select

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

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

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

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

Syntax Description

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

Command Default

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

Command Modes

SSG-auto-domain

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

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

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

Examples

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

```
ssg enable
ssg auto-domain
 mode extended
 select username
```

```
 exclude apn motorola
 exclude domain cisco
 download exclude-profile abc password1
 nat user-address
```

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

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

Related Commands

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

server (SSG)

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

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

server *ip-address port*

no server *ip-address port*

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

SSG-redirect-group configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
server-group	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

server-group

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

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

server-group *group-name*

no server-group *group-name*

Syntax Description

group-name	The name of the captive portal group.

Command Default

No default behavior or values.

Command Modes

SSG-redirect configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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 define and name a captive portal group. Service Selection Gateway (SSG) TCP Redirect for Services provides nonauthorized users access to controlled services within an SSG. Packets sent upstream from an unauthenticated user are forwarded to the captive portal that deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services into which they are not logged.

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

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

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

Examples

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

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

Related Commands

Command	Description
server (SSG)	Adds a server to a captive portal group.
show ssg tcp-redirect group	Displays information about the captive portal groups and the networks associated with the captive portal groups.
show tcp-redirect mappings	Displays information about the TCP redirect mappings for hosts within your system.
ssg enable	Enables SSG.
ssg tcp-redirect	Enables SSG TCP redirect and enters SSG-redirect mode.

server-port

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

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

server-port [**auth** *auth-port*] [**acct** *acct-port*]

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

Syntax Description

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

Command Default

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

Command Modes

SSG-radius-proxy configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
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 the authentication and accounting ports for the SSG Autologon Using Proxy RADIUS feature. Ports configured with this command are global parameters that apply to all proxy clients in the SSG.

Examples

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

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

Related Commands

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

session-identifier

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

To override Service Selection Gateway (SSG) automatic RADIUS client session identification and to configure SSG to identify the specified client session by a specific type of ID attribute, use the **session-identifier** command in SSG-radius-proxy-client mode. To configure SSG to perform user identification only by the username without using a session identification, use the **no** form of this command.

session-identifier [**auto** | **msid** | **correlation-id** | **acct-sess-id**]

no session-identifier [**auto** | **msid** | **correlation-id** | **acct-sess-id**]

Syntax Description

auto	Automatically determines the session identifier.
msid	Uses the MSID as the client session identifier.
correlation-id	Uses the Correlation-ID as the client session identifier.
acct-sess-id	Uses the Accounting-Session-ID as a client session identifier.

Command Default

SSG selects the attribute used for session identification according to the type of client device.

Command Modes

SSG-radius-proxy-client

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

By default, SSG automatically selects the attribute to use for session identification according to the type of RADIUS client device. This attribute is used in the SSG Proxy RADIUS logon table. SSG assigns the following vendor-specific attributes (VSAs) to identify client sessions:

- 3GPP2-Correlation-ID for Packet Data Serving Nodes (PDSNs)
- Accounting-Session-ID for Home Agents (HAs)
- Calling-Station-ID (MSID) for non-CDMA2000 devices such as a general packet radio system (GPRS)

Use the **session-identifier** command to override the automatic session identification. Use the **auto** keyword to return to automatic session identification.

Examples

The following example shows how to configure SSG to use the Correlation-ID to identify the specified client session:

```
session-identifier correlation-id
```

The following example shows how to configure the RADIUS client to proxy all requests from IP address 172.16.0.0 to the RADIUS server, to assign the shared secret "cisco" to the client, and to use the Accounting-Session-ID attribute to identify the specified client session:

```
client-address 172.16.0.0
 key cisco
 session-identifier acct-session-id
```

Related Commands

Command	Description
client-address	Configures the RADIUS client to proxy requests from the specified IP address to the RADIUS server and enters SSG-radius-proxy-client mode.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.

sessions auto cleanup

Note Effective with Cisco IOS Release 15.0(1)M, the **sessions auto-cleanup** command is not available in Cisco IOS software.

To configure an aggregation device to attempt to recover PPP over Ethernet (PPPoE) sessions that failed after reload by notifying customer premises equipment (CPE) devices about the PPPoE session failures, use the **sessions auto cleanup** command in BBA group configuration mode. To disable PPPoE session recovery after reload, use the **no** form of this command.

sessions auto cleanup

no sessions auto cleanup

Syntax Description

This command has no arguments or keywords.

Command Default

PPPoE session recovery after reload is not enabled.

Command Modes

BBA group configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.0(1)M	This command was removed.

Usage Guidelines

If the PPP keepalive mechanism is disabled on a CPE device, the CPE device has no way to detect link or peer device failures over PPPoE connections. When an aggregation device that serves as the PPPoE session endpoint reloads, the CPE will assume that the link is up and will continue to send traffic to the aggregation device. The aggregation device will drop the traffic for the failed PPPoE session.

The **sessions auto cleanup** command enables an aggregation device to attempt to recover PPPoE sessions that existed before a reload. When the aggregation device detects a PPPoE packet for a "half-active" PPPoE session (a PPPoE session that is active on the CPE end only), the device notifies the CPE of the PPPoE session failure by sending a PPPoE active discovery terminate (PADT) packet. The CPE device is expected to respond to the PADT packet by taking failure recovery action.

The **sessions auto cleanup** command must be configured in a PPPoE profile. This command enables PPPoE session recovery after reload on all ingress ports that use the PPPoE profile.

Examples

In the following example, PPPoE session recovery after reload is configured in PPPoE profile “group1”.

```
bba-group pppoe group1
 virtual-template 1
 sessions auto cleanup
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.

show ssg auto-domain exclude-profile

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

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

show ssg auto-domain exclude-profile

Syntax Description

This command has no arguments or keywords.

Command Modes

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

Examples

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

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

Exclude APN Entries Downloaded:

apn1.gprs   apr2.com

Exclude Domain Entries Downloaded:

cisco.com   abcd.com
```

Related Commands

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

Command	Description
select	Configures the Autodomain selection mode.
show ssg auto-domain exclude-profile	Adds to the Autodomain download exclusion list.
ssg enable	Enables SSG functionality.

show ssg binding

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

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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 display services and the interfaces to which they have been bound.

