



Broadband Access: Service Selection Gateway Commands

Use the commands described in this chapter to configure Service Selection Gateway (SSG) switching solutions for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as digital subscriber lines (DSL), cable modems, or wireless. SSG allows simultaneous access to network services.

For information about how to configure SSG, refer to the “[Service Selection Gateway](#)” 12.2(8)T feature module and the [Service Selection Gateway \(SSG\) Features in Release 12.2\(13\)T](#) index.

address-pool

To define local IP pools that are to be used by Service Selection Gateway (SSG) to assign IP addresses to users for which SSG is acting as a RADIUS client, use the **address-pool** command in SSG-radius-proxy mode. To remove a local IP pool, use the **no** form of this command.

address-pool *start-ip end-ip* [**domain** *domain-name*]

no address-pool *start-ip end-ip* [**domain** *domain-name*]

Syntax Description

<i>start-ip</i>	First IP address of the local IP address pool.
<i>end-ip</i>	Last IP address of the local IP address pool.
domain	(Optional) IP address pool for a specific domain.
<i>domain-name</i>	(Optional) Name of the domain.

Defaults

SSG does not assign IP addresses from a local IP pool.

Command Modes

SSG-radius-proxy

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 T.

Usage Guidelines

Use this command to configure SSG to assign an IP address taken from a local pool to a user for which SSG is acting as a RADIUS client. SSG assigns an IP address from a local pool only when one has not been assigned by one of the following methods:

- Assignment in the Access-Accept from the AAA server
- Assignment in the Access-Request received from the client
- Assignment from an Autodomain service (tunnel or proxy) that does not have the **auto-domain nat user-address** configuration enabled



Note

You must have SSG Autodomain configured in order for an IP address to be assigned from an Autodomain tunnel. See [SSG AutoDomain](#) for more information about configuring SSG Autodomain.

You can use this command to define a global local IP address pool or an IP address pool for a specific domain by using the **domain** keyword. You cannot create pools with more than 20,000 addresses.



Note

Using IP address pools within SSG is completely standalone and unrelated to Cisco IOS IP local pools.

Examples

The following example shows how to configure a local IP address pool for SSG:

```
address-pool 172.16.16.0 172.16.20.0
```

The following example shows how to configure a local IP address pool for the domain named “cisco”.

```
address-pool 172.21.21.0 172.21.25.0 domain cisco
```

Related Commands

Command	Description
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
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 a specific domain.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.
ssg tcp-redirect	Configures the RADIUS proxy IP address and shared secret.

attribute

To configure an attribute in a local service profile, use the **attribute** command in profile configuration mode. To delete an attribute from a service profile, use the **no** form of this command.

attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

no attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

Syntax Description

<i>radius-attribute-id</i>	RADIUS attribute ID to be configured.
<i>vendor-id</i>	(Optional) Vendor ID. Required if the RADIUS attribute ID is 26, indicating a vendor-specific attribute (VSA) . The Cisco vendor ID is 9.
<i>cisco-vsa-type</i>	(Optional) Cisco VSA type. Required if the vendor ID is 9, indicating a Cisco VSA.
<i>attribute-value</i>	Attribute value. The following optional attribute values are also supported: <ul style="list-style-type: none"> Linterval—Required to change an interim accounting interval. Specifies the new accounting interval in seconds. Q—Configures the token bucket parameters for the Service Selection Gateway (SSG) Hierarchical Policing feature.

Defaults

For the **Linterval** option: If the L option is not defined, the accounting records for a service profile will be sent at the interval configured by the **ssg accounting interval** command. If the **ssg accounting interval** command is not set, the accounting records are sent every 600 seconds.

Otherwise, no default behavior or values are set.

Command Modes

Profile configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(4)B	The L and Q attributes were introduced as an <i>attribute-value</i> .
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified for Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to configure attributes in local service profiles.

For the SSG Open Garden feature, use this command to configure the Service Route, DNS Server Address, and Domain Name attributes in a local service profile before adding the service to the open garden.

To change the SSG accounting interval for a service profile, use the *Linterval* option in the **attribute** command. For example, if L80 is entered as the attribute value, the service profile sends accounting information every 80 seconds. Interim accounting can be disabled by entering the value (in seconds) as 0 (for instance, L0). When interim accounting is disabled, the normal accounting stops and starts are still sent.

For the SSG Hierarchical Policing feature, use the Q option to configure the token bucket parameters (token rate, normal burst, and excess burst). The syntax for the Q option is as follows:

```
Router(config-prof)# attribute radius-attribute-id vendor-id cisco-vsa-type
"QU;upstream-committed-rate;upstream-normal-burst;
[upstream-excess-burst];D;downstream-committed-rate;
downstream-normal-burst;[downstream-excess-burst]"
```

The variables are used to configure upstream (U) and downstream (D) policing. The upstream traffic is the traffic that travels from the subscriber to the network, and the downstream traffic is the traffic that travels from the network to the subscriber.

Examples

In the following example, the Cisco AV pair Upstream Access Control List (inac1) attribute is configured in the local service profile called "cisco.com":

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "ip:inac1#101=deny tcp 10.2.1.0 0.0.0.255 any eq 21"
```

In the following example, the Session-Timeout attribute is deleted from the local service profile called "cisco.com":

```
Router(config)# local-profile cisco.com
Router(config-prof)# no attribute 27 600
```

In the following example, the local profile cisco.com is configured to send an interim accounting update every 90 seconds:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "L90"
```

In the following example, the SSG Hierarchical Policing parameters are set for upstream and downstream traffic:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 251 "QU:8000:16000:20000:D10000:20000:30000"
```

In the following example, an open garden service called "opencisco.com" is defined.

```
Router(config)# local-profile opencisco.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 opencisco.com
```

Related Commands

Command	Description
debug ssg data	Displays SSG QoS information.
local-profile	Configures a local service profile.
show ssg connection	Displays information about a particular SSG connection, including the policing parameters.

Command	Description
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 open-garden	Displays a list of all configured open garden services.
ssg accounting interval	Specifies the interval at which accounting updates are sent to the server.
ssg open-garden	Designates a service, defined in a local service profile, to be an open garden service.
ssg qos police	Enables SSG Hierarchical Policing on a router.

clear ssg connection

To remove the connections of a given host and a service name, use the **clear ssg connection** command in privileged EXEC mode.

```
clear ssg connection ip-address service-name [interface]
```

Syntax Description

<i>ip-address</i>	IP address of an active Service Selection Gateway (SSG) connection.
<i>service-name</i>	Name of an active SSG connection.
<i>interface</i>	(Optional) Interface to which the host is connected.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(2)B	The <i>interface</i> argument was added.
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 remove the service connection for Service1 to host 192.168.1.1, connected through Fast Ethernet:

```
Router# clear ssg connection 192.168.1.1 fastethernet Service1
```

Related Commands

Command	Description
show ssg connection	Displays the connections of a given host and a service name.

clear ssg host

To remove or disable a given host or subscriber, use the **clear ssg host** command in privileged EXEC mode.

clear ssg host *ip-address interface*

Syntax Description		
	<i>ip-address</i>	IP address of the host or subscriber.
	<i>interface</i>	Interface through which the host or subscriber is connected.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(2)B	The <i>interface</i> argument was added for the SSG Host Key feature.
	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 remove the connection for host 192.168.1.1:

```
Router# clear ssg host 192.168.1.1 fastethernet
```

Related Commands	Command	Description
	show ssg host	Displays the information about a subscriber and current connections of the subscriber.

clear ssg next-hop

To remove a next-hop table, use the **clear ssg next-hop** command in privileged EXEC mode.

