



Implementing SSG: Initial Tasks

First Published: May 2, 2005
Last Updated: October 2, 2009



Note

Effective with Cisco IOS Release 15.0(1)M, this feature is not available in Cisco IOS software.

This document describes the initial tasks you need to perform to enable SSG on the router and to establish SSG communication with other key components of the network, including Subscriber Edge Services Manager (SESM) and the authentication, authorization, and accounting (AAA) server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Implementing SSG” section on page 26](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Implementing SSG, page 2](#)
- [Restrictions for Implementing SSG, page 2](#)
- [How to Establish Initial SSG Communication, page 2](#)
- [Configuration Examples for Establishing Initial SSG Communication, page 20](#)
- [Additional References, page 24](#)
- [Feature Information for Implementing SSG, page 26](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Implementing SSG

Knowledge

Before configuring SSG, you should understand the concepts in [Overview of SSG](#).

Interfaces

SSG is supported on all logical and physical interfaces on which Cisco Express Forwarding (CEF) switching is supported. This includes physical interfaces such as ATM, Ethernet, and Packet-over-SONET (POS), and logical interfaces such as GRE, 802.1q virtual LANs, and Point-to-Point Protocol (PPPoX).

CEF Switching

IP CEF must be enabled globally before SSG will work.

Cisco Subscriber Edge Services Manager

If you want to perform Layer 3 service selection, you must install and configure Cisco SESM as described in the [Cisco Subscriber Edge Services Manager Administration and Configuration Guide](#).

AAA or LDAP

An authentication, authorization, and accounting (AAA) RADIUS server or LDAP server are typically used to authenticate subscribers and to store subscriber and service profiles.

Restrictions for Implementing SSG

SSG does not process IP multicast packets. IP multicast packets will be handled by Cisco IOS software in the traditional way.

How to Establish Initial SSG Communication

To enable SSG and establish SSG communication with other network devices, perform the tasks in the following sections:

- [Enabling SSG, page 3](#)
- [System Resource Cleanup When SSG Is Unconfigured, page 3](#)
- [Configuring the Default Network, page 10](#)
- Configuring SSG Communication with SESM:
 - [Configuring SSG-SESM API Communication, page 11](#)
 - [Configuring SSG Port-Bundle Host-Key Functionality, page 12](#)
- [Configuring SSG to AAA Server Interaction, page 17](#)
- [Troubleshooting Initial SSG Communication, page 20](#)

Enabling SSG

Perform this task to enter global configuration and enable SSG on the router.



Note

This task must be performed before any other SSG functionality can be configured.

SSG and Cisco Express Forwarding

SSG works with CEF switching technology to provide maximum Layer 3 switching performance. Because CEF is topology-driven rather than traffic-driven, its performance is unaffected by network size or dynamics. CEF must be enabled for SSG to work.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **ssg enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip cef Example: Router(config)ip cef	Enables global IP CEF.
Step 4	ssg enable Example: Router(config)# ssg enable	Enables SSG.

System Resource Cleanup When SSG Is Unconfigured

When you enable SSG, the SSG subsystem in Cisco IOS software acquires system resources that are never released unless the router is rebooted. To release and clean up system resources acquired by SSG, use the **no ssg enable force-cleanup** command.

Configuring SSG Interface Direction

Before you can configure SSG interfaces, you need to understand the following concepts:

- [Interface Direction, page 4](#)
- [Uplink Interface Redundancy Overview, page 4](#)
- [Downlink Interface Redundancy Overview, page 5](#)
- [SSG Uplink Interface Redundancy Topologies, page 5](#)
- [Restrictions, page 7](#)

Perform the following tasks to configure SSG interfaces:

- [Setting SSG Interface Direction for an Individual Interface, page 7](#)
- [Setting the Direction on an ATM Subinterface \(with PVC or PVC Range\), page 8](#)
- [Verifying SSG Interface Binding, page 9](#)

Interface Direction

SSG implements service selection through selective routing of IP packets to destination networks on a per-subscriber basis. SSG uses the concept of interface direction (uplink or downlink) to help determine the forwarding path of incoming packets. An uplink interface is an interface towards the services; a downlink interface is an interface towards the subscribers. You can configure interface direction for a single interface or a range of subinterfaces at once.