Examples

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

```
Router# show ssg binding

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

Related Commands

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

show ssg connection

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

To display the connections of a given Service Selection Gateway (SSG) host and a service name, use the **show ssg connection** command in privileged EXEC mode.

show ssg connection {*ip-address* | *network-id subnet-mask*} *service-name* [*interface*]

Syntax Description

ip-address	The IP address of an active SSG connection. This is always a subscribed host.
network-id	The IP network ID of an active SSG connection. This is always a subscribed host.
subnet-mask	The IP subnet mask of the subnet-based subscribed host.
service-name	Name of an active SSG connection.
interface	(Optional) IP address through which the host is connected.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(2)B	The *interface* argument was added for the SSG Host Key feature.
12.2(4)B	This command was modified to display information about SSG prepaid billing.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	The modifications from Release 12.2(4)B were integrated into Cisco IOS Release 12.2(13)T.
12.3(1a)BW	This command was modified to display the MSISDN (Calling Station ID) used for service logon.
12.3(3)B	The modifications from Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	The modifications from Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	The *network-id* and *subnet-mask* arguments were added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

Prepaid Service Based on Volume: Example

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

```
Router# show ssg connection 10.10.1.1 InstMsg

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

User Name:
Owner Host:10.10.1.1
Associated Service:InstMsg
Connection State:0 (UP)
Connection Started since:*00:25:58.000 UTC Tue Oct 23 2001
User last activity at:*00:25:59.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
          Input Bytes = 0, Input packets = 0
          Output Bytes = 0, Output packets = 0
          Quota Type = 'VOLUME', Quota Value = 100
Session policing disabled
```

Prepaid Service Based on Time: Example

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

```
Router# show ssg connection 10.10.1.2 Prepaid-internet

------------------------ConnectionObject Content -----------------------
User Name:Host
Owner Host:10.10.1.2
Associated Service:Prepaid-internet
Connection State:0 (UP)
Connection Started since:*00:34:06.000 UTC Tue Oct 23 2001
User last activity at:*00:34:07.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
            Input Bytes = 0, Input packets = 0
            Output Bytes = 0, Output packets = 0
            Quota Type = 'TIME', Quota Value = 100
Session policing disabled
```

Autologin Service: Example

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

```
Router# show ssg connection 10.3.6.1 autologin

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

MSISDN: Example

The following sample output for the **show ssg connection** command shows the MSISDN that is used for service logon:

```
Router# show ssg connection 10.0.1.1 proxy2
```

```
-----------------------ConnectionObject Content -----------------------
User Name: dev-user2
Owner Host: 10.0.1.1
Associated Service: proxy2
Calling station id: 12345
Connection State: 0 (UP)
Connection Started since: *17:44:59.000 GMT Sun Jul 6 2003
User last activity at: *17:44:59.000 GMT Sun Jul 6 2003
Connection Traffic Statistics:
        Input Bytes = 0, Input packets = 0
        Output Bytes = 0, Output packets = 0
Session policing disabled
```

Subnet-Based Subscriber: Example

The following sample output for the **show ssg connection** command shows the subnet mask of the subscribed host:

```
Router# show ssg connection 10.0.1.1 255.255.255.0 passthru

-----------------------ConnectionObject Content -----------------------
User Name: dev-user2
Owner Host: 10.0.1.1 (Mask : 255.255.255.0)
Associated Service: passthru1
Calling station id: 00d0.792f.8054
Connection State: 0 (UP)
Connection Started since: *17:44:59.000 GMT Sun Jul 6 2004
User last activity at: *17:44:59.000 GMT Sun Jul 6 2004
Connection Traffic Statistics:
        Input Bytes = 0, Input packets = 0
        Output Bytes = 0, Output packets = 0
```

Table 9 describes the significant fields shown in the displays.

Table 9 show ssg connection Field Descriptions

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

Related Commands

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

show ssg dial-out exclude-list

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

To display information about the Dialed Number Identification Service (DNIS) prefix profile and the DNIS exclusion list, use the **show ssg dial-out exclude-list** command in privileged EXEC mode.

show ssg dial-out exclude-list

Syntax Description

This command has no arguments or keywords.

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

Use this command to display the DNIS profile name and all DNIS entries configured via CLI or downloaded from a authentication, authorization, and accounting (AAA) server.

Examples

The following example shows sample output for the **show ssg dial-out exclude-list** command:

```
Router# show ssg dial-out exclude-list

Exclude DNIS prefixes downloaded from profile exclude_dnis_aaa
```

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.
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.

show ssg direction

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

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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 show all interfaces that have been specified as uplinks or downlinks.

Examples

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

```
Router# show ssg direction

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

Related Commands

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

show ssg host

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

To display information about a Service Selection Gateway (SSG) subscriber and the current connections of the subscriber, use the **show ssg host** command in privileged EXEC mode. The command syntax of the **show ssg host** command depends on whether the SSG Port-Bundle Host Key feature is enabled.

When SSG Port-Bundle Host Key Is Not Enabled

show ssg host [*ip-address* | **count** | **username** [*subnet-mask*]]

When SSG Port-Bundle Host Key Is Enabled

show ssg host [*ip-address* | **count** | **username**] [*interface* [**username**] [*subnet-mask*]]

Syntax Description

ip-address	(Optional) Host IP address.
count	(Optional) Displays host object count, including inactive hosts.
username	(Optional) Displays all host usernames and IP addresses.
interface	(Optional) Downlink interface through which the host or subscriber is connected, such as ATM, Fast Ethernet, or Virtual-Access. For more information, use the question mark (?) online help function.
subnet-mask	(Optional) The IP subnet mask of the subnet-based subscribed host.

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 Node Route Processor (NRP).
12.2(2)B	The *interface* argument was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)B	This command was modified as follows: • Introduced syntax dependence on SSG host key. • Introduced **count** keyword. • Added fields to the output to display additional information about the status of hosts.
12.3(4)T	The modifications made in Cisco IOS Release 12.2(15)B were integrated into Cisco IOS Release 12.3(4)T.

Release	Modification
12.3(11)T	The output was enhanced to show information about the VPN routing/forwarding instance (VRF) that is associated with a host.
12.3(14)T	The *subnet-mask* argument was added.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

You can specify the Service Selection Gateway (SSG) downlink interface only when the SSG Port-Bundle Host Key feature is enabled. To enable the host key, enter the **ssg port-map** command in global configuration mode. To disable the host key, enter the **no ssg port-map** command.

Examples

Display All Active Hosts: Example

The following example shows all active hosts:

```
Router# show ssg host

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

### Active HostObject Count:2
```

Simple IP Host: Example

The following example shows information about a simple IP host with an IP address of 10.0.0.0:

```
Router# show ssg host 10.0.0.0

----------------------- HostObject Content -----------------------
Activated: TRUE
Interface:
User Name: user1
Owner Host: 10.0.0.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Proxy logon from client IP: 10.0.48.3
    Device: PDSN (Simple IP)
    NASIP : 10.0.48.3
    SessID: 12345678
    APN   :
    MSID  : 5551000
    Timer : None
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *05:59:46.000 UTC Fri May 3 2002
User last activity at: *05:59:52.000 UTC Fri May 3 2002
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: internet-blue;
AutoService: internet-blue;
Subscribed Services: internet-blue; iptv; games; distlearn; corporate; shop; banking;
vidconf;
```

```
Subscribed Service Groups: NONE
```

Mobile IP Host: Example

The following example shows information about a mobile IP host with an IP address of 10.0.0.0:

```
Router# show ssg host 10.0.0.0

----------------------- HostObject Content -----------------------
Activated: TRUE
Interface:
User Name: user1
Owner Host: 10.0.0.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Proxy logon from client IP: 10.0.48.4
    Device: HA
    NASIP : 10.0.48.4
    SessID: 44444445
    APN   :
    MSID  : 5551001
    Timer : None
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *06:01:02.000 UTC Fri May 3 2002
User last activity at: *06:01:09.000 UTC Fri May 3 2002
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: internet-blue;
AutoService: internet-blue;
Subscribed Services: internet-blue; iptv; games; distlearn; corporate; shop; banking;
vidconf;
Subscribed Service Groups: NONE
```

Two Hosts with the Same IP Address: Examples

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

```
Router# show ssg host 10.3.1.1

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

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

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

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

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

```
Router# show ssg host username

   1:10.3.1.1        (active) Host name:pppoauser
```

```
   2:10.3.6.1        (active) Host name:ssguser2

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

Host Associated with a VRF: Example

The following sample output for the **show ssg host** command shows a VRF called "BLUE" associated with a host that has the IP address 10.0.0.2:

```
Router# show ssg host 10.0.0.2

------------------------ HostObject Content ----------------------
Activated: TRUE
Interface: Ethernet1/0   VRF Name: BLUE
User Name: prep-user1
Owner Host: 10.0.0.2
```

Subnet-Based Subscriber: Example

The following example shows information about a subnet-based subscriber with an IP address of 10.0.0.0 and a subnet mask of 255.255.255.0:

```
Router# show ssg host 10.0.0.0 255.255.255.0

------------------------ HostObject Content ------------------------
Activated: TRUE
Interface:
User Name: user1
Host IP : 10.0.0.0
Mask : 255.255.255.0
Msg IP: 0.0.0.0 (0)
Host DNS IP: 0.0.0.0
Maximum Session Timeout: 0 seconds
Host Idle Timeout: 60000 seconds
Class Attr: NONE
User policing disabled
User logged on since: *05:59:46.000 UTC Fri May 3 2004
User last activity at: *05:59:52.000 UTC Fri May 3 2004
SMTP Forwarding: NO
Initial TCP captivate: NO
TCP Advertisement captivate: NO
Default Service: NONE
DNS Default Service: NONE
Active Services: NONE
AutoService: NONE
Subscribed Services: passthru1; proxynat1; tunnel1; proxy1
Subscribed Service Groups: NONE
```

Table 10 describes the significant fields shown in the displays.

Table 10 show ssg host Field Descriptions

Field	Description
Activated:	State of host object. Can be activated or inactivated. Activated—IP address has been assigned to the host, and the host object was created successfully Inactivated—A host is inactivated in the following situations: • When SSG, acting as a RADIUS proxy, is waiting for the IP address of the host, the host object is created, but the state is inactive. • If a host that is using PPP logs off from SSG, but the virtual-access interface of that PPP host is still up, SSG moves the host object to the inactivated state.
Interface:	The interface on the SSG device from which the SSG host is routable.
User Name:	Username that is used to authenticate the host at the authentication, authorization, and accounting (AAA) server.
VRF Name:	VRF associated with the interface for the host.
Owner Host:	IP address and subnet mask assigned to host object.
Msg IP:	IP address of the messaging server. SSG notifies the messaging server of events such as the logging off of a host, an idle-timeout expiration, and a session-timeout expiration. The default messaging server is Subscriber Edge Services Manager (SESM).
Host DNS IP:	IP address of the Domain Name System (DNS) server of the host. This server will be used only if DNS queries cannot be forwarded to a DNS server for the services that are subscribed to by the host.
Device:	Type of device. Device types can be a home agent (HA), Packet Data Serving Node (PDSN), or Generic (for non-CDMA2000 devices).
SessID:	A numeric string derived from the attribute specified as the Session-Identifier.
Timer:	Timer type can be None, Wait for IP, Hand-off, or Wait for MSID.
Maximum Session Timeout:	Session timeout value (RADIUS attribute 27) defined in the user profile. The session timeout value is the amount of time for which the user will stay active after logging on. After this timer expires, the host object is deleted.
Host Idle Timeout:	Maximum amount of time that a host can stay idle (not forwarding any traffic) before the host is deleted from SSG.
Class Attr:	Class attribute (RADIUS attribute 25) defined in the user profile. The class attribute is sent in all host accounting records. This attribute is used by some accounting servers.

Table 10 show ssg host Field Descriptions (continued)

Field	Description
User logged on since:	Time at which the user logged on to SSG.
User last activity at:	Last time the user forwarded traffic via SSG.
Default Service:	This field is not currently supported.
DNS Default Service:	This field is not currently supported.
Active Services:	List of services to which the host has logged on.
AutoService:	List of services to which the host logged on at the time of SSG host logon. These services are defined in the user profile, and the user can access these services after logging on to SSG.
Subscribed Services:	List of services to which the host is able to log on.

Related Commands

Command	Description
clear ssg host	Removes a host object or a range of host objects.
ssg port-map	Enables the SSG port-bundle host key.

show ssg interface

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

To display information about Service Selection Gateway (SSG) interfaces, use the **show ssg interface** command in user EXEC or privileged EXEC mode.

show ssg interface [*interface* | **brief**]

Syntax Description

interface	(Optional) Specific interface for which to display information.
brief	(Optional) Gives brief information about each of the SSG interfaces and their usage.

Command Modes

User EXEC (>)
Privileged EXEC (#)

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

Use this command without any keywords or arguments to display information about all SSG interfaces.

Examples

The following example shows the **show ssg interface brief** command:

```
Router# show ssg interface brief

Interface   Direction           bindingtype    Status
ATM3/0.1    Uplink              Dynamic        Up
ATM3/0.2    Downlink            Static         Down
```

Related Commands

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the IP addresses to which they have been bound.
show ssg direction	Displays the direction of all interfaces for which a direction has been specified.
show ssg summary	Displays a summary of the SSG configuration.

show ssg multidomain ppp exclude-list

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

To display the contents of a PPP Termination Aggregation-Multidomain (PTA-MD) exclusion list, use the **show ssg multidomain ppp exclude-list** command in privileged EXEC mode.

show ssg multidomain ppp exclude-list

Syntax Description

This command has no arguments or keywords.

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 verify the contents of a PTA-MD exclusion list.

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 authentication, authorization, and accounting (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 command-line interface (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 from the AAA server to the router.
exclude (SSG PTA-MD)	Adds a domain name to the existing PTA-MD exclusion list.
ssg multidomain ppp	Enters PTA-MD configuration mode.

show ssg next-hop

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

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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 display all next-hop IP addresses.

Examples

The following example shows the next-hop table:

```
Router# show ssg next-hop

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

Related Commands

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

show ssg open-garden

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

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

show ssg open-garden

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(5)DC	This command was introduced on the Cisco 6400 series node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Examples

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

```
Router# show ssg open-garden

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

Related Commands

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

show ssg pass-through-filter

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

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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 display the downloaded transparent pass-through filter. The filter prevents pass-through traffic from accessing the specified IP address and subnet mask combinations. The filter is set using the **ssg pass-through** command.

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

Examples

The following example shows the pass-through filter:

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

        Service name:  filter01
        Password:      cisco

        Direction:     Uplink

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

Related Commands

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

show ssg pending-command

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

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

show ssg pending-command

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows the pending commands:

```
Router# show ssg pending-command

SSG pending command list:
    ssg bind service Service1.com 192.168.103.1
    ssg bind service Perftest206 192.168.104.5
```

Related Commands

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

show ssg port-map ip

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

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

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

Syntax Description

ip-address	IP address used to identify the port bundle.
port *port-number*	TCP port number used to identify the port bundle.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(11)T	This command was modified to display the downlink VRF associated with the port bundle.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

This command displays the following information about a port bundle:

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

Examples

The following is sample output for the **show ssg port-map ip** command:

```
Router# show ssg port-map ip 192.168.0.1 port 64

State = RESERVED
Subscriber Address = 10.1.1.1
Downlink Interface = Ethernet1/0
Downlink VRF = BLUE

Port-mappings:-

Subscriber Port:   1           Mapped Port:   1039
```

Table 11 describes the significant fields shown in the display.

Table 11 show ssg port-map ip Field Descriptions

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

Related Commands

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

show ssg port-map status

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

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)B	This command was introduced on the Cisco 6400 series.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

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

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

Examples

Display All Bundles Example

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

```
Router# show ssg port-map status

Bundle-length = 4

Bundle-groups:-
```

```
IP Address              Free Bundles            Reserved Bundles         In-use Bundles
10.13.60.2                      4032                       0                      0
```

Table 12 describes the significant fields shown in the display.

Table 12 show ssg port-map status Field Descriptions

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

Display In-Use Bundles Example

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

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

Bundle-group 10.13.60.2 has the following in-use port-bundles:-

Port-bundle             Subscriber Address              Interface

64                      10.10.3.1                       Virtual-Access2
```

Table 13 describes the significant fields shown in the display.

Table 13 show ssg port-map status inuse Field Descriptions

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

Related Commands

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

show ssg prepaid default-quota

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

To display the values of the Service Selection Gateway (SSG) prepaid default quota counters, use the **show ssg prepaid default-quota** command in privileged EXEC mode.

show ssg prepaid default-quota

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

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

SSG maintains two counters to keep track of the number of times the SSG prepaid default quota has been allotted. One counter is for the total number of default quotas allotted by SSG (irrespective of how many times the prepaid server has become available and unavailable). The other counter keeps track of the number of default quotas allotted by SSG during the latest instance of prepaid server unavailability.

Note that the value of the counter for currently allocated default quotas will be zero when the prepaid billing server is available. The counter for currently allocated default quotas restarts at 1 each time the prepaid billing server becomes unavailable.

The **clear ssg prepaid default-quota** command clears the SSG default quota counters.

Examples

The following example shows sample output for the **show ssg prepaid default-quota** command:

```
Router# show ssg prepaid default-quota

### Total default quotas allocated since this counter was last cleared:10

    Default Quota Threshold:100
    Currently allocated Default Quotas:4
```

Table 14 describes the significant fields shown in the display.

Table 14 show ssg prepaid default-quota Field Descriptions

Field	Description
Total default quotas allocated since this counter was last cleared	Total number of default quotas allocated by SSG since the last time the **clear ssg prepaid default-quota** command was entered.
Default Quota Threshold	The maximum number of default quotas that SSG will allocate each time the prepaid billing server is unavailable. This value can be configured by using the **ssg prepaid threshold** command.
Currently allocated Default Quotas	Number of default quotas allocated by SSG during the current instance of prepaid billing server unavailability.

Related Commands

Command	Description
clear ssg prepaid default-quota	Clears the SSG prepaid default quota counters.
ssg prepaid threshold	Configures an SSG prepaid threshold value.

show ssg radius-proxy

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

To display a list of all RADIUS proxy clients, details of a particular RADIUS proxy client, or the pool of IP addresses configured for a router or for a specific domain, use the **show ssg radius-proxy** command in privileged EXEC mode.

show ssg radius-proxy [*ip-address* [**vrf** *vrf-name*]] | [**address-pool** [**domain** *domain-name*] [**free** | **inuse**]]

Syntax Description

ip-address	(Optional) Details for the RADIUS proxy client at this IP address.
vrf *vrf-name*	(Optional) Details for the RADIUS proxy client associated with the specified VPN routing/forwarding (VRF) instance.
address-pool	(Optional) IP addresses configured in an IP pool.
domain	(Optional) IP addresses configured for a specific domain.
domain-name	(Optional) Name of the domain to display.
free	(Optional) IP addresses currently available in the free pool.
inuse	(Optional) IP addresses currently in use.

