ssg default-network

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg default-network** command is not available in Cisco IOS software.

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

ip-address	Service Selection Gateway (SSG) default IP address or subnet.
mask	SSG default network destination mask.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

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:

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

ssg dfp ip

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg dfp ip** command is not available in Cisco IOS software.

To specify the interface between Service Selection Gateway (SSG) and a load-balancing device, use the **ssg dfp ip** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg dfp ip {*interface* | *ip-address*}

no ssg dfp ip {*interface* | *ip-address*}

Syntax Description

interface	Type and number of the interface between SSG and the load balancer.
ip-address	IP address of the SSG interface to the load balancer.

Command Default

An interface between SSG and the load balancer is not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The interface between the load balancer and SSG must be configured on SSG, or SSG will not be able to hand load-balancing weights to the DFP agent.

The interface or the IP address configured with this command must be the same as the interface or IP address configured on the load balancer under the server configuration. The interface or IP address is sent in the DFP packet along with the weight to the load balancer. The load balancer uses this information to identify the server from which the weight was received. If the interface or IP address is not the same as that configured on the load balancer, the weight information will not be associated with the correct SSG.

The interface specified by the **ssg dfp ip** command should be a downlink interface.

Examples

The following examples show the configuration of the interface between SSG and load balancer and the corresponding configuration on the load-balancing device:

Configuration on SSG Device: Example

```
ssg enable
```

```
ssg dfp weight 25
ssg dfp ip Ethernet1/0
!
!
interface Ethernet1/0
 ip address 10.0.0.20 255.0.0.0
 duplex half
 pppoe enable
 ssg direction downlink
!
```

Configuration on Cisco IOS Server Load Balancing Device: Example

```
!
ip slb serverfarm SSGFARM
 real 10.0.0.20
  inservice
!
ip slb vserver VSSG
 virtual 10.8.8.8 tcp 0
 serverfarm SSGFARM
 inservice
!
ip slb dfp
 agent 10.0.0.20 655
!
```

Related Commands

Command	Description
ssg dfp weight	Specifies the DFP weight, which will be used to calculate load balancing among SSGs, for an SSG device.

ssg dfp weight

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg dfp weight** command is not available in Cisco IOS software.

To specify the Dynamic Feedback Protocol (DFP) weight used to calculate load balancing for a Service Selection Gateway (SSG) device, use the **ssg dfp weight** command in global configuration mode. To reset the weight to the default value of 100, use the **no** form of this command.

ssg dfp weight *weight*

no ssg dfp weight

Syntax Description

weight	Weight to be used in the DFP load-balancing algorithm for load balancing among SSGs. Range is from 0 to 100. 100 is the default. A higher weight indicates higher availability. A weight of zero indicates that a server has no availability.

Command Default

The default DFP weight is 100.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

The DFP weight is used to calculate load balancing among SSGs.

You can use the **ssg dfp weight** command to prioritize SSGs that are being load-balanced. A higher weight indicates that the device can accept a heavier load.

Every time the DFP weight is changed by using the **ssg dfp weight** command, SSG sends the new weight to the DFP agent.

SSG calculates the weight that it hands over to the DFP agent on the basis of three factors:

- The DFP weight configured for the SSG
- CPU load
- Memory utilization

The DFP agent forwards the calculated weight to the load balancer.

Examples

The following example shows how to configure SSG with a DFP weight of 25:

```
ssg dfp weight 25
```

Related Commands

Command	Description
ssg dfp ip	Specifies the interface between SSG and the load-balancing device.

ssg dial-out

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg dial-out** command is not available in Cisco IOS software.

To enable the SSG L2TP Dial-Out feature and enter SSG dial-out configuration mode, use the **ssg dial-out** command in global configuration mode. To remove all SSG dial-out configurations, use the **no** form of this command.

ssg dial-out

no ssg dial-out

Syntax Description

This command has no arguments or keywords.

Command Default

The SSG L2TP Dial-Out feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enter SSG dial-out configuration mode to configure the SSG L2TP Dial-Out feature. Use the **no** form of this command to remove all Service Selection Gateway (SSG) L2TP dial-out configurations.

