identifier (NAS-Port-ID) string before authorizing the domain name, use the **subscriber access** command in global configuration mode. To disable SSS preauthorization, use the **no** form of this command.

```
subscriber access {pppoe | pppoa} pre-authorize nas-port-id [default | list-name] [send
username]
```

```
no subscriber access {pppoe | pppoa} pre-authorize nas-port-id
```

Syntax Description		
pppoe		Specifies PPP over Ethernet (PPPoE).
pppoa		Specifies PPP over ATM (PPPoATM).
pre-authorize nas-port-id		Signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name.
default		(Optional) Uses the default method list name instead of the named <i>list-name</i> argument.
<i>list-name</i>		(Optional) Authentication, authorization, and accounting (AAA) authorization configured on the LAC.
send username		(Optional) Specifies to send the authentication username of the session in the Change_Info attribute (attribute 77).

Defaults Preauthorization is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(8)B	This command was introduced on the Cisco 6400 series, the Cisco 7200 series, and the Cisco 7401 Application Specific Router (ASR).
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, and the pppoe and pppoa keywords were added.
	12.4(2)T	The send username keyword was added.
	12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7301, Cisco 7204VXR, and Cisco 7206VXR routers.

Usage Guidelines The NAS-Port-ID string is used to locate the first service record, which may contain one of three attributes, as follows:

- A restricted set of values for the domain substring of the unauthenticated PPP name.

This filtered service key then locates the final service. See the **vpdn authorize domain** command for more information.

- PPPoE session limit.
- The logical line ID (LLID).

Once NAS port authorization has taken place, normal authorization, which is usually the domain authorization, continues.

Logical Line ID

The LLID is an alphanumeric string of from 1 to 253 characters that serves as the logical identification of a subscriber line. LLID is maintained in a RADIUS server customer profile database and enables users to track their customers on the basis of the physical lines on which customer calls originate.

Downloading the LLID is also referred to as “preauthorization” because it occurs before normal virtual private dialup network (VPDN) authorization downloads L2TP tunnel information.

This command enables LLID and SSS querying only for PPP over Ethernet over ATM (PPPoEoATM) and PPP over Ethernet over VLAN (PPPoEoVLAN or Dot1Q) calls; all other calls, such as ISDN, are not supported.

Per-NAS-Port Session Limits for PPPoE

Use this command to configure SSS preauthorization on the LAC so that the PPPoE per-NAS-port session limit can be downloaded from the customer profile database. To use PPPoE per-NAS-port session limits, you must also configure the PPPoE Session-Limit per NAS-Port Cisco attribute-value pair in the user profile.

Examples

The following example signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name. This policy applies only to sessions that have a PPPoE access type.

```

aaa new-model
aaa group server radius sg_llid
  server 172.20.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_group
  server 172.20.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization cfg-commands
aaa authorization network default group sg_group
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_group password 0 lab
vpdn enable
!
vpdn-group 2
  request-dialin
  protocol l2tp
  domain group.com
  initiate-to ip 10.1.1.1
  local name s7200_2
!
vpdn-group 3
  accept dialin
  protocol pppoe
  virtual-template 1
!
! Signals Subscriber Service Switch to preauthorize the NAS-Port-ID string before
! authorizing the domain name.
subscriber access pppoe pre-authorize nas-port-id mlist_llid
!

```

```

interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 10.2.2.2 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0.1 point-to-point
 pvc 1/100
 encapsulation aa15snap
 protocol pppoe
!
interface virtual-templatel
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.20.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.20.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1

```

The following example is identical to the previous example except that it also adds support for sending the PPP authenticating username with the preauthorization in the Connect-Info attribute. This example also includes command line interface (CLI) suppression on the LLID if the username that is used to authenticate has a domain that includes #184.

```

aaa new-model
aaa group server radius sg_llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_group
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group sg_group
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_group password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain group.com
 domain group.com#184
 initiate-to ip 10.1.1.1
 local name s7200_2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
 accept dialin
 proccotol pppoe
 virtual-template 1