Command Default

Displays a list of RADIUS proxy clients.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	This command was enhanced to allow display of a list of RADIUS proxy clients.
12.3(4)T	The enhancements from Cisco IOS Release 12.2(15)B were integrated into Cisco IOS Release 12.3(4)T.
12.3(11)T	This command was enhanced to display information about VRFs associated with RADIUS proxy clients.
12.4	This command was integrated into Cisco IOS Release 12.4.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **show ssg radius-proxy** command without any keywords or arguments to display a list of RADIUS proxy clients. This command also displays the IP addresses, device types, timers, and the number of proxy users for each proxy client. Use the *ip-address* argument to display the full list of proxy users for the specified RADIUS proxy client.

Use the **address-pool** keyword to display the IP address pools configured for a router or for a specific domain. You can also display which IP addresses are available or are in use.

Examples

The following example shows how to display a list of RADIUS proxy clients:

```
Router# show ssg radius-proxy

::::: SSG RADIUS CLIENT TABLE :::::

Client IP       VRF             Device type     Users
10.0.0.2       Global          PDSN            2
10.1.1.1        BLUE            HA              1
```

The following example shows how to display details about the RADIUS proxy client at IP address 172.16.0.0:

```
Router# show ssg radius-proxy 172.16.0.0

::::: SSG RADIUS PROXY LOGON TABLE :::::
User                    SessionID       Host IP          Timer           IP Tech
user1                    12345678        50.0.0.100      None            Simple
user1                    12345679        (no host)        None            Mobile
```

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

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

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

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

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

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

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

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

Inuse Addresses in Domain Pool(ssg.com):10
10.1.5.1
10.1.5.2
10.1.5.3
10.1.5.4
10.1.5.5
10.1.5.6
10.1.5.7
10.1.5.8
10.1.5.9
10.1.5.10
```

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

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

Free Addresses in Domain Pool(ssg.com):20
10.1.5.11
10.1.5.12
10.1.5.13
10.1.5.14
10.1.5.15
10.1.5.16
10.1.5.17
10.1.5.18
10.1.5.19
10.1.5.20
10.1.5.21
10.1.5.22
10.1.5.23
10.1.5.24
10.1.5.25
10.1.5.26
10.1.5.27
10.1.5.28
10.1.5.29
10.1.5.30
```

Table 15 describes significant fields shown in the displays.

Table 15 show ssg radius-proxy Field Descriptions

Field	Description
Client IP	IP address of the client device.
VRF	Name of the VRF associated with a RADIUS proxy client. The value “Global” indicates that the client is not associated with a VRF.
Device type	Type of client device. Device types can be PDSN, HA, or Generic (for non-CDMA2000 devices).
Users	Number of users connected to client device.
User	The user name for the end user.
SessionID	A numeric string derived from the attribute specified as the “Session-Identifier”.
Host IP	IP address of the user.
Timer	Timer type can be “None”, “Wait for IP”, “Hand-off” or “Wait for MSID”.
IP Tech	IP technology: simple or mobile.

Related Commands

Command	Description
debug radius	Displays information associated with RADIUS.
debug ssg ctrl-errors	Displays all error messages for control modules.
debug ssg ctrl-event	Displays all event messages for control modules.
debug ssg ctrl-packet	Displays packet contents handled by control modules.
debug ssg data	Displays all data-path packets.

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
show ssg connection	Displays the connections of a given host and a service name.
show ssg service	Displays the information for a service.

show ssg service

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

To display the information for a Service Selection Gateway (SSG) service, use the **show ssg service** command in privileged EXEC mode.

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

Syntax Description

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

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3) DC	This command was introduced on the Cisco 6400 node route processor.
12.1(1) DC1	The output of this command was modified on the Cisco 6400 node route processor to display the following Service-Info Attributes when they are present in the proxy RADIUS service profile: • Service-Defined Cookie • Full Username Attribute
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(1a)BW	This command was modified to display the attribute filter that is set in the service profile.
12.3(3)B	The modifications in Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B. The output for this command was modified to display information about default DNS redirection.
12.3(7)T	The modifications in Release 12.3(3)B were 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.

Usage Guidelines

Use this command to display connection information for a service.

Examples

L2TP Tunnel Service: Example

The following example shows the information for the L2TP tunnel service called “tunnel1”. The attribute filter that is set in the service profile can be seen in the output.

```
Router# show ssg service tunnel1

------------------------ ServiceInfo Content -----------------------
Uplink IDB:  gw: 0.0.0.0
Name: tunnel1
Type: TUNNEL
Mode: CONCURRENT
Service Session Timeout: 0 seconds
Service Idle Timeout: 0 seconds
Service refresh timeleft: 99 minutes
No Authorization Required
Authentication Type: CHAP
Attribute Filter: 31
Session policing disabled
Reference Count: 1

DNS Server(s):
No Radius server group created. No remote Radius servers.

TunnelId: ssg1
TunnelPassword: cisco
HomeGateway Addresses: 172.0.0.1
ConnectionCount 1
Full User Name not used


Domain List: Included Network Segments:
        0.0.0.0/0.0.0.0

Active Connections:
        1   : RealIP=172.0.1.1, Subscriber=10.0.1.1

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

Proxy Service: Example

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