Examples

The following example shows how to enable the SSG L2TP Dial-Out feature and enter SSG dial-out configuration mode:

```
Router(config)# ssg dial-out
Router(config-dial-out)#
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
download exclude-profile (ssg dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.

Command	Description
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
show ssg dial-out exclude-list	Displays information about the DNIS prefix profile and the DNIS exclusion list.

ssg direction

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg direction** command is not available in Cisco IOS software.

To configure an interface or range of subinterfaces as downlink or uplink, use the **ssg direction** command in interface configuration mode or subinterface configuration mode. To clear the directional specification, use the **no** form of this command.

ssg direction {**downlink** | **uplink** [**member** *group-name*]}

no ssg direction

Syntax Description

downlink	Specifies the interface direction as downlink. A downlink interface is an interface to subscribers.
uplink	Specifies the interface direction as uplink. An uplink interface is an interface to services.
member	(Optional) Specifies that the uplink interface is a member of a group of uplink interfaces that reach the same services.
group-name	(Optional) Name of the group of uplink services.

Command Default

An interface is neither uplink nor downlink.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The **member** keyword and *group-name* argument were added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Service Selection Gateway (SSG) applies the concept of an interface direction, either uplink or downlink. It uses this direction when determining the forwarding path of an incoming packet. The **ssg direction** command allows you to specify a direction for an interface or a range of subinterfaces.

The **ssg direction** command allows you to configure the direction for a range of permanent virtual circuits (PVCs). All members of a range must have the same direction.

Before you can change a direction from uplink to downlink or vice versa, you must use the **no ssg direction** command to clear the direction.

The **ssg direction** command replaces the **ssg bind direction** command. If you reboot a router that uses an old configuration, the **ssg bind direction** commands will be converted to **ssg direction** commands until the **ssg bind direction** command is made obsolete. In a later release, the **ssg bind direction** command may no longer be supported.

Note An interface that does not exist will not be created as a result of the **ssg direction** command.

In cases where a service has a single next-hop IP address, the **ssg direction** uplink command can be used with the **member** keyword and *group-name* argument to group together uplink interfaces that share a common service and enable the interfaces to be treated similarly.

The group setting for an uplink interface cannot be changed when there are active services bound to that interface.

The **no** form of the **ssg direction** command can be used only when there are no active services bound to the uplink interface.

The command operates on a variety of interfaces, including async, group async, ATM, extended tag ATM (XTagATM), bridge group virtual (BVI), CTunnel, tunnel, dialer, IEEE 802.3 Ethernet, IEEE 802.3 Fast Ethernet, IEEE 802.3z GigabitEthernet, loopback, multilink Frame Relay (MFR) bundle, multilink group, Pragmatic General Multicast (PGM) Host (Vif), virtual access, virtual template, and virtual Token Ring.

Examples

The following example sets the direction of a Fast Ethernet interface to downlink while in interface configuration mode:

```
ssg enable
interface FastEthernet 1/0
 ssg direction downlink
```

The next example creates a range called “MyRange” and sets the direction of all subinterfaces in the range to downlink while in subinterface configuration mode:

```
ssg enable
interface ATM 1/0.1 point-to-point
 range MyRange pvc 1/32 1/42
 ssg direction downlink
```

Related Commands

Command	Description
range pvc	Defines a range of ATM PVCs.
show ssg direction	Displays the direction of all interfaces for which a direction has been specified.
show ssg interface	Displays SSG information about one or more interfaces.

ssg enable

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg enable** command is not available in Cisco IOS software.

To enable 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 [**force-cleanup**]

Syntax Description

force-cleanup	(Optional) Unconfigures SSG and releases all resources that were acquired by SSG.

Command Default

SSG is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 node route processor (NRP).
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.
12.2(15)B	The **force-cleanup** keyword was added.
12.3(4)T	The **force-cleanup** keyword was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enable SSG. If you enter the **ssg enable** command while the system is in the process of unconfiguring SSG, you will see a warning message, and the command will have no effect.

Use the **no ssg enable force-cleanup** command to unconfigure SSG and release all system resources for SSG.

Examples

The following example shows how to enable SSG:

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

The following example shows how to stop SSG packet processing and control events:

```
Router(config)# no ssg enable
```

The following example shows how to stop SSG packet processing and control events, unconfigure SSG, and release all SSG resources:

```
Router(config)# no ssg enable force-cleanup
```

ssg intercept dhcp

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg intercept dhcp** command is not available in Cisco IOS software.

To configure the Service Selection Gateway (SSG) to force subscribers to get IP addresses from their ISPs using Dynamic Host Configuration Protocol (DHCP), use the **ssg intercept dhcp** command in global configuration mode. To disable IP address assignment from the ISP via DHCP, use the **no** form of this command.

ssg intercept dhcp

no ssg intercept dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

SSG performs Network Address Translation (NAT) between the IP address assigned by the ISP with the original IP address of the subscriber.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **ssg intercept dhcp** command to force subscribers to request IP addresses from their ISPs using DHCP.

When a subscriber's router acts either as an IOS DHCP server or an IOS DHCP relay agent and the subscriber is a DHCP client, then configuring SSG/DHCP Awareness will remove the SSG host object. When an active host object receives a DHCPRELEASE or when the DHCP lease for an active host object expires, the SSG host object is removed.

For more information on the **ssg intercept dhcp** command, see the *Cisco IOS Intelligent Service Gateway Configuration Guide.*

Examples

The following example shows how to enable the IP address assignment from the ISP via DHCP:

```
ssg intercept dhcp
```

Related Commands

Command	Description
debug ssg dhcp	Enables the display of control errors and events related to SSG-DHCP IP address allocation.

ssg local-forwarding

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg local-forwarding** command is not available in Cisco IOS software.

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.

Command Default

Disabled

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

The following example enables local forwarding:

```
ssg local-forwarding
```

ssg login transparent

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg login transparent** command is not available in Cisco IOS software.

To enable the Service Selection Gateway (SSG) Transparent Autologon feature and enable transparent auto-logon configuration mode, use the **ssg login transparent** command in global configuration mode. To disable the Transparent Autologon feature, remove all the commands that were configured under transparent auto-logon mode, log off all the transparent autologon users, and refuse new logons, use the **no** form of this command.

ssg login transparent

no ssg login transparent

Syntax Description

This command has no arguments or keywords.

Command Default

The SSG Transparent Autologon feature is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

The following example enables the SSG Transparent Autologon feature:

```
ssg login transparent
```

Related Commands

Command	Description
show ssg user transparent	Displays a list of all the SSG transparent autologon users.

ssg maximum host

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg maximum host** command is not available in Cisco IOS software.

To limit the number of user connections (hosts) allowed on a Service Selection Gateway (SSG) device, use the **ssg maximum host** command in global configuration mode. To remove the limitation on the number of hosts, use the **no** form of this command.

ssg maximum host *number-of-hosts*

no ssg maximum host *number-of-hosts*

Syntax Description

number-of-hosts	Limits the number of host objects allowed on an SSG device. Range: 1 to 2147483647.

Command Default

Unlimited hosts are allowed on an SSG device.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)M	This command was removed.

Usage Guidelines

This command prevents resource exhaustion on a router by limiting the number of host connections. When the router reaches the maximum number of connections, it refuses any new connections. As users log out, new users are allowed to connect.

This command limits only the number of host connections; it does not limit the number of services available to users.

Examples

The following example limits the number of host connections to 1,000:

```
Router(config)# ssg maximum host 1000
```

Related Commands

Command	Description
ssg maximum service	Limits the number of services available to SSG users.
user passthrough maximum	Limits the number of SSG transparent autologon users on an SSG device.

ssg maximum service

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg maximum service** command is not available in Cisco IOS software.

To limit the number of services available to a user on a Service Selection Gateway (SSG) device, use the **ssg maximum service** command in global configuration mode. To remove the limitation on the number of services, use the **no** form of this command.

ssg maximum service *number-of-services*

no ssg maximum service *number-of-services*

Syntax Description

number-of-services	Limits the number of services available to a user on an SSG device. The valid range of services is 1 to 20.

Command Default

Users have up to 20 services available.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced. This command replaces the **ssg maxservice** command.
15.0(1)M	This command was removed.

Usage Guidelines

This command enables you to limit the number of services available to a user. This command replaces the **ssg maxservice** command. If you issue the **ssg maxservice** command and save your configuration, the saved configuration shows the **ssg maximum service** command.

Examples

The following example limits the number of user services to 10:

```
Router(config)# ssg maximum service 10
```

Related Commands

Command	Description
ssg maximum host	Limits the number of host connections on an SSG device.

ssg maxservice

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg maxservice** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Release 12.4(2)T, the **ssg maxservice** command is replaced by the **ssg maximum service** command. See the **ssg maximum service** command for more information.

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

number	Maximum number of services per user. The minimum value is 0; the maximum is 20.

Command Default

The default maximum number of services per user is 20.

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4(2)T	This command was replaced by the **ssg maximum service** command.
15.0(1)M	This command was removed.

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:

```
ssg maxservice 10
```

ssg multidomain ppp

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg multidomain ppp** command is not available in Cisco IOS software.

To enter PPP Termination Aggregation-Multidomain (PTA-MD) configuration mode, use the **ssg multidomain ppp** command in global configuration mode. To disable all PTA-MD configurations, use the **no** form of this command.

ssg multidomain ppp

no ssg multidomain ppp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

It is important to note that the **no** form of this command disables everything configured for PTA-MD. If you want to exit PTA-MD configuration mode, enter the **exit** command.

Examples

Adding Domains to an Existing PTA-MD Exclusion List

In the following example, a PTA-MD exclusion list that already includes “cisco”, “motorola”, “nokia”, and “voice-stream” is downloaded from the AAA server. After the exclusion list is downloaded, “microsoft” and “sun” are added to the exclusion list.

The exclusion list currently on the AAA server includes “cisco”, “motorola”, “nokia”, and “voice-stream”:

```
user = pta_md{
profile_id = 119
profile_cycle = 2
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
```

```
}
reply_attributes= {
9,253="XPcisco"
9,253="XPmotorola"
9,253="XPnokia"
9,253="XPvoice-stream"
```

In the following example, the PTA-MD exclusion list is downloaded to the router from the AAA server. The password to download the exclusion list is “cisco”. After the PTA-MD exclusion list is downloaded, “microsoft” and “sun” are added to the list using the router CLI:

```
ssg multidomain ppp
 download exclude-profile pta_md cisco
 exclude domain microsoft
 exclude domain sun
```

The enhancements to the exclusion list are then verified:

```
Router# show ssg multidomain ppp exclude-list

Profile name :pta_md
1   cisco
2   motorola
3   nokia
4   voice-stream

Domains added via CLI :
1   microsoft
2   sun
```

Related Commands

Command	Description
download exclude-profile (SSG PTA-MD)	Downloads the PTA-MD exclusion list on the AAA server to the router.
exclude (SSG PTA-MD)	Adds a domain name to the existing PTA-MD exclusion list.
show ssg multidomain ppp exclude-list	Displays the contents of the PTA-MD exclusion list.

ssg next-hop download

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg next-hop download** command is not available in Cisco IOS software.

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

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

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

Syntax Description

profile-name	(Optional) Profile name.
profile-password	(Optional) Profile password.

Command Default

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 (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

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:

```
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

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg open-garden** command is not available in Cisco IOS software.