```
clear ssg next-hop
```

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

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 If you use this command to clear the next-hop table, nothing appears when you use the **show ssg next-hop** command. However, the next-hop table will still appear in the running configuration. To remove the next-hop table from the running configuration, use the **no** form of the **ssg next-hop download** command.

Examples The following example shows how to remove the next-hop table:

```
Router# clear ssg next-hop
```

Related Commands	Command	Description
	show ssg next-hop	Displays the next-hop table.
	ssg next-hop download	Downloads the next-hop table from a RADIUS server.

clear ssg open-garden

To remove open garden configurations and all open garden service objects, use the **clear ssg open-garden** command in privileged EXEC mode.

clear ssg open-garden

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC

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 This command removes the open garden configuration by deleting all instances of the **ssg open-garden** global configuration command. This command also removes the service object of all the open garden services. The local service profiles of the open garden services are not deleted from the configuration.

Examples In the following example, all open garden services are displayed and then removed:

```
Router# show ssg open-garden
```

```
nrp1-nrp2_og1
nrp1-nrp2_og2
nrp1-nrp2_og3
nrp1-nrp2_og4
```

```
Router# clear ssg open-garden
Router# show ssg open-garden
Router#
```

Related Commands	Command	Description
	local-profile	Configures a local service profile.
	show ssg open-garden	Displays a list of all configured open garden services.
	ssg open-garden	Designates a service, defined in a local service profile, as an open garden service.

clear ssg pass-through-filter

To remove the downloaded filter for transparent pass-through, use the **clear ssg pass-through-filter** command in privileged EXEC mode.

clear ssg pass-through-filter

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

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 Removing the filter allows unauthenticated traffic to pass through the Service Selection Gateway in either direction without modification. If you use this command to clear the downloaded transparent pass-through filter, nothing will be displayed when you use the **show ssg pass-through-filter** command. However, the transparent pass-through filter will still appear in the running configuration. To remove the transparent pass-through filter from the running configuration, use the **no** form of the **ssg pass-through** command.

Examples The following example shows how to remove the downloaded transparent pass-through filter:

```
Router# clear ssg pass-through-filter
```

Related Commands	Command	Description
	show ssg pass-through-filter	Displays the downloaded filter for transparent pass-through.
	ssg pass-through	Enables transparent pass-through.

clear ssg pending-command

To remove all pending commands, use the **clear ssg pending-command** command in privileged EXEC mode.

clear ssg pending-command

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

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 clear pending commands.

Examples The following example shows how to clear pending commands:

```
Router# clear ssg pending-command
```

Related Commands	Command	Description
	show ssg pending-command	Displays current pending commands.

clear ssg radius-proxy client-address

To clear all hosts connected to a specific RADIUS client, use the **clear ssg radius-proxy client-address** command in privileged EXEC mode.

client ssg radius-proxy client-address *ip-address*

Syntax Description

<i>ip-address</i>	IP address of a RADIUS client.
-------------------	--------------------------------

Command Modes

Privileged EXEC

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 clear all hosts connected to a specific RADIUS client. This command deactivates and destroys all host objects associated with the specified RADIUS client.

Examples

The following example shows how to clear all hosts connected to the RADIUS client that has the IP address 172.16.0.0:

```
clear ssg radius-proxy client-address 172.16.0.0
```

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 nas-address	Clears all hosts connected to a specific NAS.
idle-timeout (SSG)	Configures a host object timeout value.
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 radius-proxy	Enables SSG RADIUS Proxy.
ssg tcp-redirect	Configures the RADIUS proxy IP address and shared secret.

clear ssg radius-proxy nas-address

To clear all hosts connected to a specific network access server (NAS), use the **clear ssg radius-proxy nas-address** command in privileged EXEC mode.

client ssg radius-proxy nas-address *ip-address*

Syntax Description

<i>ip-address</i>	IP address of a RADIUS client.
-------------------	--------------------------------

Command Modes

Privileged EXEC

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 clear all hosts connected to a specific NAS. This command deactivates and destroys all host objects associated with the specified NAS client.



Note

Service Selection Gateway (SSG) does not currently notify RADIUS clients when a host object is removed from the SSG.

Examples

The following example shows how to clear all hosts connected to the NAS with IP address 172.16.0.0:

```
clear ssg radius-proxy nas-address 172.16.0.0
```

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 nas-address	Clears all hosts connected to a specific RADIUS client.
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 radius-proxy	Enables SSG RADIUS Proxy.
ssg tcp-redirect	Configures the RADIUS proxy IP address and shared secret.

clear ssg service

To remove a service, use the **clear ssg service** command in privileged EXEC mode.

```
clear ssg service service-name
```

Syntax Description	<i>service-name</i>	Name of an active Service Selection Gateway (SSG) service.
---------------------------	---------------------	--

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

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

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 remove services.
-------------------------	--------------------------------------

Examples	The following example shows how to remove a service called “Perftest”:
-----------------	--

```
Router# clear ssg service Perftest
```

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.
	show ssg service	Displays the information for a service.
	ssg bind service	Specifies the interface for a service.

client-address

To configure a RADIUS client IP address and shared secret, use the **client-address** command in SSG-radius-proxy mode. To disable the RADIUS proxy IP address and shared secret, use the **no** form of this command.

client-address *ip-address* **key** *secret*

no client-address *ip-address* **key** *secret*

Syntax Description

<i>ip-address</i>	IP address of a RADIUS client.
key	Shared secret between the Service Selection Gateway (SSG) and the RADIUS client.
<i>secret</i>	Description of the shared secret.

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy

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 configure the RADIUS client to proxy requests from the specified IP address to the RADIUS server. Use the *secret* attribute to configure each client IP with a unique shared secret. This shared secret should be the same one configured on the RADIUS client.

Examples

The following example shows how to configure the RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server and assigns the shared secret "cisco" to the client:

```
client-address 172.16.0.0 key cisco
```

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.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.

Command	Description
forward accounting-start-stop	Proxies accounting start, stop, and update packets generated by any RADIUS client 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 radius-proxy	Enables SSG RADIUS Proxy.

download exclude-profile

To add domain or Access Point Names (APNs) names to the Service Selection Gateway (SSG) Autodomain exclusion list, use the **download exclude-profile** command in SSG-auto-domain mode. To remove a name from the Autodomain exclusion list, use the **no** form of this command.

download exclude-profile *profile-name password*

no download exclude-profile *profile-name password*

Syntax Description

<i>profile-name</i>	Specifies the name for a list of excluded names that may be downloaded from the AAA server.
<i>password</i>	Specifies the password for a list of excluded names that may be downloaded from the AAA server.

Defaults

No default behavior or values.

Command Modes

SSG-auto-domain

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 the **download exclude-profile** command to specify the name and password for a list of names that are excluded from being downloaded from the AAA server. Downloads from the AAA server occur at the time of entering the configuration and also on subsequent Route Processor reloads. By reentering the configuration command, you can synchronize with a modified table on the AAA server by forcing a new download. For every successful exclude-profile download, Service Selection Gateway (SSG) deletes the exclude entries added by the previous exclude-profile download and adds the new downloaded entries to the Autodomain exclusion list. The excluded name list introduces the following new attributes to the SSG Control-Info vendor-specific attributes (VSAs):

X—Excluded name list entry.

A—Add this name to the APN exclusion list.

D—Add this name to the domain name exclusion list.

The following is an example profile using the new exclusion list attributes:

```
abc Password = "cisco" Service-Type = Outbound
Control-Info = XAapn1.gprs
Control-Info = XAapn2.com
Control-Info = XDcisco.com
Control-Info = XDredhotant.com
```

Examples

The following example shows how to add a list of names called “abc” with the password “cisco” to the Autodomain exclusion list:

```
download exclude-profile abc cisco
```

Related Commands

Command	Description
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
nat user-address	Enables Network Address Translation (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.

exclude

To add Access Point Names (APNs) and domain names to a Service Selection Gateway (SSG) Autodomain exclusion list, use the **exclude** command in SSG-auto-domain mode. To remove an APN or domain name from the Autodomain exclusion list, use the **no** form of this command.

```
exclude {apn | domain} name
```

```
no exclude {apn | domain} name
```

Syntax Description

apn	Adds an APN to the exclusion list.
domain	Adds a domain to the exclusion list.
<i>name</i>	Name of the APN or domain to be added to the exclusion list.

Defaults

No default behavior or values.

Command Modes

SSG-auto-domain

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 the **exclude** command to add an APN or a domain to the Autodomain exclusion list. APN and domain names that are not on an exclusion are used to perform Autodomain for a user. You can use the **no download exclude-profile** command to remove a domain or APN name that is downloaded from the AAA server.

Examples

The following example shows how to add the APN named “abc” to the exclusion list:

```
exclude apn abc
```

The following example shows how to add the domain named “xyz” to the exclusion list:

```
exclude domain xyz
```

Related Commands

Command	Description
exclude	Adds to the Autodomain download exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
nat user-address	Enables NAT on Autodomain tunnel service.
select	Configures the Autodomain selection mode.

Command	Description
show ssg auto-domain exclude-profile	Displays the contents of an Autodomain exclude-profile downloaded from the AAA server.
ssg enable	Enables SSG functionality.

forward accounting-start-stop

To proxy accounting start, stop, and update packets generated by any RADIUS clients to the AAA server, use the **forward accounting-start-stop** command in SSG-radius-proxy mode. To stop forwarding accounting start, stop, and update packets, use the **no** form of this command.

forward accounting-start-stop

no forward accounting-start-stop

Syntax Description This command has no arguments or keywords.

Defaults Forward accounting-start-stop is disabled by default.

Command Modes SSG-radius-proxy

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 proxy accounting start, stop, and update packets generated by all RADIUS clients to the AAA server. Disabling this command reduces RADIUS packet traffic and processing for deployments where the billing server is not using these packets for billing purposes.



Note

The **forward accounting-start-stop** command does not affect accounting on and off packets, which are forwarded regardless of this command.

Examples The following example shows how to proxy accounting packets generated by all RADIUS clients to the AAA server:

```

ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 10.1.2.2 key secret1
 client-address 10.2.25.90 key secret2
 client-address 10.0.0.1 key secret3
 client-address 10.23.3.2 key secret4
 idle-timeout 30
 forward accounting-start-stop
 address-pool 10.1.1.1 10.1.40.250
 address-pool 10.1.5.1 10.1.5.30 domain ssg.com

```

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.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
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 radius-proxy	Enables SSG RADIUS Proxy.

idle-timeout (SSG)

To configure a host object timeout value, use the **idle-timeout** command in SSG-radius-proxy mode. To disable the timeout value, use the **no** form of this command.

idle-timeout *timeout*

no idle-timeout *timeout*

Syntax Description

timeout Timeout value in seconds. Valid range is from 30 to 65536.

Defaults

No timeout value is configured.

Command Modes

SSG-radius-proxy

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 configure a timeout value for a host object. Configuring this command prevents dangling host objects on the Service Selection Gateway (SSG). If a RADIUS client reloads and does not indicate its fault condition to the SSG, the SSG retains the host objects that are no longer valid. This command removes all host objects from a RADIUS client that has been idle for the time specified by the *timeout* argument. When configured, this timeout value is added to the host object.



Note

Timeout values configured in the user profile that appear in the Access-Accept take precedence over any timeout value configured by the **idle-timeout** command.

Examples

The following example shows how to configure a timeout value of 60 seconds:

```
ssg radius-proxy
server-port auth 1645 acct 1646
client-address 10.1.2.2 key secret1
client-address 10.2.25.90 key secret2
client-address 10.0.0.1 key secret3
client-address 10.23.3.2 key secret4
idle-timeout 60
forward accounting-start-stop
address-pool 10.1.1.1 10.1.40.250
address-pool 10.1.5.1 10.1.5.30 domain ssg.com
```

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.
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.
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 radius-proxy	Enables SSG RADIUS Proxy.

local-profile

To configure a local service profile and enter profile configuration mode, use the **local-profile** command in global configuration mode. To delete the local service profile, use the **no** form of this command.

local-profile *profile-name*

no local-profile *profile-name*

Syntax Description

profile-name Name of profile to be configured.

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 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 configure local service profiles.

Examples

The following example shows how to configure a RADIUS profile called “fictitiousname.com” and enter profile configuration mode:

```
Router(config)# local-profile fictitiousname.com
Router(config-prof)#
```

In the following example, two services called “og1” and “og2” are defined and added to the open garden:

```
!
ssg open-garden og1
ssg open-garden og2
!
local-profile og1
 attribute 26 9 251 "Oopengarden1.com"
 attribute 26 9 251 "D10.13.1.5"
 attribute 26 9 251 "R10.1.1.0;255.255.255.0"
local-profile og2
 attribute 26 9 251 "Oopengarden2.com"
 attribute 26 9 251 "D10.14.1.5"
 attribute 26 9 251 "R10.2.1.0;255.255.255.0"
 attribute 26 9 251 "R10.3.1.0;255.255.255.0"
!
ssg bind service og2 10.5.5.1
```

Related Commands	Command	Description
	attribute	Configures attributes in local RADIUS profiles.
	show ssg open-garden	Displays a list of all configured open garden services.
	ssg open-garden	Designates a service, defined in a local service profile, as an open garden service.
	ssg service-search-order	Specifies the order in which SSG searches for a service profile.

mode extended

To select extended Autodomain mode, use the **mode extended** command in SSG-auto-domain mode. To reenable basic Autodomain mode, use the **no** form of this command.

mode extended

no mode extended

Syntax Description This command has no arguments or keywords.

Defaults Basic Autodomain mode is selected.

Command Modes SSG-auto-domain

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 the **mode extended** command to select the extended Autodomain mode. In basic Autodomain mode, the profile downloaded from the AAA server for the selected Autodomain name is a service profile, which may or may not contain attributes specific to Service Selection Gateway (SSG). In extended Autodomain mode, the profile is a “virtual user” profile, which may contain a list of services in addition to other account attributes. The “virtual user” profile contains one autoservice to an authenticated service such as a proxy, VPDN, or tunnel. Connection to the autoservice occurs in the same way as in basic Autodomain mode. The host object is not activated until the user is authenticated at the service. The presence of SSD allows the user to access any other service in the specified user profile. Extended mode also enables users with multiple service selection to log on.

Examples The following example shows how to enable extended Autodomain mode:

```

ssg enable
ssg auto-domain
mode extended
select username
exclude apn motorola
exclude domain cisco
download exclude-profile abc password1
nat user-address

```

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

Command	Description
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 auto-domain	Enables SSG Autodomain mode.
ssg enable	Enables SSG functionality.

nat user-address

To enable Network Address Translation (NAT) toward Autodomain service, use the **nat user-address** command in SSG-auto-domain mode. To disable NAT on Autodomain service, use the **no** form of this command.

nat user-address

no nat user-address

Syntax Description

This command has no arguments or keywords.

Defaults

NAT is not applied toward Autodomain services and IP addresses assigned at the tunnel, VPDN, or proxy service will be assigned at the host and then sent back to the RADIUS client. NAT is always applied towards the Autodomain connection regardless of the configuration of the **nat user-address** command when the Access-Request from the RADIUS client contains an IP address.

Command Modes

SSG-auto-domain

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 the **nat user-address** command to enable NAT toward the Autodomain connection. When a host object has not been assigned an IP address using the Access-Request from the RADIUS client, Service Selection Gateway (SSG) by default passes an IP address assigned at the tunnel, VPDN, or proxy service back to the RADIUS client and NAT does not happen toward the Autodomain connection. The **nat user-address** command overrides the default behavior and specifies that NAT should be performed towards Autodomain services. If a host has been assigned an IP address via the Access-Request, NAT happens toward the Autodomain connection regardless of the status of this command.

Examples

The following example enables NAT toward the Autodomain connection:

```

ssg enable
ssg auto-domain
mode extended
select username
exclude apn motorola
exclude domain cisco
download exclude-profile abc password1
nat user-address

```

Related Commands

Command	Description
download exclude-profile	Adds to the Autodomain download exclusion list.
exclude	Configures the Autodomain exclusion list.
mode extended	Enables extended mode for SSG Autodomain.
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.

network (ssg-redirect)

To add an IP address to a named network list, use the **network** command in SSG-redirect-network configuration mode. To remove an IP address from a named network list, use the **no** form of this command.

network *ip-address*

no network *ip-address*

Syntax Description

<i>ip-address</i>	The IP address that is to be added to a named network list.
-------------------	---

Defaults

No default behavior or values.

Command Modes

SSG-redirect-network 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 define an individual network that is found in a named network list. Use the **network-list** command to define and name the network list and the **network** command to add an individual IP address to the named network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example creates a network list named “RedirectNw” and adds IP address 10.0.0.0 255.0.0.0 and address 10.2.2.0 255.255.255.0 to the “RedirectNw” network list:

```
ssg tcp-redirect
network-list RedirectNw
network 10.0.0.0 255.0.0.0
network 10.2.2.0 255.255.255.0
```

Related Commands

Command	Description
network-list	Defines a list of one or more IP networks that make up a named network list.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

network-list

To define a list of one or more IP networks that make up a named network list and to enter SSG-redirect-network configuration mode, use the **network-list** command in SSG-redirect configuration mode. To remove a named network list, use the **no** form of this command.

network-list *network-listname*

no network-list *network-listname*

Syntax Description

<i>network-listname</i>	Defines the name of the network list.
-------------------------	---------------------------------------

Defaults

No default behavior or values.

Command Modes

SSG-redirect 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 define a list of one or more IP networks that make up a named network list. Use the *network-listname* attribute to name the IP network list.

Packets arriving from an authorized user who is attempting to access an unauthorized service from an IP address that is part of a named network list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen. Service Selection Gateway (SSG) TCP Redirect for Services uses a marked TCP port or TCP port list in addition to the destination IP address to determine if a packet is redirected to a captive portal group.

Define a named TCP port list using the **port-list** command, and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named network list.

Examples

The following example defines an IP network list named "RedirectNw":

```
network-list RedirectNw
```

Related Commands

Command	Description
network (ssg-redirect)	Adds an IP address to a named network list.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named captive portal group.

Command	Description
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

port (ssg-redirect)

To add a TCP port to a named port list, use the **port** command in SSG-redirect-port configuration mode. To remove a TCP port from a named port list, use the **no port** form of this command.

port *port-number*

no port *port-number*

Syntax Description

<i>port-number</i>	Incoming destination port number.
--------------------	-----------------------------------

Defaults

No default behavior or values.

Command Modes

SSG-redirect-port 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 add incoming destination ports to a named TCP port list. Incoming packets directed to a port in the named TCP port list can be redirected by the named captive portal group. Configure the named captive portal group using the **server-group** command, and add servers to the captive portal group using the **server (SSG)** command. Define and name the TCP port list using the **port-list** command.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define or add incoming destination ports to a named TCP port list.

Examples

The following example creates a named TCP port list named “WebPorts” and adds TCP ports 80 and 8080:

```
ssg enable
ssg tcp-redirect
  port-list WebPorts
    port 80
    port 8080
```

Related Commands

Command	Description
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.
server (SSG)	Adds a server to a captive portal group.

Command	Description
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.

port-list

To define a list of one or more TCP ports that make up a named port list and to enter SSG-redirect-port configuration mode, use the **port-list** command in SSG-redirect configuration mode. To disable a port list, use the **no** form of this command.

port-list *port-listname*

no port-list *port-listname*

Syntax Description

<i>port-listname</i>	Defines the name of the port list.
----------------------	------------------------------------

Defaults

No default behavior or values.

Command Modes

SSG-redirect 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 define a named port list. Use this command to create a list of TCP ports that can be redirected by the captive portal group. Use the **port (ssg-redirect)** command in SSG-redirect-port configuration mode to add TCP ports to the named port list.

You must enable Service Selection Gateway (SSG) using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a named port list.

Examples

The following example creates a port list named “WebPorts”:

```
ssg enable
ssg tcp-redirect
port-list WebPorts
```

Related Commands

Command	Description
port (ssg-redirect)	Adds a TCP port to a named port list.
redirect port to	Marks a TCP port or named TCP port list for SSG TCP redirection.
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.

Command	Description
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.

redirect captive advertising default group

To configure the default captive portal group, duration, and frequency for advertising captivation, use the **redirect captive advertising default group** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for advertising captivation, use the **no** form of this command.

redirect captive advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

no redirect captive advertising default group *group-name* **duration** *seconds* **frequency** *frequency*

Syntax Description

<i>group-name</i>	Name of the captive portal group.
<i>seconds</i>	The duration in seconds of the advertising captivation. The valid range is from 1 to 65,536 seconds.
<i>frequency</i>	The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is from 1 to 65,536 seconds.

Defaults

No default behavior or values.

Command Modes

SSG-redirect 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 select the default captive portal group for advertising captivation of users upon Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the advertising captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

Use the *frequency* argument to configure how often Service Selection Gateway (SSG) attempts to forward packets from the user to the captive portal.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

Examples

The following example shows how to configure the captive portal group named “CaptiveServer” to forward packets from a user for 30 seconds at intervals of 3600 seconds:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captive initial default group CaptivateServer duration 10
 redirect captive advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands

Command	Description
redirect captive 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 TCP traffic from unauthenticated users to a specified captive portal group.
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.

redirect captivate initial default group duration

To select a default captive portal group and duration of the initial captivation of users on Account Logon, use the **redirect captivate initial default group duration** command in SSG-redirect configuration mode. To deselect a captive portal group as the default for initial captivation, use the **no** form of this command.

redirect captivate initial default group *group-name* **duration** *seconds*

no redirect captivate initial default group *group-name* **duration** *seconds*

Syntax Description		
	<i>group-name</i>	Name of the captive portal group.
	<i>seconds</i>	The duration in seconds of the initial captivation. The valid range is from 1 to 65,536 seconds.

Defaults No default behavior or values.

Command Modes SSG-redirect 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 select the default captive portal group for initial captivation of users on Account Logon. Use the *seconds* argument to configure the duration, in seconds, of the initial captivation. Any packets arriving from the user and marked for one of the TCP ports configured in the captive portal group *group-name* are redirected to one of the captive portals defined in that captive portal group for the duration configured by the *seconds* argument.

The parameters set by this command can be overridden by the RADIUS attributes set for a user.

Examples The following example shows that the captive portal group named “CaptiveServer” will be used to forward packets from a user for the first 10 seconds that the user is connected:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands	Command	Description
	redirect captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
	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 TCP traffic from unauthenticated users to a specified captive portal group.
	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.

redirect port to

To configure a TCP port or named TCP port list for Service Selection Gateway (SSG) TCP Redirect for Services, use the **redirect port to** command in SSG-redirect configuration mode. To disable SSG TCP Redirect for Services on a TCP port or named TCP port list, use the **no** form of this command.

redirect { **port-list** *port-listname* | **port** *port-number* } **to** *group-name*

no redirect { **port-list** *port-listname* | **port** *port-number* } **to** *group-name*

Syntax Description

port-list	Specifies the named TCP port list to mark for SSG TCP redirection.
<i>port-listname</i>	Specifies the name of the named TCP port list.
port	Specifies a TCP port to mark for SSG TCP redirection.
<i>port-number</i>	Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
<i>group-name</i>	Defines the name of the captive portal group to redirect packets to that are marked for a destination port or named TCP port list.

Defaults

No default behavior or values.

Command Modes

SSG-redirect 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 mark a TCP port or a named TCP port list for SSG TCP Redirect for Services. Define a named TCP port list using the **port-list** command and add TCP ports to the named TCP port list using the **port (ssg-redirect)** command. Packets arriving from an authorized user, or from an authorized user attempting to access an unauthorized service at a marked TCP port or named TCP port list can be redirected to a captive portal group that presents the user with an appropriate response, such as a logon screen.



Note

You can associate only one port or port list with a portal group.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a TCP port or named TCP port list for SSG TCP redirection.



Note

This command replaces the **ssg http-redirect port group** command.

Examples

The following example marks TCP port 8080 for SSG TCP redirection. Packets with a destination port of 8080 are redirected to the captive portal group named “RedirectServer”:

```
server-group RedirectServer
 server 10.2.36.253 8080
!
 redirect port 8080 to RedirectServer
 redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example marks the named TCP port “WebPorts” for SSG TCP redirection. Packets with a destination port that is one of the ports in the port list “WebPorts” are redirected to the captive portal group named “RedirectServer”:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to RedirectServer
!
```

Related Commands

Command	Description
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 captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive initial default group duration	Selects a default captive portal group and duration of the initial captivation of users on Account Logon.
redirect unauthorized-service to	Sets a list of destination IP networks that can be redirected by a specified, named 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.

redirect smtp group

To select a captive portal group for redirection of Simple Mail Transfer Protocol (SMTP) traffic, use the **redirect smtp group** command in SSG-redirect configuration mode. To stop redirecting SMTP traffic to a captive portal group, use the **no** form of this command.

```
redirect smtp group group-name [all | user]
```

```
no redirect smtp group group-name [all | user]
```

Syntax Description

<i>group-name</i>	Name of the captive portal group.
all	(Optional) Any SMTP packets are forwarded.
user	(Optional) SMTP packets from users that have SMTP forwarding permission are forwarded.

Defaults

The **all** keyword is the default if no keyword is specified.

Command Modes

SSG-redirect 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 select a captive portal group for redirection of SMTP traffic. If you select the **all** keyword, all SMTP packets (TCP port 25) from authorized users are redirected to one of the servers in the captive portal group specified by the *group-name* argument. If you select the **user** keyword, only SMTP packets from authorized users that have SMTP forwarding permission set through a RADIUS attribute are redirected. If you do not select a keyword, the default is the **all** keyword.

Examples

The following example shows how to configure all SMTP packets from authorized users to be redirected to the captive portal group named “SMTPServer”:

```
server-group SSD
 server 10.0.0.253 8080
!
 redirect port-list WebPorts to SSD
!
 redirect unauthenticated-user to RedirectServer
 redirect unauthorized-service to SSD
 redirect smtp group SMTPServer all
 redirect captivate initial default group CaptivateServer duration 10
 redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

The following example shows how to configure SMTP packets from any authorized user with the SMTP forwarding permission set through a RADIUS attribute to be redirected to the captive portal group named “SMTPServer”:

```
redirect smtp group SMTPServer user
```

Related Commands	Command	Description
	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 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 TCP traffic from unauthenticated users to a specified captive portal group.
	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.

redirect unauthenticated-user to

To redirect TCP traffic from unauthenticated users to a specified captive portal group, use the **redirect unauthenticated-user to** command in Service Selection Gateway SSG-redirect configuration mode. To stop redirecting traffic from unauthenticated users to the specified captive portal group, use the **no** form of this command.

redirect unauthenticated-user to *group-name*

no redirect unauthenticated-user to *group-name*

Syntax Description

<i>group-name</i>	The name of the captive portal group.
-------------------	---------------------------------------

Defaults

No default behavior or values.

Command Modes

SSG-redirect 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 redirect traffic from unauthenticated users to a specified captive portal group.



Note

This command replaces the **ssg http-redirect unauthorized-user group** command.