```
Router# show ssg service serv1-proxy

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

Next Hop Gateway Key:my-key

DNS Server(s):Primary:10.13.1.5
```

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

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


Domain List:service1.com;

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



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

Table 16 describes the significant fields shown in the display.

Table 16 show ssg service Field Descriptions

Field	Description
Uplink IDB	Interface through which the service is reachable.
Name	Service name.
Type	Type of service.
Mode	One of the following values: Concurrent—user can log into this service and other services simultaneously. Sequential—user cannot log into this service simultaneously with other services.
Service Session Timeout	Period of time after which the session (SSG connection) will be terminated.
Service Idle Timeout	If the session (SSG connection) is idle for this many seconds, the session will be terminated.
Service refresh timeleft	Amount of time after which SSG will refresh the service profile.
Authentication Type	Type of authentication that will be used for proxy or tunnel services. Values are PAP and CHAP.
Attribute Filter	RADIUS attribute that is being filtered out from user authentication.
Next Hop Gateway Key	Defines the next-hop binding. Services can be bound to the next hop using next-hop gateways. The key to next-hop-gateway mapping is present in the next-hop profile.
DNS Server(s)	DNS server used for this service.
TunnelId	ID for tunneling services.
TunnelPassword	Password for tunneling services.
HomeGateway Addresses	IP address of the LNS.

Table 16 show ssg service Field Descriptions (continued)

Field	Description
Radius Server: IP authPort acctPort secret	Information about the RADIUS server where proxy users are authenticated for service connectivity.
Included Network Segments	IP address subnets that form the service network.
Excluded Network Segments	IP address subnets that are excluded from the service network.
Full User Name Used	Indicates that the RADIUS authentication and accounting requests use the full username (user@service).
Service Defined Cookie exist	Indicates that user-defined information is included in RADIUS authentication and accounting requests.
Domain List	List of domain names that belong to the service and can be resolved by the DNS server specified for this service.
Active Connections Virtual Subscriber	Lists the host IP address for active connections. The subscriber IP address is the IP address of the host. In cases where there is a service-defined NAT, the virtual IP address is not zero and is the IP address given by the service.

Related Commands

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

show ssg summary

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

To display a summary of the Service Selection Gateway (SSG) configuration, use the **show ssg summary** command in user EXEC or privileged EXEC mode.

show ssg summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

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

Use this command to display information such as which SSG features are enabled, how many users are active, how many services are active, and what filters are active.

Examples

The following example shows the **show ssg summary** command:

```
Router# show ssg summary

SSG Features Enabled:
TCP Redirect: Unauthenticated, Service, Captive portal.
QOS: User policing, Session Policing.
Host Key: Enabled
```

Related Commands

Command	Description
show ssg binding	Displays service names that have been bound to interfaces and the IP addresses to which they have been bound.
show ssg direction	Displays the direction of all interfaces for which a direction has been specified.
show ssg interface	Displays information about SSG interfaces.

show ssg tcp-redirect group

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

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

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

Syntax Description

group-name	(Optional) The previously defined name for the captive portal group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)B	This command was introduced. This command replaced the **show ssg http-redirect group** command.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(1a)BW	This command was modified to display the access lists that are associated with TCP redirection.
12.3(3)B	The modifications in Release 12.3(1a)BW were integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	The modifications in Release 12.3(3)B were 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.

Usage Guidelines

Use this command to display information about the captive portal groups and their associated networks as defined in your system.

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

Examples

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

```
Router# show ssg tcp-redirect group

Current TCP redirect groups:
  SESM1
  SESM2
Default access-list: 101
Default unauthenticated user redirect group: None Set
Default service redirect group: None Set
```

```
Prepaid user default redirect group: None Set
SMTP forwarding group: None Set
Default initial captivation group: None Set
Default advertising  captivation group: None Set
```

Table 17 describes the significant fields shown in the display.

Table 17 show ssg tcp-redirect group Field Descriptions

Field	Description
Current TCP redirect groups	List of all TCP-redirect groups.
Default access-list	Name of the default access-list.
Default unauthenticated user redirect group	Name of the captivation group to which unauthenticated users are redirected.
Default service redirect group	Default service redirect group.
Prepaid user default redirect group	Name of the captivation group to which prepaid users are redirected.
SMTP forwarding group	SMTP redirection settings.
Default initial captivation group	Name of the default initial captivation group and duration of captivation.
Default advertising captivation group	Name of the default advertising captivation group and duration and frequency of advertising captivation.

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

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

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

Table 18 describes the significant fields shown in the display.

Table 18 show ssg tcp-redirect group group-name Field Descriptions

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

Related Commands

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

show ssg user transparent

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

To display a list of all the Service Selection Gateway (SSG) transparent autologon users, use the **show ssg user transparent** command in privileged EXEC mode.

show ssg user transparent

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use this command to display the IP addresses and the states of all transparent autologon users that are active on SSG. The transparent autologon user states are passthrough (TP), suspect (SP), unidentified (NR), and waiting for authorization (WA).

Examples

The following is sample output from the **show ssg user transparent** command:

```
Router# show ssg user transparent

10.10.10.10      Passthrough
10.11.11.11      Suspect
10.120.120.120  Authorizing

### Total number of transparent users: 3
```

Related Commands

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

show ssg user transparent authorizing

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

To display a list of all Service Selection Gateway (SSG) transparent autologon users for whom authorization is in progress and who are waiting for authentication, authorization, and accounting (AAA) server response, use the **show ssg user transparent authorizing** command in privileged EXEC mode.

show ssg user transparent authorizing [**count**]

Syntax Description

count	(Optional) Displays the number of authorizing users.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use this command to display all SSG transparent autologon users that are waiting for authorization (WA).

Examples

The following is sample output from the **show ssg user transparent authorizing** command with the **count** keyword:

```
Router# show ssg user transparent authorizing count

### Total number of WA users : 1
```

Related Commands

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

show ssg user transparent passthrough

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

To display information about Service Selection Gateway (SSG) transparent autologon pass-through users, use the **show ssg user transparent passthrough** command in privileged EXEC mode.

show ssg user transparent passthrough [*ip-address* | **count**]

Syntax Description

ip-address	(Optional) Display details for specified user IP address.
count	(Optional) Displays the number of pass-through users.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use this command to display all SSG transparent autologon pass-through (TP) users that are active on SSG.

Examples

The following is sample output from the **show ssg user transparent passthrough** command for the user having IP address 10.10.10.10:

```
Router# show ssg user transparent passthrough 10.10.10.10

User IP Address :       10.10.10.10
Session Timeout :       200 (seconds)
Idle Timeout :          100 (seconds)

User logged on since : *16:33:57.000 GMT Mon May 19 2003
User last activity at : *16:33:57.000 GMT Mon May 19 2003