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

profile-name	Local service profile name.

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.

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:

```
local-profile cisco.com
 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"
 exit
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.

Command	Description
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

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg pass-through** command is not available in Cisco IOS software.

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.
ip-access-list	(Optional) IP access list (standard or extended).
ip-extended-access-list	(Optional) IP extended access list (standard or extended).
access-list-name	(Optional) Access list name.
download	(Optional) Load a service profile and use its filters as default filters.
profile-name	(Optional) Service profile name.
profile-password	(Optional) Service profile password.
downlink	(Optional) Apply filter to downlink packets.
uplink	(Optional) Apply filter to uplink packets.

Command Default

Transparent pass-through is disabled.

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

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”:

```
ssg pass-through
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

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map** command is not available in Cisco IOS software.

To enable the Service Selection Gateway (SSG) Port-Bundle Host Key feature and enter SSG portmap configuration mode, use the **ssg port-map** command in global configuration mode. To disable the port-bundle host key feature, use the **no** form of this command.

ssg port-map

no ssg port-map

Syntax Description

This command has no arguments or keywords.

Command Default

The Port-Bundle Host Key feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command will not take effect until the router has 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).

Examples

The following example shows how to enable the SSG port-bundle host key and enter SSG portmap configuration mode:

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

Related Commands

Command	Description
destination access-list	Specifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.
destination range	Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic.
length (SSG)	Modifies the port-bundle length upon the next SSG reload.
source ip	Specifies SSG source IP addresses to which to map the destination IP addresses in subscriber traffic.

ssg port-map destination access-list

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map destination access-list** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the **destination access-list** command. See the **destination access-list** command page for more information.

To identify packets for port-mapping by specifying an access list to compare against 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

access-list-number	Integer from 100 to 199 that is the number or name of an extended access list.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **destination access-list** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **destination access-list** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

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 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
```

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

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map destination range** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the **destination range** command. See the **destination range** command page for more information.

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

Command Default

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 (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **destination range** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **destination range** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

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 from 8080 to 8081 will be port-mapped:

```
ssg port-map destination range from 8080 to 8081
```

Related Commands

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

ssg port-map enable

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map enable** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the **ssg port-map** command. See the **ssg port-map** command page for more information.

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.

Command Default

SSG port-bundle host key is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **ssg port-map** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **ssg port-map** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

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 CiscoSubscriber 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:

```
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

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map length** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the length command. See the **length (SSG)** command page for more information.

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.

Command Default

4 bits.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **length** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **length** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

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 19 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 19 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
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

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg port-map source ip** command is not available in Cisco IOS software.

Note Effective with Cisco IOS Releases 12.2(16)B and 12.3(4)T, this command is replaced by the **source ip** command. See the **source ip** command page for more information.

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

ip-address	SSG source IP address.
interface	Interface whose main IP address is used as the SSG source IP address.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	Support for this command was added to other platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(16)B	This command was replaced by the **source ip** command in Cisco IOS Release 12.2(16)B.
12.3(4)T	This command was replaced by the **source ip** command in Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

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 are 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** command in global configuration mode.

Examples

The following example shows the SSG source IP address 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 prepaid reauthorization drop-packet

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg prepaid reauthorization drop-packet** command is not available in Cisco IOS software.

To configure Service Selection Gateway (SSG) to drop prepaid traffic during reauthorization if threshold values are not configured, use the **ssg prepaid reauthorization drop-packet** command in global configuration mode. To configure SSG to forward traffic during reauthorization and not to drop traffic during reauthorization, use the **no** form of this command.

ssg prepaid reauthorization drop-packet

no ssg prepaid reauthorization drop-packet

Syntax Description

This command has no arguments or keywords.

Command Default

SSG forwards traffic during reauthorization by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

SSG sends a service reauthorization request to the billing server when a prepaid user's quota is consumed or after the configured idle timeout expires. If the billing sever returns a zero quota in the reauthorization response, the connection is terminated, but the data that was in progress during the reauthorization is not counted in the reauthorization.

Use this command to configure how traffic is handled during reauthorization. This command configures SSG to drop all prepaid user traffic during reauthorization when threshold values are not configured. If you configure SSG to drop traffic during reauthorization and a threshold value is configured, traffic is not dropped during reauthorization until the user exhausts the allotted quota. If a user exhausts the allotted quota, traffic gets dropped until SSG receives the reauthorization response. By default, traffic continues during reauthorization.

Use the **no ssg prepaid reauthorization drop-packet** command to configure SSG not to drop any traffic during reauthorization.

Examples

The following example shows how to configure SSG to drop traffic during reauthorization:

```
ssg prepaid reauthorization drop-packet
```

Related Commands

Command	Description
ssg prepaid threshold	Configures SSG to reauthorize a prepaid user's connection when the user's remaining quota reaches the configured threshold value.

ssg prepaid threshold

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg prepaid threshold** command is not available in Cisco IOS software.