Examples

The following example sets redirection of traffic from unauthenticated users to the captive portal group named "RedirectServer":

```
server-group SSD
  server 10.0.0.253 8080
!
  redirect port-list WebPorts to SSD
!
  redirect unauthenticated-user to RedirectServer
  redirect unauthorized-service to SSD
  redirect smtp group SMTPServer all
  redirect captivate initial default group CaptivateServer duration 10
  redirect captivate advertising default group CaptivateServer duration 30 frequency 3600
```

Related Commands

Command	Description
redirect captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive 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.
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.

redirect unauthorized-service to

To set a list of destination IP networks that can be redirected by a specified, named captive portal group, use the **redirect unauthorized-service to** command in SSG-redirect configuration mode. To remove the list of IP networks that can be redirected by a specified named captive portal group, use the **no** form of this command.

redirect unauthorized-service [**destination network-list** *network-listname*] **to** *group-name*

no redirect unauthorized-service [**destination network-list** *network-listname*] **to** *group-name*

Syntax Description

destination network list	(Optional) Checks incoming packets from authenticated hosts to networks that they are not authorized to access to determine if they need redirection.
<i>network-listname</i>	(Optional) Name of the list of destination IP networks.
<i>group-name</i>	Name of the captive portal group.

Defaults

No default behavior or values.

Command Modes

SSG-redirect 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 set a list of destination IP networks that can be redirected by the named captive portal group specified by the *group-name* argument. Incoming packets from authenticated hosts to networks that they are not authorized to access are checked against the destination IP network list to determine if they need redirection. If you do not specify a destination IP network by configuring the optional **destination network-list** keywords, the captive portal group specified in the *group-name* argument is used as the default group for unauthorized service redirection when the IP address of the unauthorized packet does not fall into any network list associated with any captive portal group.

You can associate only one destination IP network list with a captive portal group. You can associate a destination IP network list with multiple captive portal groups.

When you associate a destination IP network list with a captive portal group, packets arriving marked with a destination IP network that matches an IP network list may be redirected via SSG TCP redirection. The incoming destination TCP port also determines whether a packet is a candidate for SSG TCP redirection.

You can associate different server groups with overlapping IP network addresses. You must configure the captive portal group associated with a more specific network group first. For example, you must configure

```
redirect 10.1.0.0/255.255.0.0 to IPTVGroup
```

before you can configure

```
redirect 10.0.0.0/255.0.0.0 to ISPGroup
```

Examples

The following example shows how to set the captive portal group called “RedirectServer” as a possible candidate for redirection when the destination of a packet matches one of the networks in the destination IP network list named “RedirectNW”:

```
server-group RedirectServer
 server 10.2.36.253 8080
!
 redirect port 80 to RedirectServer
 redirect unauthorized-service destination network-list RedirectNw to RedirectServer
```

The following example shows how to set the captive portal group called “DefaultRedirectServer” as a possible candidate for redirection when the destination of a packet does not match any of the networks defined in any destination IP network list:

```
redirect unauthorized-service to DefaultRedirectServer
```

Related Commands

Command	Description
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 unauthenticated-user to	Redirects TCP traffic from unauthenticated users to a specified captive portal group.
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.

select

To override the default Autodomain selection algorithm, use the **select** command in SSG-auto-domain mode. To reenable the default algorithm for selecting the Autodomain, use the **no** form of this command.

```
select {username | called-station-id}
```

```
no select {username | called-station-id}
```

Syntax Description

username	Configures the algorithm to use only the username to select the Autodomain.
called-station-id	Configures the algorithm to use only the Access Point Name (APN) Called-Station-ID.

Defaults

The algorithm attempts to find a valid Autodomain based on the APN Called-Station-ID and then by username.

Command Modes

SSG-auto-domain

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 the **select** command to override the default algorithm for selecting the Autodomain. By default, the algorithm attempts to find a valid Autodomain based on APN Called-Station-ID and then by username. Using this command, you can configure the algorithm to use only the APN or only the username.



Note

The Autodomain exclusion list is applied even if the mode is selected using the **select** command.

Examples

The following example shows how to configure the algorithm to search for a valid Autodomain based only on the username:

```
ssg enable
ssg auto-domain
mode extended
select username
exclude apn motorola
exclude domain cisco
download exclude-profile abc password1
nat user-address
```

The following example shows how to configure the algorithm to search for a valid Autodomain based only on the APN:

```
select called-station-id
```

Related Commands

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

server (SSG)

To add a server to a captive portal group, use the **server** command in SSG-redirect-group configuration mode. To remove a server from a captive portal group, use the **no** form of this command.

server *ip-address* *port*

no server *ip-address* *port*

Syntax Description

<i>ip-address</i>	IP address of the server to be added to the captive portal group.
<i>port</i>	TCP port of the server to be added to the captive portal group.

Defaults

No default behavior or values.

Command Modes

SSG-redirect-group

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 the **server** command in SSG-redirect-group configuration mode to add a server, defined by its IP address and TCP port, to a captive portal group.

Service Selection Gateway (SSG) TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a captive portal group. Use the **server-group** command in SSG-redirect configuration mode to create and name a captive portal group before using the **server** command to add servers to the captive portal group.

Examples

The following example adds a server at IP address 10.0.0.0 and TCP port 8080 and a server at IP address 10.1.2.3 and TCP port 8081 to a captive portal group named "RedirectServer":

```
ssg enable
ssg tcp-redirect
server-group RedirectServer
server 10.0.0.0 8080
server 10.1.2.3 8081
```

Related Commands

Command	Description
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.

server-group

To define a group of one or more servers that make up a named captive portal group and enter SSG-redirect-group configuration mode, use the **server-group** command in SSG-redirect configuration mode. To remove a captive portal group and any servers configured within that portal group, use the **no** form of this command.

server-group *group-name*

no server-group *group-name*

Syntax Description

<i>group-name</i>	The name of the captive portal group.
-------------------	---------------------------------------

Defaults

No default behavior or values.

Command Modes

SSG-redirect 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 define and name a captive portal group. Service Selection Gateway (SSG) TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

After defining a captive portal group with the **server-group** command, identify individual servers for inclusion in the captive portal group using the **server** *ip-address port* command in SSG-redirect-group configuration mode.

You must enable SSG using the **ssg enable** command and SSG TCP Redirect for Services using the **ssg tcp-redirect** command before you can define a captive portal group.



Note

This command, along with the **server** command, replaces the **ssg http-redirect group** *group-name* **server** *ip-address port* command.

Examples

The following example defines a captive portal group named “RedirectServer”:

```
ssg enable
ssg tcp-redirect
server-group RedirectServer
```

Related Commands	Command	Description
	server (SSG)	Adds a server to a captive portal group.
	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.

server-port

To configure the ports on which Service Selection Gateway (SSG) listens for RADIUS-requests from configured RADIUS clients, use the **server-port** command in SSG-radius-proxy configuration mode. To stop SSG from listening for RADIUS requests from configured RADIUS clients on a port, use the **no** form of this command.

```
server-port [auth auth-port] [acct acct-port]
```

```
no server-port [auth auth-port] [acct acct-port]
```

Syntax Description

auth	(Optional) RADIUS authentication port.
<i>auth-port</i>	(Optional) Port number to be used for RADIUS authentication. The default is 1645.
acct	(Optional) RADIUS accounting port.
<i>acct-port</i>	(Optional) Port number to be used for RADIUS accounting. The default is 1646.

Defaults

Port 1645 is the default RADIUS authentication port.
Port 1646 is the default RADIUS accounting port.

Command Modes

SSG-radius-proxy 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 configure the authentication and accounting ports for the SSG Autologon Using Proxy RADIUS feature. Ports configured with this command are global parameters that apply to all proxy clients in the SSG.

Examples

The following example shows how to configure port 23 as the RADIUS authentication port and port 45 as the RADIUS accounting port:

```
server-port auth 23 acct 45
```

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.
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.
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 radius-proxy	Enables SSG RADIUS Proxy.

show ssg auto-domain exclude-profile

To display the contents of an Autodomain exclude-profile downloaded from the AAA server, use the **show ssg auto-domain exclude-profile** command in global configuration mode.

```
show ssg auto-domain exclude-profile
```

Syntax Description This command has no arguments or keywords.

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 in global configuration mode to display the contents of an Autodomain exclude-profile downloaded from the AAA server. If any exclude entries downloaded from the AAA server are removed by the **no exclude {apn | domain} name** command, these entries will not be displayed by the **show ssg auto-domain exclude-profile** command.

Examples The following sample displays the contents of an Autodomain exclude-profile downloaded from the AAA server. The report is self-explanatory.

```
Router# show ssg auto-domain exclude-profile
```

```
Exclude APN Entries Downloaded:
```

```
apn1.gprs   apr2.com
```

```
Exclude Domain Entries Downloaded:
```

```
cisco.com  abcd.com
```

Related Commands	Command	Description
	exclude	Configures the Autodomain exclusion list.
	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	Adds to the Autodomain download exclusion list.
	ssg enable	Enables SSG functionality.

show ssg binding

To display service names that have been bound to interfaces and the IP addresses to which they have been bound, use the **show ssg binding** command in privileged EXEC mode.

```
show ssg binding [begin expression | exclude expression | include expression]
```

Syntax Description	begin	(Optional) Begin with the line that contains <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
	exclude	(Optional) Exclude lines that contain <i>expression</i> .
	include	(Optional) Include lines that contain <i>expression</i> .