Current Time : *16:35:17.000 GMT Mon May 19 2003
```

Related Commands

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

show ssg user transparent suspect

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

To display a list of all Service Selection Gateway (SSG) transparent autologon suspect (SP) user IP addresses, use the **show ssg user transparent suspect** command in privileged EXEC mode.

show ssg user transparent suspect [**count**]

Syntax Description

count	(Optional) Displays the number of suspect users.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

An SSG transparent autologon suspect user is a user whose authentication, authorization, and accounting (AAA) authorization resulted in an Access Reject.

Examples

The following is sample output from the **show ssg user transparent suspect** command with and without the **count** keyword:

```
Router# show ssg user transparent suspect count

### Total number of SP users : 1

Router# show ssg user transparent suspect

        10.0.0.1


### Total number of SP users : 1

Router#
```

Related Commands

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

show ssg user transparent unidentified

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

display a list of Service Selection Gateway (SSG) transparent autologon users for whom there is no response from the authentication, authorization, and accounting (AAA) server to an authorization request (unidentified users), use the **show ssg user transparent unidentified** command in privileged EXEC mode.

show ssg user transparent unidentified [**count**]

Syntax Description

count	(Optional) Displays the number of unidentified (NR) users.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use this command to display all SSG transparent autologon unidentified (NR) users that are active on the SSG.

Examples

The following is sample output from the **show ssg user transparent unidentified** command with and without the **count** keyword:

```
Router# show ssg user transparent unidentified count

### Total number of NR (Unidentified) users : 1

Router# show ssg user transparent unidentified

        10.0.0.2


### Total number of NR (Unidentified) users : 1

Router#
```

Related Commands

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

show ssg vc-service-map

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

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
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 display VC-to-service-name mappings.

Examples

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

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

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

Related Commands

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

source ip

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

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

source ip {*ip-address* | *interface*}

no 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

SSG portmap configuration

Command History

Release	Modification
12.2(16)B	This command was introduced. This command replaces the **ssg port-map source ip** command.
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

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 **source ip** command must be routable in the management network where the Cisco Service Selection Dashboard (SSD) or Subscriber Edge Services Manager (SESM) resides.

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

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

Examples

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

```
ssg port-map
 source ip 10.0.50.1
 source ip Ethernet 0/0/0
 ssg port-map source ip Loopback 1
```

Related Commands

Command	Description
length (SSG)	Modifies the port-bundle length upon the next SSG reload.
ssg port-map	Enables the SSG port-bundle host key and enters SSG portmap configuration mode.

ssg aaa group prepaid

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

To specify the server group to be used for Service Selection Gateway (SSG) prepaid authorization, use the **ssg aaa group prepaid** command in global configuration mode. To remove this specification, use the **no** form of this command.

ssg aaa group prepaid *server-group*

no ssg aaa group prepaid *server-group*

Syntax Description

server-group	Name of the server group to be used for SSG prepaid authorization.

Command Default

If a server group is not specified by using the **ssg aaa group prepaid** command, the default RADIUS server configured on the router will be used for SSG prepaid authorization.

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

The **ssg aaa group prepaid** command allows you to configure a global server for SSG prepaid authorization. Configure the global server group by using the **aaa group server radius** command. Use the **ssg aaa group prepaid** command to attach the server group to SSG for SSG prepaid authorization.

Examples

The following example shows how to configure a global SSG prepaid authorization server:

```
aaa group server radius ssg_prepaid
 server 10.2.3.4 auth-port 1645 acct-port 1646
.
.
.
ssg aaa group prepaid ssg_prepaid
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.

ssg accounting

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

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

ssg accounting [**per-host**] [**per-service**] [**interva**l *seconds*] [{**stop rate-limit** *records*}]

no ssg accounting [**per-host**] [**per-service**] [**interval** *seconds*] [{**stop rate-limit** *records*}]

Syntax Description

per-host	(Optional) Enables the sending of per-host accounting records only.
per-service	(Optional) Enables the sending of per-service accounting records only.
interval	(Optional) Specifies the interval at which accounting updates are sent to the accounting server.
seconds	(Optional) Number of seconds after which an accounting update will be sent to the accounting server. The range is from 60 to 2,147,483,647 seconds, in increments of 60 seconds. The value entered will be rounded up to the next multiple of 60. Default is 600.
stop	(Optional) Enables rate-limiting of SSG accounting records.
rate-limit	(Optional) Specifies the number of accounting records sent per second.
records	(Optional) Number of accounting stop records sent per second. The range is from 10 to 5000.

Command Default

Accounting is enabled.
The interval is set at 600 seconds.

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.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(16)B	The **per-host** and **per-service** keywords were added.
12.3(4)T	The **per-host** and **per-service** keywords were integrated into Cisco IOS Release 12.3(4)T.
12.3(14)T	The stop and rate-limit keywords and the records argument were integrated into Cisco IOS Release 12.3(14)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 accounting** command enables the sending of start, stop, and interim accounting records for hosts and connections.

Examples

The following example shows how to enable the sending of per-host SSG accounting records at intervals of 60 seconds:

```
ssg accounting per-host interval 60
```

ssg attribute 44 suffix host ip

Note Effective with Cisco IOS Release 15.0(1)M, the **ssg attribute 44 suffix host ip** command is not available in Cisco IOS software.

To enable the appending of a client IP address to an accounting session ID to create a unique SSG accounting session ID, use the **ssg attribute 44 suffix host ip** command in global configuration mode. To disable the appending of the IP address, use the **no** form of this command.

ssg attribute 44 suffix host ip

no ssg attribute 44 suffix host ip

Syntax Description

This command has no arguments or keywords.

Command Default

SSG does not append the client IP address to the accounting session ID.

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

Use the **ssg attribute 44 suffix host ip** command to create a unique session ID by appending the client's IP address to the RADIUS accounting session number (acct-session-id). This functionality applies to accounting packets generated by SSG for host accounting or connection accounting records.

Examples

The following example enables the SSG unique session ID:

```
ssg attribute 44 suffix host ip
```

Related Commands

Command	Description
ssg accounting	Enables SSG accounting.

ssg auto-domain

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

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

ssg auto-domain

no ssg auto-domain

Syntax Description

This command has no arguments or keywords.