To configure a Service Selection Gateway (SSG) prepaid threshold value, use the **ssg prepaid threshold** command in global configuration mode. To disable the SSG prepaid threshold value, use the **no** form of this command.

ssg prepaid threshold {**volume** *bytes* | **time** *seconds* | **default-quota** *number-of-times*}

no ssg prepaid threshold {**volume** *bytes* | **time** *seconds* | **default-quota** *number-of-times*}

Syntax Description

volume	Prepaid threshold volume configuration.
bytes	Threshold volume, in bytes. Range: 0 to 65535566.
time	Prepaid threshold time configuration.
seconds	Threshold time, in seconds. Range: 0 to 6565656.
default-quota	Default quota for prepaid server failure.
number-of-times	Maximum number of times SSG will allocate the default quota.

Command Default

No SSG prepaid threshold values are configured, and reauthorization happens only after a user has completely exhausted the allotted quota.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	The **default-quota** keyword was added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to configure an SSG prepaid threshold value. By default, SSG reauthorizes a prepaid user's connection only after the user's allotted quota has been consumed. When a prepaid threshold value is configured, SSG reauthorizes a prepaid user's connection before the user has completely consumed the allotted quota for a service.

For a prepaid threshold time configuration, the threshold time is in seconds and should be configured to be at least equal to the connection reauthorization time.

For a prepaid threshold volume configuration, the threshold volume is in bytes and should be at least equal to the user's bandwidth multiplied by the reauthorization time. Calculate the prepaid threshold volume value using the following formula:

(*threshold value*) >= *B* * *T*

where

B (Bps) = user's bandwidth

T (seconds) = reauthorization time

SSG can be configured to allocate a default quota when the prepaid server fails to respond to an authorization or reauthorization request. Use the **default-quota** keyword to specify the maximum number of times that SSG will allocate the default quota per instance of prepaid billing server unavailability.

Examples

The following example shows how to configure a threshold time value of 10 seconds:

```
ssg prepaid threshold time 10
```

The following example shows how to configure a threshold volume value of 2000 bytes:

```
ssg prepaid threshold volume 2000
```

The following example shows how to configure a prepaid default quota threshold of 65:

```
ssg prepaid threshold default-quota 65
```

Related Commands

Command	Description
ssg prepaid reauthorization drop-packet	Configures SSG to drop prepaid traffic during reauthorization.

ssg profile-cache

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg profile-cache** command is not available in Cisco IOS software.

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.

Command Default

User-profile caching is not enabled.

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

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:

```
ssg profile-cache
```

ssg qos police

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg qos police** command is not available in Cisco IOS software.

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

ssg qos police [**user** | **session**]

no ssg qos police [**user** | **session**]

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

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

Examples

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

```
user = johndoe
radius = 7200-SSG-v1.1
check_items= {
2 = cisco
```

```
}
reply_attributes={
9,250="Nproxy_ser"
9,250="Ntunnel_ser"
9,250="QD8000;2000;0"
```

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

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

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

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

- The first packet is 500 bytes and arrives 3/4 second after the last packet.
  - The packet size is 500 bytes.
  - The time difference (td) is 3/4 of a second.
  - actual_debt = previous_actual_debt + packet_size = 0 + 500 = 500
  - tokens = committed_rate * 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.
  - actual_debt = 0 + 1500 = 1500
  - tokens = 1000 * 1/2 = 500
  - 500 < 1500. Therefore, the tokens are less than the actual debt. Because the tokens are less than the actual debt, an updated actual debt must be calculated and compared to the normal burst size.
  - New actual_debt = previous_actual_debt – 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.
  - actual_debt = previous_actual_debt + packet_size = 1000 + 4000 = 5000
  - tokens = 1000 * 1/2 = 500
  - 500 < 5000. The tokens are less than the actual debt, so the new actual debt must be computed.
  - actual_debt = previous_actual_debt – 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 query mac dhcp

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg query mac dhcp** command is not available in Cisco IOS software.

To configure the Service Selection Gateway (SSG) to send a Dynamic Host Control Protocol (DHCP) lease query request to the configured DHCP server when a subscriber's Media Access Control (MAC) address is not already known, use the **ssg query mac dhcp** command in global configuration mode. To disable the sending of DHCP lease query requests, use the **no** form of this command.

ssg query mac dhcp

no ssg query mac dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

SSG does not send DHCP lease query requests.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

SSG can be configured to authenticate a subscriber on the basis of the subscriber's MAC address. Use the **ssg query mac dhcp** command to configure SSG to request a subscriber's MAC address when the MAC address is not already present in a subscriber's user profile.

Examples

The following example enables SSG to send a DHCP lease query request to determine the MAC address of a subscriber:

```
ssg query mac dhcp
```

Related Commands

Command	Description
query ip dhcp	Sends DHCP lease query requests for the subscriber session when no IP address is received in the accounting start record.
username mac	Sends a subscriber's MAC address as RADIUS attribute 1 in TAL requests.

ssg radius-helper

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg radius-helper** command is not available in Cisco IOS software.