Command Modes Privileged EXEC

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 display services and the interfaces to which they have been bound.

Examples The following example shows all service names that have been bound to interfaces:

```
Router# show ssg binding

WhipitNet      -> 192.168.1.1 (NHT)
Service1.com   -> 192.168.1.2 (NHT)
Service2.com   -> 192.168.1.3 (NHT)
Service3.com   -> 192.168.1.4 (NHT)
GoodNet        -> 192.168.2.1
Perftest       -> 192.168.1.6
```

Related Commands	Command	Description
	clear ssg service	Removes a service.
	show ssg service	Displays the information for a service.
	ssg bind service	Specifies the interface for a service.

show ssg connection

To display the connections of a given host and a service name, use the **show ssg connection** command in privileged EXEC mode.

```
show ssg connection ip-address service-name [interface]
```

Syntax Description		
	<i>ip-address</i>	IP address of an active Service Selection Gateway (SSG) connection. This is always a subscribed host.
	<i>service-name</i>	Name of an active SSG connection.
	<i>interface</i>	(Optional) The IP address through which the host is connected.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(2)B	The <i>interface</i> argument was added for the SSG Host Key feature.
	12.2(4)B	This command was modified to display information about SSG prepaid billing.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(13)T	This command was modified for Cisco IOS Release 12.2(13)T.

Examples

Prepaid Service Based on Volume Example

The following example displays the SSG connection for a prepaid service that uses a volume-based quota:

```
Router# show ssg connection 19.1.1.19 InstMsg

-----ConnectionObject Content -----

User Name:
Owner Host:19.1.1.19
Associated Service:InstMsg
Connection State:0 (UP)
Connection Started since:*00:25:58.000 UTC Tue Oct 23 2001
User last activity at:*00:25:59.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
    Quota Type = 'VOLUME', Quota Value = 100
Session policing disabled
```

Prepaid Service Based on Time Example

The following example displays the SSG connection for a prepaid service that uses a time-based quota:

```
Router# show ssg connection 19.1.1.22 Prepaid-internet
```

```
-----ConnectionObject Content -----
User Name:Host
Owner Host:19.1.1.22
Associated Service:Prepaid-internet
Connection State:0 (UP)
Connection Started since:*00:34:06.000 UTC Tue Oct 23 2001
User last activity at:*00:34:07.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
    Quota Type = 'TIME', Quota Value = 100
Session policing disabled
```

Autologin Service Example

The following example shows the service connection for the autologin service to host 10.3.6.1:

```
Router# show ssg connection 10.3.6.1 autologin
```

```
----- ConnectionObject Content -----
User Name:autologin
Owner Host:10.3.6.1
Associated Service:autologin
Connection State:0 (UP)
Connection Started since:
*20:41:26.000 UTC Fri Jul 27 2001
User last activity at:*20:41:26.000 UTC Fri Jul 27 2001
Connection Traffic Statistics:
    Input Bytes = 0 (HI = 0), Input packets = 0
    Output Bytes = 0 (HI = 0), Output packets = 0
```

Table 24 describes the significant fields shown in the displays.

Table 24 *show ssg connection Field Descriptions*

Field	Description
User Name	Subscriber name supplied at authentication.
Owner Host	IP address of the subscribed host.
Associated Service	Service name of the connected service.
Connection State	State of activation (active or inactive).
Connection Started since	Time of host connection to the associated service.
User last activity at	Time of last data packet sent over this connection.
Input Bytes	Number of bytes received on this connection.
Input packets	Number of packets received on this connection.
Output Bytes	Number of bytes sent on this connection.
Output packets	Number of packets sent on this connection.
Quota Type	Form in which the quota value is expressed (time or volume).
Quota Value	Value of the quota (in bytes for volume or seconds for time).

■ show ssg connection

Related Commands

Command	Description
clear ssg connection	Removes the connections of a given host and a service name.

show ssg direction

To display the direction of all interfaces for which a direction has been specified, use the **show ssg direction** command in privileged EXEC mode.

show ssg direction [**begin** *expression* | **exclude** *expression* | **include** *expression*]

Syntax Description	begin	(Optional) Begin with the line that contains <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
	exclude	(Optional) Exclude lines that contain <i>expression</i> .
	include	(Optional) Include lines that contain <i>expression</i> .

Command Modes Privileged EXEC

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 show all interfaces that have been specified as uplinks or downlinks.

Examples The following example shows the direction of all interfaces that have been specified as uplinks or downlinks.

```
Router# show ssg direction

ATM0/0/0.10: Uplink
BVI1: Downlink
FastEthernet0/0/0: Uplink
```

Related Commands	Command	Description
	ssg bind direction	Specifies an interface as a downlink or uplink interface.

show ssg host

To display the information about a subscriber and current connections of the subscriber, use the **show ssg host** command in privileged EXEC mode.

```
show ssg host [ip-address [interface] | username]
```

Syntax Description		
	<i>ip-address</i>	(Optional) IP address of the host.
	<i>interface</i>	(Optional) Interface through which the host is connected.
	username	(Optional) Displays the usernames logged into the active hosts.

Defaults If no argument is provided, all current connections are displayed.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(2)B	The <i>interface</i> argument was added.
	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 all active hosts:

```
Router# show ssg host

1:10.3.1.1      [Host-Key 70.13.60.3:64]
2:10.3.6.1     [Host-Key 70.13.60.3:65]

### Active HostObject Count:2
```

The following example shows information about host 10.3.1.1:

```
Router# show ssg host 10.3.1.1

----- HostObject Content -----
Activated:TRUE
Interface:Virtual-Access1
User Name:pppoauser
Host IP:10.3.1.1
Msg IP:0.0.0.0 (0)
Host DNS IP:0.0.0.0
Maximum Session Timeout:0 seconds
Host Idle Timeout:0 seconds
Class Attr:NONE
User logged on since:*20:59:51.000 UTC Fri Jul 27 2001
User last activity at:*20:59:51.000 UTC Fri Jul 27 2001
Default Service:NONE
```

```
DNS Default Service:NONE
Active Services:autologon;
AutoService:autologon;
Subscribed Services:
```

The following example shows two host objects with the same IP address:

```
Router# show ssg host 10.3.1.1
```

```
SSG:Overlapping hosts for IP 10.3.1.1 at interfaces:FastEthernet0/0/0
Virtual-Access1
```

In this case, use the *interface* argument to uniquely identify the host:

```
Router# show ssg host 10.3.1.1 FastEthernet0/0/0
```

Note that the output produced by this command is the same as that produced by the command without the *interface* argument. The *interface* argument is used only to uniquely identify a host when there are overlapping host IP addresses.

The following example shows the usernames logged in to the active hosts:

```
RouterA# show ssg host user
```

```
1:10.3.1.1      (active) Host name:pppoauser
2:10.3.6.1      (active) Host name:ssguser2
```

```
### Total HostObject Count(including inactive hosts):2
```

Related Commands

Command	Description
clear ssg host	Removes or disables a given host or subscriber.

show ssg next-hop

To display the next-hop table, use the **show ssg next-hop** command in privileged EXEC mode.

show ssg next-hop [**begin** *expression* | **exclude** *expression* | **include** *expression*]

Syntax Description	begin	(Optional) Displays lines beginning with the line that contains <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
	exclude	(Optional) Excludes lines that contain <i>expression</i> .
	include	(Optional) Includes lines that contain <i>expression</i> .

Command Modes Privileged EXEC

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 display all next-hop IP addresses.

Examples The following example shows the next-hop table:

```
Router# show ssg next-hop

Next hop table loaded from profile prof-nhg:
  WhipitNet          -> 192.168.1.6
  Service1.com       -> 192.168.1.3
  Service2.com       -> 192.168.1.2
  Service3.com       -> 192.168.1.1
  GoodNet            -> 192.168.1.2
  Perfctest          -> 192.168.1.5
End of next hop table.
```

Related Commands	Command	Description
	clear ssg next-hop	Removes the next-hop table.
	ssg next-hop download	Downloads the next-hop table from a RADIUS server.

show ssg open-garden

To display a list of all configured open garden services, use the **show ssg open-garden** command in privileged EXEC mode.

```
show ssg open-garden
```

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC

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.

Examples In the following example, all configured open garden services are displayed:

```
Router# show ssg open-garden

nrp1-nrp2_og1
nrp1-nrp2_og2
nrp1-nrp2_og3
nrp1-nrp2_og4
```

Related Commands	Command	Description
	local-profile	Configures a local service profile.
	ssg open-garden	Designates a service, defined in a local service profile, as an open garden service.
	ssg service-search-order	Specifies the order in which SSG searches for a service profile.

show ssg pass-through-filter

To display the downloaded filter for transparent pass-through, use the **show ssg pass-through-filter** command in privileged EXEC mode.

```
show ssg pass-through-filter [begin expression | exclude expression | include expression]
```

Syntax Description	begin	(Optional) Begin with the line that contains <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
	exclude	(Optional) Exclude lines that contain <i>expression</i> .
	include	(Optional) Include lines that contain <i>expression</i> .