Uplink Interface Redundancy Overview

In SSG, each service is associated with an uplink interface, configured by binding the service to the next-hop or to an interface. When a subscriber chooses to use a service, SSG connects the subscriber to the service through the associated uplink interface. SSG interface redundancy allows services to be associated with more than one interface to protect against link failures.

When redundant interfaces are configured for a service, the distance metric assigned to the service binding is used to determine the order in which SSG selects the interface to be used to reach a service. The interface for the service binding with the lowest metric is the primary interface. The interface for the service binding with the second-lowest weight is the secondary interface, and so on.

If a failure occurs on an active interface, SSG recognizes the failure and switches the traffic to the interface associated with the next-lowest metric. When the primary uplink interface or next hop becomes available again, SSG switches traffic back to the primary interface.



Note

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

If a host has a connection that uses NAT to one of the services on a set of redundant uplink interfaces, all traffic from a user to any of the uplink interfaces uses NAT.

SSG interface redundancy can be configured for pass-through and proxy services, including open garden services, walled garden services, and the default network. This feature is supported on all physical and logical interfaces that SSG supports.

SSG uplink interface redundancy is configured by binding a service to more than one interface or next hop and grouping the redundant interfaces to ensure that SSG treats them similarly. See the “Configuring Services for Subscribers” module for information about how to bind services. To group redundant uplink interfaces, see the “Setting SSG Interface Direction for an Individual Interface” section on page 7

Downlink Interface Redundancy Overview

Subscriber traffic can be received by SSG on any of the downlink configured interfaces, which allows for downlink interface redundancy.

The SSG Downlink Interface Redundancy feature can be configured with or without the Port-Bundle Host-Key (PBHK) feature. When PBHK is disabled, downlink interface redundancy is the default behavior. When PBHK is enabled, you must disable SSG’s support of overlapping host IP addresses with the **no host overlap** command. For more information on configuring PBHK, see the “Configuring SSG Port-Bundle Host-Key Functionality” section on page 12.

SSG Uplink Interface Redundancy Topologies

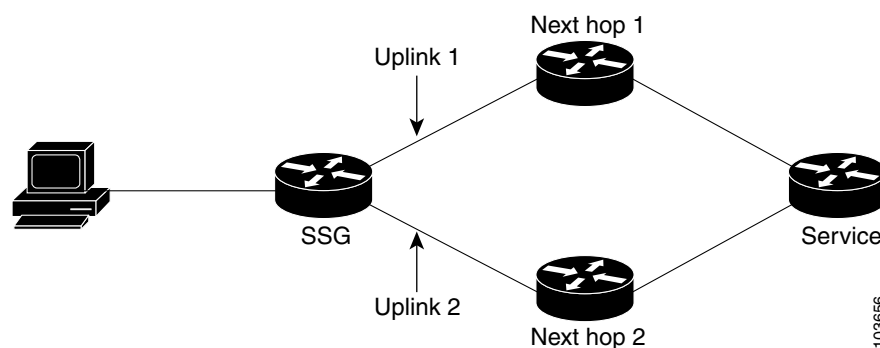
The SSG Interface Redundancy feature supports uplink interface redundancy in the following network topologies:

- [Multiple Next Hops per Service, page 5](#)
- [Multiple Uplink Interfaces with a Single Next Hop, page 6](#)
- [Multiple Uplink Interfaces with No Next Hop, page 6](#)
- [Combination of Directly Connected Uplink Interfaces and Interfaces with Next Hops, page 6](#)

Multiple Next Hops per Service

Figure 1 shows an example of SSG interface redundancy configured to support multiple next-hop IP addresses per service. In this type of topology, each next hop is routable on a different uplink interface. SSG forwards traffic to the appropriate next hop on the basis of the distance metric assigned to it.