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* | **access-list** *acl-id* | **validate**]

no ssg radius-helper [**acct-port** *port-number* | **auth-port** *port-number* | **key** *key* | **access-list** *acl-id* | **validate**]

Syntax Description

acct-port *port-number*	(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 *port-number*	(Optional) UDP destination port for RADIUS authentication requests; the host is not used for authentication if set to 0. The default is 1645.
key *key*	(Optional) Key shared with the RADIUS clients.
access-list *acl-id*	(Optional) Specifies the access list to be applied to traffic from the Subscriber Edge Services Manager (SESM). • *acl-id* specifies the IP access list number (or list name) for packets from radius clients. The number range is 1 to 99 (or 1300 to 2699 for an expanded range of RADIUS clients). **Note** The *acl-id* argument also allows you to enter the IP access list name for packets from RADIUS clients.
validate	(Optional) Enables the validation of SESM IP addresses. **Note** The Service Selection Gateway (SSG) accepts commands only from validated IP addresses.

1. UDP = User Datagram Protocol

Command Default

Communications with the Cisco SSD is not enabled.

Command Modes

Global configuration (config)

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.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(3)T	The **validate** keyword was added.
12.3(4)T	The **access-list** *acl-id* keyword and argument were added.
15.0(1)M	This command was removed.

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 communications with the Cisco SSD:

```
router(config)# ssg radius-helper acct-port 1646 auth-port 1645
router(config)# ssg radius-helper key MyKey
router(config)# ssg radius-helper access-list 98
router(config)# ssg radius-helper validate
```

ssg radius-proxy

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg radius-proxy** command is not available in Cisco IOS software.

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.

Command Default

SSG RADIUS Proxy is not enabled by default.

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

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.
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-cache

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg service-cache** command is not available in Cisco IOS software.

To enable the Service Selection Gateway (SSG) Service Profile Caching feature, or to change the refresh interval for services in the service profile cache, use the **ssg service-cache** command in global configuration mode. To disable Service Selection Gateway (SSG) service profile caching, use the **no** form of this command.

ssg service-cache [**refresh-interval** *minutes*]

no ssg service-cache [**refresh-interval** *minutes*]

Syntax Description

refresh-interval	(Optional) Changes the refresh rate for the SSG service profile cache. An SSG service profile refreshes by getting the service profile from the authentication, authorization, and accounting (AAA) server. If the **refresh-interval** argument is not entered, the default refresh rate of every 120 minutes is used.
minutes	(Optional) Specifies how often, in minutes, the service profiles in the SSG service profile cache will be refreshed.The refresh interval can be configured in one-minute increments between 10 minutes and 34,560 minutes (24 days). The default is every 120 minutes.

Command Default

SSG service profile caching is enabled by default.
The default refresh interval for the SSG service profile cache is every 120 minutes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

The **ssg service-cache** command is used to enable SSG service profile caching. A refresh interval does not have to be specified (the default of 120 minutes will be used if no refresh interval is configured).

If the refresh interval is set at 180, the SSG service profile cache will check the AAA server for the service profiles in the cache every 180 minutes.

This command enhances the authentication process for SSG service logon by allowing users to authorize to a service using a service profile cached in SSG instead of downloading the service profile from the AAA server.

When this command is entered, all of the service profiles currently in use in SSG are immediately cached.

Examples

In the following example, SSG service profile caching is enabled:

```
ssg service-cache enable
```

In the following example, the service profiles in the SSG service profile cache will be updated from the AAA server every 240 minutes:

```
ssg service-cache refresh-interval 240
```

Related Commands

Command	Description
show ssg service	Displays various information about an SSG service, including the time remaining for the specified service to refresh.
ssg service-cache refresh	Manually updates the SSG service profile cache with the service profiles available on the AAA server.

ssg service-cache refresh

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg service-cache refresh** command is not available in Cisco IOS software.

To trigger an update to the Service Selection Gateway (SSG) service profile cache with the service profiles available on the authentication, authorization, and accounting (AAA) server, use the **ssg service-cache refresh** command in privileged EXEC mode.

ssg service-cache refresh [*service-name* | **all**]

no ssg service-cache refresh [*service-name* | **all**]

Syntax Description

service-name	Specifies a specific service should be refreshed. Required to refresh one SSG service profile in the SSG service profile cache.
all	Specifies that all of the service profiles in the SSG service profile cache should be refreshed. Required to refresh all SSG profiles in the SSG profile cache.

Command Default

The SSG service profile cache, if enabled, is refreshed at intervals based on the **ssg service-cache refresh-interval** configuration. If an **ssg service-cache refresh-interval** is not specified, the default refresh rate is every 120 minutes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command is used to refresh the profiles in the SSG service profile cache manually from the AAA server. The service profiles in the SSG service profile cache are automatically refreshed with the profiles from the AAA server at user-configurable intervals using the **ssg service-cache refresh-interval** command. The user can trigger a refresh at any time by issuing this command.

If an SSG service cache refresh fails for any reason (for instance, the AAA server is unreachable or down), the service profile caching for that service is disabled. Once a user is able to download the service successfully, caching for the service begins again.