Command Default

Autodomain is disabled 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

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

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

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

Examples

The following example enables basic SSG Autodomain:

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

Related Commands

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

ssg auto-logoff arp

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

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

ssg auto-logoff arp [**match-mac-address**] [**interval** *seconds*]

no ssg auto-logoff arp

Syntax Description

match-mac-address	(Optional) Configures SSG to check the MAC address of a host each time that host performs an ARP ping.
interval *seconds*	(Optional) ARP ping interval, in seconds. The interval specified is rounded to the nearest multiple of 30. An interval of less than 30 is rounded up to 30 seconds. The default interval is 30 seconds.

Command Default

SSG autologoff is not enabled by default.
The default ARP ping interval is 30 seconds.

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.
12.2(15)B	The **match-mac-address** keyword was added.
12.3(4)T	The **match-mac-address** 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 the **ssg auto-logoff arp** command to configure SSG to use the ARP ping mechanism to detect connectivity to hosts. Use the optional **match-mac-address** keyword to configure SSG to check the MAC address of a host each time that host performs an ARP ping. If the SSG finds that the MAC address of the host has changed, SSG automatically initiates the logoff of that host.

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

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

ICMP ping can be used in all types of deployments. Refer to the **ssg auto-logoff icmp** command reference page for more information about SSG autologoff using ICMP ping.

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

ARP ping does not support overlapping IP addresses.

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

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

Examples

The following example shows how to enable SSG autologoff and to configure SSG to use ARP ping to detect connectivity to hosts:

```
ssg auto-logoff arp interval 60
```

The following example shows how to enable SSG MAC address checking for autologoff:

```
ssg auto-logoff arp match-mac-address
```

The following example shows how to enable SSG MAC address checking for autologoff and to specify an ARP ping interval of 60 seconds:

```
ssg auto-logoff arp match-mac-address interval 60
```

Related Commands

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

ssg auto-logoff icmp

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

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

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

no auto-logoff icmp

Syntax Description

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

Command Default

SSG autologoff is not enabled.

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

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

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

ICMP ping supports overlapping IP addresses.

If a user is not reachable, a configured number of packets (*p*) will be sent, and each packet will be timed out (*t*). The user will be logged off in *p* * *t* milliseconds after the first pinging attempt. If *p* * *t* milliseconds is greater than the configured pinging interval, then the time taken to log off the host after

connectivity is lost will be greater than the configured autologoff interval. If parameters are configured this way, the following warning will be issued: "Hosts will be auto-logged off (*p* * *t*) msecs after connectivity is lost." When the pinging interval is less than *p* * *t*, the timeout process for a host that has become unreachable will be invoked when the pinging to that host is still occurring. However, because the timeout process will check the status of the host object and find that it is in a pinging state, the host will not be pinged again.

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

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

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

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

Examples

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

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

Related Commands

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

ssg bind direction

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

Note Effective with Cisco IOS Release 12.2(16)B, this command was replaced by the **ssg direction** command. The **ssg bind direction** command is still supported for backward compatibility, but support for this command may be removed in a future Cisco IOS release.

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

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

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

Syntax Description

downlink	Specifies interface direction as downlink.
uplink	Specifies interface direction as uplink.
ATM	Indicates that the interface is ATM.
atm-interface	ATM interface.
Async	Indicates that the interface is asynchronous.
async-interface	Async interface.
BVI	Indicates that the interface is BVI.
bvi-interface	Bridge-Group Virtual Interface.
Dialer	Indicates that the interface is dialer.
dialer-interface	Dialer interface.
Ethernet	Indicates that the interface is IEEE 802.3 Ethernet.
ethernet-interface	Ethernet interface.
FastEthernet	Indicates that the interface is IEEE 802.3 Fast Ethernet.
fastethernet-interface	Fast Ethernet interface.
Group-Async	Indicates that the interface is group async.

group-async-interface	Group async interface.
Lex	Indicates that the interface is lex.
lex-interface	Lex interface.
Loopback	Indicates that the interface is loopback.
loopback-interface	Loopback interface.
Multilink	Indicates that the interface is multilink.
multilink-interface	Multilink interface.
Null	Indicates that the interface is null.
null-interface	Null interface.
Port-channel	Indicates that the interface is port channel.
port-channel-interface	Port channel interface.
Tunnel	Indicates that the interface is tunnel.
tunnel-interface	Tunnel interface.
Virtual-Access	Indicates that the interface is virtual access.
virtual-access-interface	Virtual access interface.
Virtual-Template	Indicates that the interface is virtual template.
virtual-template-interface	Virtual template interface.
Virtual-TokenRing	Indicates that the interface is virtual token ring.
virtual-tokenring-interface	Virtual token ring interface.

Command Default

All interfaces are configured as uplink interfaces by default.

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.
12.2(16)B	This command was replaced by the **ssg direction** command.
12.3(4)T	This command was replaced by the **ssg direction** command.
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 an interface as downlink or uplink. An uplink interface is an interface to services; a downlink interface is an interface to subscribers.

Examples

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

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

Related Commands

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

ssg bind service

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

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

ssg bind service *service-name* {*ip-address* | *interface-type interface-number*} [*distance-metric*]

no ssg bind service *service-name* {*ip-address* | *interface-type interface-number*} [*distance-metric*]

Syntax Description

service-name	Service name.
ip-address	IP address of the next-hop router.
interface-type	Type of interface.
interface-number	Number of the interface.
distance-metric	(Optional) Metric to be used to determine the path for upstream traffic. The range is from 1 to 255. Default is 0.

Command Default

A service is not bound to an interface.

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.
12.3(8)T	This command was modified to enable the configuration of interface redundancy for a service, and the *distance-metric* argument 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 bind a service to an interface. You can enter this command more than once in order to bind a service to more than one interface for interface redundancy.

Use the *distance-metric* argument to control the routing of upstream traffic. If more than one entry of the **ssg bind service** command for a service have the same metric, the upstream traffic will be load-balanced.

If a service is configured for multiple uplink interfaces, downstream traffic will be allowed on all the interfaces for any service bound to even one of those interfaces.

Examples

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

```
ssg bind service MyService ATM 0/0/0.10
```

The following example shows uplink interface redundancy configured for the service “sample-service”. ATM interface 1/0.1 is configured as the primary interface and ATM interface 1/0.2 as the secondary interface.

```
ssg bind service sample-service atm 1/0.1
ssg bind service sample-service atm 1/0.2 100
```

Related Commands

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