```

```
!
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
l2tp attribute clid mask-method	Configure a NAS to provide L2TP calling line ID suppression for calls belonging to a VPDN group.
subscriber authorization enable	Enables SSS type authorization.
vpdn authorize domain	Enables domain preauthorization on a NAS.
vpdn l2tp attribute clid mask-method	Configure a NAS to provide L2TP calling line ID suppression globally on the router.

subscriber authorization enable

To enable Subscriber Service Switch type authorization, use the **subscriber authorization enable** command in global configuration mode. To disable the Subscriber Service Switch authorization, use the **no** form of this command.

subscriber authorization enable

no subscriber authorization enable

Syntax Description This command has no arguments or keywords.

Defaults Authorization is disabled.

Command Modes Global configuration

Release	Modification
12.2(13)T	This feature was introduced.

Usage Guidelines The **subscriber authorization enable** command triggers Subscriber Service Switch type authorization for local termination, even if virtual private dialup network (VPDN) and Stack Group Bidding Protocol (SGBP) are disabled.

Examples The following example enables Subscriber Service Switch type authorization:

```
subscriber authorization enable
```

Command	Description
subscriber access	Enables Subscriber Service Switch preauthorization.
vpdn authorize domain	Enables domain preauthorization on a NAS.

SVC

To create an ATM switched virtual circuit (SVC) and specify the destination network service access point (NSAP) address on a main interface or subinterface, use the **svc** interface configuration command. To disable the SVC, use the **no** form of this command.

```
svc [name] [nsap address] [ces]
```

```
no svc [name] [nsap address] [ces]
```

Syntax Description

<i>name</i>	(Optional) The name of the SVC and map. The name can be up to 16 characters long. A name is required when creating passive a CES SVC.
nsap address	(Optional) The destination ATM NSAP address. Must be exactly 40 hexadecimal digits long and in the correct format. See the “Usage Guidelines” section. An NSAP address is required when creating an active CES SVC.
ces	(Optional) Circuit Emulation Service encapsulation. This keyword is available on the OC-3/STM-1 ATM Circuit Emulation Service network module only.

Defaults

No NSAP address is defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(2)T	The ces keyword was added to configure CES encapsulation when using the OC-3/STM-1 ATM Circuit Emulation Service network module on Cisco 2600 and Cisco 3600 series platform.
12.1(3)T	This command was modified to allow an SVC to be created without having a specific NSAP address associated with it.

Usage Guidelines

After configuring the parameters for an ATM SVC, you must exit the interface-ATM-VC or interface-CES-VC configuration mode in order to enable the SVC settings.

Once you specify a *name* for an SVC, you can reenter the interface-ATM-VC or interface-CES-VC configuration mode by simply entering **svc name**.

You can remove an NSAP address and any associated parameters by entering **no svc name** or **no svc nsap address**.

Creating an SVC without a specific NSAP address will allow a router to accept calls from any ATM address, and allow multiple VCs to be set up using the same configuration.

Use the **ces** keyword to configure an active or passive CES SVC. An active CES SVC can originate and terminate SVC calls. A passive CES SVC can only terminate calls.

Note Cisco IOS does not support creation of SVCs on a point-to-point subinterface.

Examples

SVC Example

The following example creates an SVC called “chicago” on ATM interface 2/0/0:

```
interface atm 2/0/0
  svc chicago
```

SVC with NSAP Address Example

The following example creates an SVC with the name “lion” and specifies the 40-digit hexadecimal destination ATM NSAP address:

```
svc lion nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
```

Active CES SVC Example

The following example creates an active CES SVC named "ces1":

```
interface atm 1/0
  svc ces1 nsap 47.00.00.000000.0040.0B0A.2501.ABC1.01.01.00 ces
```

Passive CES SVC Example

The following example creates a passive CES SVC named "ces2":

```
interface atm 1/0
  svc ces2 ces
```