Examples

In the following example, all of the service profiles in the SSG service profile cache will be retrieved from the AAA server and will replace the service profiles in the SSG service profile cache:

```
ssg service-cache refresh all
```

In the following example, service profile “service1” will be retrieved from the AAA server and will replace the current “service1” profile in the SSG service profile cache:

```
ssg service-cache refresh service1
```

Related Commands

Command	Description
ssg service-cache	Enables SSG service profile caching.

ssg service-password

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg service-password** command is not available in Cisco IOS software.

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

password	Service profile password.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

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:

```
ssg service-password MyPassword
```

ssg service-search-order

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg service-search-order** command is not available in Cisco IOS software.

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.

Command Default

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

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

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:

```
ssg service-search-order local remote
```

Related Commands

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

ssg tcp-redirect

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg tcp-redirect** command is not available in Cisco IOS software.

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.

Command Default

This command has no default behavior.

Command Modes

Global configuration (config)

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.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

ssg vc-service-map

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg vc-service-map** command is not available in Cisco IOS software.

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-vpi*/*vci* [*end-vpi* | *end-vpi*/*vci*] **exclusive** | **non-exclusive**

no ssg vc-service-map *service-name* [**interface** *slot-module-port*] *start-vpi* | *start-vpi*/*vci* [*end-vpi* | *end-vpi*/*vci*] **exclusive** | **non-exclusive**

Syntax Description

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

Command Default

The service mapping is non-exclusive by default.

Command Modes

Global configuration (config)

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.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

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:

```
ssg vc-service-map Worldwide 3/33 exclusive
```

Related Commands

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

ssg wlan reconnect

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg wlan reconnect** command is not available in Cisco IOS software.

To enable Extensible Authentication Protocol (EAP) users to reconnect after logging off or after idle timeout has occurred, use the **ssg wlan reconnect** command in global configuration mode. To disable the ability of EAP users to reconnect, use the **no** form of this command.

ssg wlan reconnect

no ssg wlan reconnect

Syntax Description

This command has no arguments or keywords.

Command Default

EAP users cannot reconnect.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(16)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

EAP users do not have a username and password. If they access Subscriber Edge Services Manager (SESM), log off, and try to reconnect to the service later, SESM presents them with a logon page, which they cannot use. To allow users to reconnect without being asked to log on again, enable the user reconnect feature with the **ssg wlan reconnect** command.

If a user logs off through SESM, when the Service Selection Gateway (SSG) EAP transparency user reconnect functionality has been enabled, SSG inactivates the host. If the user tries to access the service again, SESM queries SSG, and SSG activates the host and enables autologon services.

The SSG host, whether active or inactive, is deleted when the Access Zone Router (AZR) sends an Accounting Stop packet to SSG (when the user walks out of the private wireless LAN (PWLAN) or the Dynamic Host Configuration Protocol (DHCP) address is released).

Note If user reconnect is enabled and a user refreshes or reloads the SESM page after an account logoff, SESM sends a query to SSG, which causes SSG to activate the host. It is recommended that users be made aware of this behavior so they do not accidentally activate the host.

Examples

The following example enables EAP users to reconnect after logging off:

```
ssg wlan reconnect
```

timeouts (SSG-radius-proxy)

Note Effective with Cisco IOS Release 15.0(1)M, the **timeouts** (SSG-radius-proxy) command is not available in Cisco IOS software.

To enter SSG-radius-proxy-timers configuration mode, use the **timeouts** command in SSG-radius-proxy configuration mode. To restore all timeouts, use the **no** form of this command.

timeouts

no timeouts

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to enter SSG-radius-proxy-timeouts configuration mode to configure SSG RADIUS proxy handoff, idle, IP address, and Mobile Station ID (MSID) timeouts.

Examples

The following example shows how to enter SSG-radius-proxy-timeouts mode:

```
ssg radius-proxy
 timeouts
```

user passthrough maximum

Note Effective with Cisco IOS Release 15.0(1)M, the **user passthrough maximum** command is not available in Cisco IOS software.

To limit the number of Service Selection Gateway (SSG) transparent autologon (TAL) users on an SSG device, use the **user passthrough maximum** command in SSG login transparent submode. To remove the limitation on the number of SSG TAL users, use the **no** form of this command.

user passthrough maximum *number-of-users*

no user passthrough maximum *number-of-users*

Syntax Description

number-of-users	Limits the number of SSG TAL users on an SSG device. Range: 1 to 2147483647.

Command Default

Unlimited TAL users can access an SSG device.

Command Modes

SSG login transparent submode

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)M	This command was removed.

Usage Guidelines

This command prevents resource exhaustion on a router by limiting the number of SSG TAL users on a device. When the router reaches the maximum number of users, it refuses any new connections.

Examples

The following example limits the number of SSG TAL users to 400:

```
Router(config)# ssg logon transparent
Router(config-login-transparent)# user passthrough maximum 400
```

Related Commands

Command	Description
ssg maximum host	Limits the number of host connections on an SSG device.
ssg maximum service	Limits the number of services available to a user on an SSG device.

user suspect maximum

Note Effective with Cisco IOS Release 15.0(1)M, the **user suspect maximum** command is not available in Cisco IOS software.