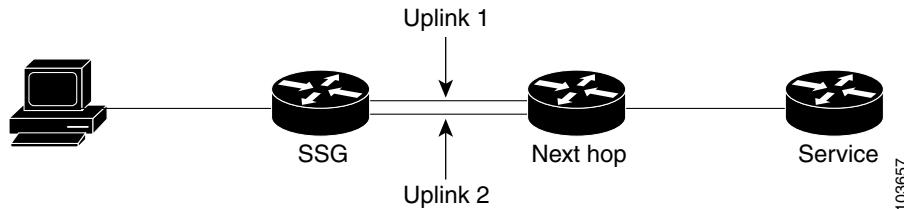
Figure 1 *Multiple Next Hops per Service: Sample Topology*



Multiple Uplink Interfaces with a Single Next Hop

Figure 2 shows an example of SSG interface redundancy configured to support multiple uplink interfaces that share a single next hop. In this type of topology, routing to the service is governed by the active route to the next-hop IP address, as dictated by the global routing table.

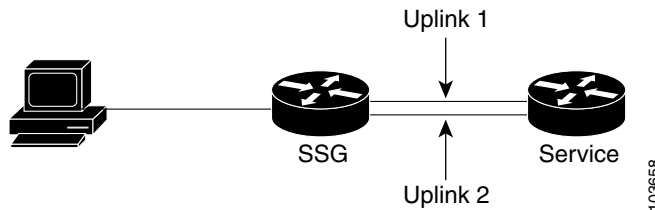
Figure 2 *Multiple Uplink Interfaces with a Single Next Hop: Sample Topology*



Multiple Uplink Interfaces with No Next Hop

Figure 3 shows an example of SSG interface redundancy configured to support multiple uplink interfaces that are directly connected to the service.

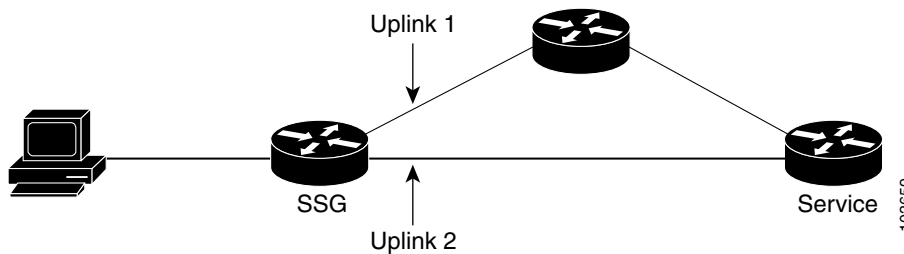
Figure 3 *Multiple Uplink Interfaces with No Next Hop: Sample Topology*



Combination of Directly Connected Uplink Interfaces and Interfaces with Next Hops

Figure 4 shows an example of SSG interface redundancy configured to support an uplink interface that is directly connected to the service and an uplink interfaces with a next hop.

Figure 4 *Combination of Directly Connected Uplink Interfaces and Interfaces with Next Hops: Sample Topology*



Restrictions

When you configure a range of ATM permanent virtual circuits (PVCs) using the **range** command, you cannot use the **ssg direction** command on an individual subinterface. All members of a range must have the same direction.

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

Before you can change a direction from uplink to downlink, or the opposite, you must use the **no ssg direction** command to clear the direction. If you do not, you will receive an error message similar to the following:

```
Changing direction from Downlink to Uplink is denied for interface interface
Please use 'no ssg direction downlink' to clear the previous bind direction
```

Setting SSG Interface Direction for an Individual Interface

Perform this task to configure interface direction for an individual interface.

SUMMARY STEPS

1. **interface** *type number*
2. **ssg direction** {**downlink** | **uplink** [**member** *group-name*]}
3. **exit**
4. Repeat steps 1 to 3 for each interface for which you want to configure direction.