Command Modes Privileged EXEC

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 display the downloaded transparent pass-through filter. The filter prevents pass-through traffic from accessing the specified IP address and subnet mask combinations. The filter is set using the [ssg pass-through](#) command.

To display a filter defined on the command line, use the **show running-config** command.

Examples The following example shows the pass-through filter:

```
Router# show ssg pass-through-filter

      Service name:  filter01
      Password:      cisco

      Direction:     Uplink

Extended IP access list (SSG ACL)
  permit tcp 172.16.6.0 0.0.0.255 any eq telnet
  permit tcp 172.16.6.0 0.0.0.255 192.168.250.0 0.0.0.255 eq ftp
```

Related Commands	Command	Description
	clear ssg pass-through-filter	Removes the downloaded filter for transparent pass-through.
	ssg pass-through	Enables transparent pass-through.

show ssg pending-command

To display current pending commands, such as next-hop or filters, use the **show ssg pending-command** command in privileged EXEC mode.

show ssg pending-command

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC

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 display the current pending commands.

Examples The following example shows the pending commands:

```
Router# show ssg pending-command

SSG pending command list:
  ssg bind service Service1.com 192.168.103.1
  ssg bind service Perfctest206 192.168.104.5
```

Related Commands	Command	Description
	clear ssg pending-command	Removes all pending commands.

show ssg port-map ip

To display information on a particular port bundle, use the **show ssg port-map ip** command in privileged EXEC mode.

show ssg port-map ip *ip-address* **port** *port-number*

Syntax Description		
	<i>ip-address</i>	IP address used to identify the port bundle.
	<i>port-number</i>	TCP port number used to identify the port bundle.

Command Modes Privileged EXEC

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 displays the following information about a port bundle:

- Port maps in the port bundle
- IP address of the subscriber
- Interface through which the subscriber is connected

Examples The following output shows the Virtual-Access2 interface connected to the subscriber:

```
Router# show ssg port-map ip 70.13.60.2 port 64

State = IN-USE
Subscriber Address = 10.10.3.1
Downlink Interface = Virtual-Access2

Port-mappings:-

Subscriber Port:   3271           Mapped Port:    1024
Subscriber Port:   3272           Mapped Port:    1025
Subscriber Port:   3273           Mapped Port:    1026
Subscriber Port:   3274           Mapped Port:    1027
Subscriber Port:   3275           Mapped Port:    1028
```

[Table 25](#) describes the significant fields shown in the display.

Table 25 *show ssg port-map ip Field Descriptions*

Field	Description
State	Port bundle status.
Subscriber Address	Subscriber IP address.
Downlink Interface	Interface through which the subscriber is connected.
Port-Mappings	Port maps in the port bundle.
Subscriber Port	Subscriber port number.
Mapped Port	Port assigned by SSG.

Related Commands

Command	Description
show ssg port-map status	Displays information on port bundles.

show ssg port-map status

To display information on port bundles, use the **show ssg port-map status** command in privileged EXEC mode.

show ssg port-map status [**free** | **reserved** | **inuse**]

Syntax Description	free	(Optional) Lists the port bundles that are in the “free” state for each bundle group.
	reserved	(Optional) Lists the port bundles that are in the “reserved” state for each bundle group. Also displays the associated subscriber IP address and interface for each port bundle.
	inuse	(Optional) Lists the port bundles that are in the “inuse” state for each bundle group. Also displays the associated subscriber IP address and interface for each port bundle.

Command Modes Privileged EXEC

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 Entered without any keywords, the command displays a summary of all port-bundle groups, including the following information:

- A list of port-bundle groups
- Port-bundle length
- Number of free, reserved, and in-use port bundles in each group

Examples

Display All Bundles Example

The following example shows output for the **show ssg port-map status** command with no keywords:

```
Router# show ssg port-map status
```

```
Bundle-length = 4
```

```
Bundle-groups:-
```

IP Address	Free Bundles	Reserved Bundles	In-use Bundles
70.13.60.2	4032	0	0

[Table 26](#) describes the significant fields shown in the display.

Table 26 *show ssg port-map status Field Descriptions*

Field	Description
Bundle-length	The bundle-length value indicates the number of ports per bundle and the number of bundles per bundle group.
Bundle-groups	List of bundle groups.
IP Address	IP address of a bundle group.
Free Bundles	Number of free bundles in the specified bundle group.
Reserved Bundles	Number of reserved bundles in the specified bundle group.
In-use Bundles	Number of in-use bundles in the specified bundle group.

Display In-Use Bundles Example

The following example shows output for the **show ssg port-map status** command with the **inuse** keyword:

```
Router# show ssg port-map status inuse
```

```
Bundle-group 70.13.60.2 has the following in-use port-bundles:-
```

Port-bundle	Subscriber Address	Interface
64	10.10.3.1	Virtual-Access2

[Table 27](#) describes the significant fields shown in the display.

Table 27 *show ssg port-map status inuse Field Descriptions*

Field	Description
Port-bundle	Port-bundle number.
Subscriber Address	Subscriber IP address of the subscriber.
Interface	Interface through which the subscriber is connected.

Related Commands

Command	Description
show ssg port-map ip	Displays information on a particular port bundle.

show ssg radius-proxy address-pool

To display the pool of IP addresses configured for a router or for a specific domain, use the **show ssg radius-proxy address-pool** command in privileged EXEC mode.

```
show ssg radius-proxy address-pool [domain domain-name] [free | inuse]
```

Syntax Description	domain	(Optional) IP addresses configured for a specific domain.
	<i>domain-name</i>	(Optional) Name of the domain to display.
	free	(Optional) IP addresses currently available in the free pool.
	inuse	(Optional) IP addresses currently in use.

Defaults If no domain name is provided, the command displays information for all IP addresses configured in an address pool.

Command Modes Privileged EXEC

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 display the IP address pools configured for a router or for a specific domain. You can also display which IP addresses are available or are in use.

Examples The following example shows how to display information for IP addresses in the IP address pool:

```
Router# show ssg radius-proxy address-pool

Global Pool:  Free Addresses= 10234   Inuse Addresses= 0
```

The following example shows how to display information about the IP addresses in the IP address pool in the domain called “ssg.com”:

```
Router# show ssg radius-proxy address-pool domain ssg.com

Domain Pool(ssg.com):  Free Addresses= 20   Inuse Addresses= 10
```

The following example shows how to display information about the IP addresses in the IP address pool for the domain called “ssg.com” that are currently in use:

```
Router# show ssg radius-proxy address-pool domain cisco inuse

Inuse Addresses in Domain Pool(ssg.com):10
19.1.5.1
19.1.5.2
19.1.5.3
```

```

19.1.5.4
19.1.5.5
19.1.5.6
19.1.5.7
19.1.5.8
19.1.5.9
19.1.5.10

```

The following example shows how to display information about the IP addresses in the IP address pool for the domain called “ssg.com” that are currently available:

```
Router# show ssg radius-proxy address-pool domain ssg.com free
```

```

Free Addresses in Domain Pool(ssg.com):20
19.1.5.11
19.1.5.12
19.1.5.13
19.1.5.14
19.1.5.15
19.1.5.16
19.1.5.17
19.1.5.18
19.1.5.19
19.1.5.20
19.1.5.21
19.1.5.22
19.1.5.23
19.1.5.24
19.1.5.25
19.1.5.26
19.1.5.27
19.1.5.28
19.1.5.29
19.1.5.30

```

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.
clear ssg radius-proxy nas-address	Clears all hosts connected to a specific NAS.
clear ssg service	Removes a service.
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 binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
ssg bind service	Specifies the interface for a service.
ssg enable	Enables SSG.
ssg radius-proxy	Enables SSG RADIUS Proxy.

show ssg service

To display the information for a service, use the **show ssg service** command in privileged EXEC mode.

```
show ssg service [service-name [begin expression | exclude expression | include expression]]
```

Syntax Description	
<i>service-name</i>	(Optional) Name of an active Service Selection Gateway (SSG) service.
begin	(Optional) Begin with the line that contains <i>expression</i> .
<i>expression</i>	(Optional) Word or phrase used to determine what lines will be shown.
exclude	(Optional) Exclude lines that contain <i>expression</i> .
include	(Optional) Include lines that contain <i>expression</i> .

Defaults If no service name is provided, the command displays information for all services.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(3) DC	This command was introduced on the Cisco 6400 node route processor.
	12.1(1) DC1	The output of this command was modified on the Cisco 6400 node route processor to display the following Service-Info Attributes when they are present in the proxy RADIUS service profile: <ul style="list-style-type: none"> • Service-Defined Cookie • Full Username Attribute
	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 display connection information for a service.