To specify the maximum number of Service Selection Gateway (SSG) transparent autologon suspect (SP) users that can be added to the suspect user list, use the **user suspect maximum** command in transparent auto-logon configuration mode. To remove the specification, use the **no** form of this command.

user suspect maximum *value*

no user suspect maximum *value*

Syntax Description

value	Maximum number of suspect users that can be added to the SP list. Valid range is from 10 to 5000.

Command Default

5000 suspect users.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

An SSG transparent autologon user becomes suspect when the user's authentication, authorization, and accounting (AAA) attempt is rejected.

If the number of suspect users exceeds the maximum value configured, SSG sends a system logging message and does not add any further users to the SP list.

Examples

The following example specifies that the maximum number of suspect users that can be added to the SP list is 200:

```
Router(config-login-transparent)# user suspect maximum 200
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

user suspect timeout

Note Effective with Cisco IOS Release 15.0(1)M, the **user suspect timeout** command is not available in Cisco IOS software.

To specify the maximum length of time for which a Service Selection Gateway (SSG) transparent autologon suspect (SP) user remains in the suspect user list, use the **user suspect timeout** command in transparent auto-logon configuration mode. To return to the default length of time, use the **no** form of this command.

user suspect timeout *timeout*

no user suspect timeout *timeout*

Syntax Description

timeout	Maximum length of time (in minutes) that a suspect user remains in the suspect user list. Range is from 1 to 34560.

Command Default

60 minutes.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

If a packet is received for a user who is marked as an SP user, packets to or from this user are dropped or TCP-redirected until the *timeout* value is reached. When the *timeout* value is reached, any new traffic received by SSG from the user triggers the transparent autologon procedure.

Examples

The following example specifies that a suspect user will remain in the suspect user list for 30 minutes:

```
Router(config-login-transparent)# user suspect timeout 30
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Auto-Logon feature.

user unidentified timeout

Note Effective with Cisco IOS Release 15.0(1)M, the **user unidentified timeout** command is not available in Cisco IOS software.

To specify the maximum length of time for which a Service Selection Gateway (SSG) transparent autologon unidentified user remains marked as no response (NR), use the **user unidentified timeout** command in transparent auto-logon configuration mode. To return to the default timeout value, use the **no** form of this command.

user unidentified timeout *timeout*

no user unidentified timeout *timeout*

Syntax Description

timeout	Length of time (in minutes) that a user remains marked as NR. Range is from 1 to 34560.

Command Default

10 minutes.

Command Modes

Transparent auto-logon

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

An unidentified user is marked NR if there is no response from the authentication, authorization, and accounting (AAA) server to an authorization request and the authorization request times out.

If a packet is received for a user who is marked as an NR user, packets to or from this user are dropped or TCP-redirected until the *timeout* value is reached. When the *timeout* value is reached, any new traffic received by SSG from the user triggers the transparent logon procedure.

Examples

The following example sets the user-unidentified timeout to 5 minutes:

```
Router(config-login-transparent)# user unidentified timeout 5
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Auto-Logon feature.

user unidentified traffic permit

Note Effective with Cisco IOS Release 15.0(1)M, the **user unidentified traffic permit** command is not available in Cisco IOS software.

To specify that packets received from a Service Selection Gateway (SSG) transparent autologon user whose authorization request has timed out will be forwarded or received, use the **user unidentified traffic permit** command in transparent auto-logon configuration mode. To return to the default, use the **no** form of this command.

user unidentified traffic permit

no user unidentified traffic permit

Syntax Description

This command has no arguments or keywords.

Command Default

Packets received from a user whose authorization request has timed out are dropped.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
15.0(1)M	This command was removed.

Usage Guidelines

Configuring this command allows traffic flow for NR users toward the service network.

Examples

The following example specifies that packets received from a user whose authorization request has timed out will be forwarded or received:

```
Router(config-login-transparent)# user unidentified traffic permit
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Auto-Logon feature.

username mac

Note Effective with Cisco IOS Release 15.0(1)M, the **username mac** command is not available in Cisco IOS software.

To configure the Service Selection Gateway (SSG) to send a subscriber's MAC address as the username (RADIUS attribute 1) in transparent autologon (TAL) authorization requests, use the **username mac** command in SSG login transparent submode. To disable the sending of the subscriber's MAC address and send the subscriber's IP address instead, use the **no** form of this command.

username mac

no username mac

Syntax Description

This command has no arguments or keywords.

Command Default

SSG sends the subscriber's IP address as the username (RADIUS attribute 1).

Command Modes

SSG login transparent submode

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **username mac** command to configure SSG to send a subscriber's MAC address as the username in TAL authorization requests.

Examples

The following example enables SSG to send a subscriber's MAC address as the username in TAL authorization requests:

```
username mac
```

Related Commands

Command	Description
query ip dhcp	Sends DHCP lease query requests for the subscriber session when no IP address is received in the accounting start record.
ssg query mac dhcp	Sends a DHCP lease query request to the DHCP server when a subscriber's MAC address is not known.