DETAILED STEPS

	Command or Action	Purpose
Step 1	interface <i>type number</i> Example: Router(config)# interface FastEthernet 1/0	Specifies an interface and enters interface configuration mode.
Step 2	ssg direction { downlink uplink [member <i>group-name</i>]} Example: Router(config-if)# ssg direction downlink	Sets the direction of the interface. <ul style="list-style-type: none"> • An uplink interface is an interface to services; a downlink interface is an interface to subscribers. • The member option specifies that the interface is a member of a group of uplink interfaces that reach the same service. Use this option to group redundant uplink interfaces and to configure SSG to treat redundant uplink interfaces similarly.
Step 3	exit Example: Router(config-if)# exit	(Optional) Exits to global configuration mode.
Step 4	Repeat steps 1 to 3 for each interface for which you want to configure direction.	

Setting the Direction on an ATM Subinterface (with PVC or PVC Range)

Uplink or downlink direction can be set on ATM subinterfaces (both point-to-point and multipoint) similar to any other interface (as explained in [Setting SSG Interface Direction for an Individual Interface, page 7](#)). However, if the point-to-point ATM subinterface contains a PVC range, this will result in several ATM subinterfaces getting created implicitly, as explained in the guide: *ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping*. In this case, all ATM subinterfaces in this PVC range will inherit the same SSG bind direction.

Perform this task to configure a range of subinterfaces as uplink or downlink. An uplink interface is an interface to services; a downlink interface is an interface to subscribers.

Restrictions

All subinterfaces in a range must have the same direction. If you try to specify the direction of an interface that is part of a PVC range, you receive an error similar to the following:

```
PVC Range: Configuring interface is not allowed.
```

SUMMARY STEPS

1. **interface atm** *interface-number.subinterface-number* { **mpls** | **multipoint** | **point-to-point** }
2. **ssg direction** { **downlink** | **uplink** [**member group-name**] }
3. **pvc vpi/vci**
or
4. **range** [*range-name*] **pvc** *start-vpi/start-vci end-vpi/end-vci*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>interface atm <i>interface-number.subinterface-number</i> { mpls multipoint point-to-point }</pre> <p>Example: Router(config)# interface ATM 1/0.1 point-to-point</p>	Specifies a subinterface and enters subinterface configuration mode.
Step 2	<pre>ssg direction { downlink uplink [member <i>group-name</i>] }</pre> <p>Example: Router(config-subif)# ssg direction downlink</p>	Sets the direction of the subinterfaces. <ul style="list-style-type: none"> • An uplink interface is an interface to services; a downlink interface is an interface to subscribers.

	Command or Action	Purpose
Step 3	<p>pvc vpi/vci</p> <p>Example: Router(config-subif)# pvc 1/32</p>	<p>Defines a PVC</p> <ul style="list-style-type: none"> Use this command to define the permanent virtual connection (PVC).
Step 4	<p>range [range-name] pvc start-vpi/start-vci end-vpi/end-vci</p> <p>Example: Router(config-subif)# range MyRange pvc 1/32 1/42</p>	<p>Defines a PVC range.</p> <ul style="list-style-type: none"> Use this command if a range was not already defined. You can also use this command after the ssg direction command, with the same effect.

Verifying SSG Interface Binding

Perform this task to verify the binding of SSG interfaces.