Examples The following example shows the information for the service called “serv1-proxy”:

```
Router# show ssg service serv1-proxy

----- ServiceInfo Content -----
Uplink IDB:
Name:serv1-proxy
Type:PROXY
Mode:CONCURRENT
Service Session Timeout:0 seconds
Service Idle Timeout:0 seconds
Class Attr:NONE
Authentication Type:CHAP
Reference Count:1
```

```

Next Hop Gateway Key:my-key

DNS Server(s):Primary:10.13.1.5

Radius Server:IP=10.13.1.2, authPort=1645, acctPort=1646, secret=my-secret

Included Network Segments:
    10.13.0.0/255.255.0.0
Excluded Network Segments:
Full User Name Used
Service Defined Cookie exist

Domain List:service1.com;

Active Connections:
    1 :Virtual=255.255.255.255, Subscriber=10.20.10.2

----- End of ServiceInfo Content -----

```

Related Commands

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.
ssg bind service	Specifies the interface for a service.

show ssg tcp-redirect group

To display information about the captive portal groups and their networks associated with those portal groups, use the **show ssg tcp-redirect group** command in privileged EXEC mode.

```
show ssg tcp-redirect group [group-name]
```

Syntax Description	<i>group-name</i>	(Optional) The previously defined name for the captive portal group.
--------------------	-------------------	--

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

Command History	Release	Modification
	12.2(4)B	This command was introduced. This command replaced the show 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 display information about the captive portal groups and their associated networks defined in your system.
------------------	---

If you omit the optional *group-name* argument, this command displays a list of all defined captive portal groups and the networks associated with the captive portal groups. If you specify the *group-name* argument, this command displays information about that group and its associated networks.

Examples	The following example shows how to display a list of all of the defined captive portal groups:
----------	--

```
Router# show ssg tcp-redirect group

Current TCP redirect groups:
RedirectServer
CaptiveServer
SMTPServer
SSD

Unauthenticated user redirect group:RedirectServer
Default service redirect group:SSD
SMTP forwarding group:SMTPServer, for all users
Default initial captivation group:CaptiveServer,
for 10 seconds
Default advertising captivation group:CaptiveServer,
for 30 seconds approximately every 3600 seconds
```

Table 28 describes the significant fields shown in the display above.

Table 28 *show ssg tcp-redirect group Field Descriptions*

Field	Description
Current TCP redirect groups:	List of all TCP-redirect groups.
Default service redirect group: SSD	Default service redirect group.
SMTP forwarding group: SMTPServer, for all users	SMTP redirection settings.
Default initial captivation group: CaptivateServer, for 10 seconds	Default initial captivation group, name of captivation, and duration of captivation.
Default advertising captivation group: CaptivateServer, for 30 seconds approximately every 3600 seconds	Default advertising captivation group, name of captivation group, duration, and frequency of advertising captivation.

The following example shows how to display a detailed description of the captive portal group called “RedirectServer”:

```
Router# show ssg tcp-redirect group RedirectServer

TCP redirect group RedirectServer:
Showing all TCP servers (Address, Port):
 10.2.36.253, 8080, FastEthernet0/0
Networks to redirect to (network-list RedirectNw):
 172.16.10.0 /24
 172.20.0.0 /16
TCP port to redirect:
 80
```

Table 29 describes the significant fields shown in the display.

Table 29 *show ssg tcp-redirect group group-name Field Descriptions*

Field	Description
Showing all TCP servers (Address, Port):	List of all servers.
10.2.36.253	Server IP address.
8080	Server port number.
FastEthernet0/0	Interface on which this server is reachable.
Networks to redirect to	List of networks.
(network-list RedirectNw):	Network list name.
TCP port to redirect:	Name of port-list (if port-list is used).

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.

■ show ssg tcp-redirect group

Command	Description
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 captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive 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 the 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 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.

show ssg vc-service-map

To display virtual circuit (VC)-to-service-name mappings, use the **show ssg vc-service-map** command in privileged EXEC mode.

```
show ssg vc-service-map [vpi/vci | service service-name]
```

Syntax Description		
<i>vpi/vci</i>	(Optional) Virtual path identifier (VPI)/virtual channel identifier (VCI) value, including the slash; for example, 3/33.	
service	(Optional) Displays the VCs mapped to a service name.	
<i>service-name</i>	(Optional) Service name.	

Command Modes Privileged EXEC

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 display VC-to-service-name mappings.

Examples

The following example shows the VCs mapped to the service name “Worldwide”:

```
Router# show ssg vc-service-map service Worldwide
```

```
Interface  From      To      Service Name      Type
All        3 /33    None    Worldwide          non-exclusive
```

Related Commands	Command	Description
	ssg vc-service-map	Maps VCs to service names.

show tcp-redirect mappings

To display information about the TCP redirect mappings for hosts within your system, use the **show tcp-redirect mappings** command in privileged EXEC mode.

```
show tcp-redirect mappings [ip-address [interface]]
```

Syntax Description		
	<i>ip-address</i>	(Optional) Displays redirection mappings for this specific host.
	<i>interface</i>	(Optional) Displays redirection mappings for the host connected to Service Selection Gateway (SSG) on the specified downlink interface.

Command Modes	
	Privileged EXEC

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 display information about the TCP redirect mappings for hosts within your system. If you omit the optional *ip-address* argument, this command displays a list of all host IP addresses that currently have stored mappings. If you include the *ip-address* argument, this command displays any mappings for the host with the specified IP address. You can use the *interface* argument when SSG is running in port mapped host key mode to specify the downlink interface on which the host is connected to the SSG. Use the *interface* argument when you want to display information about a specific host where there are overlapping IP addresses among hosts.

The TCP-redirect mappings are removed automatically after the TCP session terminates or has been idle for more than 60 seconds.



Note

This command replaces the **show http-redirect mappings** command.

Examples

The following example displays all of the hosts that have redirect mappings stored on your system:

```
Router# show tcp-redirect mappings

Authenticated hosts:
  TCP remapping Host:172.16.10.0 to servers (IP:Port)
    10.2.36.253:8080
    10.64.131.20:25
### Total authenticated hosts being redirected = 1

Unauthenticated hosts:

TCP remapping Host:172.0.0.2_to server:10.2.36.253 on port:8080
```

The following example displays detailed mapping for the host at IP address 172.16.0.0:

```

Router# show tcp-redirect mappings 172.16.0.0

TCP remapping Host:172.16.0.0
TCP remapping to server:10.2.36.253 on port:8080
Connection Mappings (src port <-> dest IP,dest port,timestamp, flags):
    11092 <-> 10.0.0.1,80,730967636,0x1
TCP remapping to server:10.64.131.20 on port:25
Connection Mappings (src port <-> dest IP,dest port,timestamp, flags):
    11093 <-> 10.0.0.1,25,730967652,0x0

```

Table 30 describes the significant fields shown in the displays.

Table 30 *show tcp-redirect mappings Field Descriptions*

Field	Description
Authenticated hosts	List of all authenticated hosts having mappings.
TCP remapping Host:172.16.10.0	Host IP address.
10.2.36.253:8080	List of server and port to which this host is being redirected.
Unauthenticated hosts	List of unauthenticated host IP addresses.
TCP remapping Host:172.0.0.2	Unauthenticated host IP address.
to server:10.2.36.253 on port:8080	Server IP address and port.
dest IP, dest port, timestamp	Timestamp when the last packet was translated using this mapping.
0x1	State of the TCP connection. 0x0 indicates a fully active session. Other values can indicate that the session has shut down partially or fully. 0x01 indicates a session reset. 0x1E indicates the session has terminated.

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 captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
redirect captive 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.

■ show tcp-redirect mappings

Command	Description
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.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

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 reenabling 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 accounting interval

To specify the interval at which accounting updates are sent 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 2,147,483,647 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 Service Selection Gateway (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 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 auto logoff, use the **no** form of this command.

```
ssg auto-logoff arp [interval seconds]
```

```
no auto-logoff arp
```

Syntax Description	interval seconds	(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 scenarios in which hosts are directly connected.

ICMP ping can be used in all types of deployment scenarios. 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.

■ ssg auto-logoff arp

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	Parameter	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

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 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
```

Related Commands

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** 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

download	Loads the next-hop table profile.
<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.
---------------------------	--

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 70.13.6.100
access-list 100 deny ip any any
```

■ ssg port-map destination access-list

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 ip-address	(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
```

■ ssg port-map destination range

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

bits 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 31](#) 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 31 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 31 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 Ethernet0/0/0
Router(config)# ssg port-map source ip Loopback 1
```

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 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; remember that the committed rate is specified in bits per seconds, but that the token bucket operates based on bytes. Hence, 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 needs to 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 needs to 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 captive advertising default group	Configures the default captive portal group, duration, and frequency for advertising.
	redirect captive 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/VCI 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/VCI 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.