SUMMARY STEPS

1. **show ssg interface [brief] [interface-type interface-number]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>show ssg interface [brief] [interface-type interface-number]</p> <p>Example: Router# show ssg interface brief</p>	<p>Displays information about SSG interfaces.</p>

Example

The following examples of output for the **show ssg interface** command show information about SSG interface binding:

```
Router# show ssg interface

Interface: Ethernet1/1
Bind Direction: Downlink
Binding Type: Static

Interface: ATM4/0.40
Bind Direction: Downlink
Binding Type: Static

Interface: ATM4/0.140
Bind Direction: Uplink
Binding Type: Static
Services bound: NONE
```

```
Router# show ssg interface brief

Interface      Direction  Binding Type
Ethernet1/1    Downlink   Static
ATM4/0.40      Downlink   Static
ATM4/0.140     Uplink     Static
```

Configuring the Default Network

SSG allows all users, even unauthenticated users, to access the default network. Typically, SESM belongs to the default network. However, other types of servers, such as DNS/DHCP servers or TCP-Redirect servers, can also be part of the default network. Perform this task to specify an IP address or an IP subnet as the default network.

Processing of Default Network Traffic

Traffic to and from the default network requires special processing by SSG. This is because traffic to and from SESM (Captive Portal and NWSP) requires special processing, and SSG cannot distinguish between SESM and non-SESM traffic. To reduce processing overhead for SSG, we recommend that you define the SESM server as the default network and place other servers in the Open Garden network.



Note

On SSG platforms that support PXF forwarding engine, SSG typically forwards packets to and from the default network through the router's PXF forwarding engine. However, SSG also forwards default network traffic through the route processor (RP) as follows:

Packets from a User and Destined for the Default Network

If the port-bundle host-key is:

- Enabled—SSG forwards the packets through the RP.
- Disabled—SSG forwards the packets through the PXF forwarding engine.

Packets from the Default Network and Destined for an SSG User

SSG forwards the packets through the RP if either of the following conditions are met:

- The port-bundle host-key is enabled.
- The port-bundle host-key is disabled, TCP is the transport protocol, and the packets are associated with an active TCP redirect mapping.

Otherwise, SSG forwards the packets through the PXF forwarding engine.

SUMMARY STEPS

1. `ssg default-network ip-address mask`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>ssg default-network <i>ip-address mask</i></p> <p>Example: Router(config) ssg default-network 10.10.1.2 255.255.255.255</p>	<p>Sets the IP address or subnet that users are able to access without authentication.</p> <ul style="list-style-type: none"> Typically, this is the address where the Cisco SESM resides. A mask provided with the IP address specifies the range of IP addresses that users are able to access without authentication.

Configuring SSG-SESM API Communication

To support subscriber login, subscriber logout, and service selection, SSG acts as a server listening for RADIUS-based SESM commands. Perform this task to establish communication between SSG and SESM.

SUMMARY STEPS

- ssg radius-helper key**
- ssg radius-helper [auth-port *UDP-port-number*] [acct-port *UDP-port-number*]**
- ssg radius-helper [access-list]**
- ssg radius-helper [validate]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>ssg radius-helper key</p> <p>Example: Router(config)# ssg radius-helper key MyKey</p>	<p>Sets the shared secret key between SSG and SESM.</p>
Step 2	<p>ssg radius-helper [auth-port <i>UDP-port-number</i>] [acct-port <i>UDP-port-number</i>]</p> <p>Example: Router(config)# ssg radius-helper [auth-port 1645] [acct-port 1646]</p>	<p>Specifies the port on which SSG will listen for SESM commands (SSG is the server). The default port number for authentication packets is 1645, and the default port number for accounting packets is 1646.</p>
Step 3	<p>ssg radius-helper access-list</p> <p>Example: Router(config)# ssg radius-helper [access-list]</p>	<p>(Optional) Specifies the access list to be applied to traffic from SESM.</p>
Step 4	<p>ssg radius-helper validate</p> <p>Example: Router(config)# ssg radius-helper validate</p>	<p>(Optional) Enables the validation of SESM IP addresses.</p> <ul style="list-style-type: none"> SSG will only accept commands from validated IP addresses.

Configuring SSG Port-Bundle Host-Key Functionality

Before you configure the SSG Port-Bundle Host-Key (PBHK) feature, you should understand the following concepts:

- [Port-Bundle Host-Key Mechanism, page 12](#)
- [Port-Bundle Length, page 13](#)
- [Benefits of SSG Port-Bundle Host-Key, page 14](#)
- [Prerequisites for SSG Port-Bundle Host-Key, page 14](#)
- [Restrictions for SSG Port-Bundle Host-Key, page 14](#)

Perform the following tasks to configure SSG Port-Bundle Host-Key functionality

- [Configuring the SSG Port-Bundle Host-Key, page 15](#) (required)
- [Verifying SSG Port-Bundle Host-Key Configuration, page 16](#) (optional)

Port-Bundle Host-Key Mechanism

When the SSG Port-Bundle Host-Key feature is enabled, SSG performs port-address translation (PAT) and network-address translation (NAT) on the HTTP traffic between the subscriber and the SESM server. The operation of changing the subscriber's IP address and port is commonly known as a port-map operation, and the mappings between the original and changed IP address and port are known as port-mappings.

When a subscriber sends traffic to the SESM server, SSG creates a port map that changes the source IP address to a configured SSG source IP address and the source TCP port to a port allocated by SSG. SSG assigns a range of ports, known as a port-bundle, to each subscriber because one subscriber can have several simultaneous TCP sessions when accessing a web page. The assigned *host-key*, or combination of SSG source IP address and port-bundle, uniquely identifies each subscriber.

When the Port-Bundle Host-Key feature is not enabled, the subscriber is uniquely identified by their IP address. When the SESM server sends a reply to the subscriber, SSG translates the destination IP address and TCP port to the subscriber's actual IP address.

The host-key is carried in RADIUS packets sent between the SESM server and SSG in the Subscriber IP vendor-specific attribute (VSA), and uniquely identifies the subscriber. [Table 1](#) describes the Subscriber IP VSA. When the SESM server sends a reply to the subscriber, SSG translates the destination IP address and destination TCP port according to the port map.

Table 1 *Subscriber IP VSA Description*

Attr ID	Vendor ID	Sub Attr ID and Type	Attr Name	Sub Attr Data
26	9	250 Account-Info	Subscriber IP	S<subscriber-ip-address>[:<port-bundle-number>]] <ul style="list-style-type: none"> • S—Account-Info code for subscriber IP. • <subscriber IP address>:<port-bundle number>—The port-bundle number is only used if the SSG Port-Bundle Host-Key feature is configured.

For each new subscriber, SSG assigns a new port-bundle. The number of port-bundles is limited, but you can assign multiple SSG source IP addresses to accommodate more subscribers. If the subscriber logs in, SSG maintains the port-bundles as long as the host is active. If the subscriber does not log in, SSG will recycle the port-bundle after a period of inactivity.

For each new TCP session between a subscriber and the SESM server, SSG uses one port from the port bundle for the port mapping. Port mappings are flagged as eligible for reuse on the basis of inactivity timers, but are not explicitly removed once assigned. The number of port bundles is limited, but you can assign multiple SSG source IP addresses to accommodate more subscribers.

Port-Bundle Length

The port-bundle length determines the number of ports that are assigned to one subscriber (number-of-ports = $2^{\text{port-bundle length}}$). By default, the port-bundle length is 4 bits, which yields 16 ports available for each subscriber. The maximum port-bundle length is 10 bits, which would support 1024 concurrent sessions to SESM. See [Table 2](#) for available port-bundle length values, the number of ports-per-bundle, and the number of bundles-per-IP address. Increasing the port-bundle length can be useful when you see frequent error messages about running out of ports in a port bundle.

Table 2 *Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values*

Port-Bundle Length (in bits)	Number of Ports per Bundle	Number of Bundles per Group (and per SSG Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63



Note

For each SESM server, all connected SSGs must have the same port-bundle length, which must correspond to the configured value given in the SESM server's BUNDLE_LENGTH argument. If you change the port-bundle length on an SSG, be sure to make the corresponding change in the SESM configuration.

Benefits of SSG Port-Bundle Host-Key

Scalable with Multiple Subscriber Subnets

Without the SSG Port-Bundle Host-Key feature, SESM must be provisioned for a static mapping between subscriber subnets and SSG IP addresses. The SSG Port-Bundle Host-Key feature eliminates the need for static mapping because the host-key contains the SSG's IP address, which SESM uses to identify which SSG is servicing the subscriber.

Reliable and Just-in-Time Notification to Cisco SSD of Subscriber State Changes

Without the SSG Port-Bundle Host-Key feature, SSG uses an asynchronous messaging mechanism to immediately notify the SESM server of subscriber state changes in SSG (such as session timeouts or idle timeout events).

The SSG Port-Bundle Host-Key feature replaces the asynchronous messaging mechanism with an implicit and reliable notification mechanism that uses the base port of a port bundle to alert the SESM server of a state change. The SESM server can then query SSG for the true state of the subscriber and update the cached object or send the information back to the subscriber.

Support for Overlapped PPP Subscribers

With the SSG Port-Bundle Host-Key feature, PPP users can have overlapped IP addresses while using SESM for service selection.

Prerequisites for SSG Port-Bundle Host-Key

The SSG Port-Bundle Host-Key feature requires Cisco SESM Release 3.1(1) or higher.

A default network must be configured and routable from SSG in order to configure the Port-Bundle Host-Key commands:



Note

SSG source IP addresses configured with the **source ip** command must be routable by SESM. This is the IP addresses that SESM will receive for subscriber traffic.

Restrictions for SSG Port-Bundle Host-Key

The SSG Port-Bundle Host-Key feature has the following restrictions:

- The SSG Port-Bundle Host-Key feature must be enabled on all SSGs connected to SESM. The port-bundle length should also be the same on all SSGs and SESM.
- The SSG Port-Bundle Host-Key feature can be enabled or disabled only when there are no active SSG host objects present.
- The port-bundle length can only be changed when there are no active SSG host objects present.
- Overlapping subscriber IP addresses are supported only for hosts reachable via routed point-to-point interfaces.
- Overlapping IP users cannot be connected to the same service or to different services that are bound to the same uplink interface or interface group.
- For each SESM server, all connected SSGs must have the same port-bundle length.
- RFC 1483 or local bridged or routed clients cannot have overlapping IP addresses, even across different interfaces.

- When the SSG Port-Bundle Host-Key is not configured, SSG local forwarding enables SSG to forward packets locally between any SSG hosts. However, when the SSG Port-Bundle Host-Key feature is configured, local forwarding works only between hosts that are connected to at least one common service.
- The SSG Port-Bundle Host-Key feature enables certain subscribers to have overlapping IP addresses. This binds subscribers to their respective downlink interfaces. Traffic from a user is not accepted if it arrives on any other interface. To enable subscriber-side interface redundancy when SSG port-bundle host-key functionality is configured and there are no overlapping IP host addresses, you must disable overlapping IP address support (and hence, the subscriber binding to the interface).

Configuring the SSG Port-Bundle Host-Key

To use SSG port-bundle host-key functionality, you must enable the feature, specify the subscriber traffic to be port-mapped, and specify the SSG source IP addresses. You can also optionally specify the port-bundle length. Perform this task to configure the SSG port-bundle host-key functionality.

SUMMARY STEPS

1. **ssg port-map**
2. **destination range** *port-range-start to port-range-end* [**ip** *ip-address*]
3. **destination access-list** *access-list-number*
4. **source ip** {*ip-address* | *interface*}
5. **length** *bits*
6. **no host overlap**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ssg port-map Example: Router(config)# ssg port-map	Enables the SSG port-bundle host-key feature and enables ssg-port-map configuration mode.
Step 2	destination range <i>port-range-start to port-range-end</i> [ip <i>ip-address</i>] Example: Router(config-ssg-portmap)# destination range 8080 to 8081	Identifies packets for port-mapping by specifying the TCP port range to compare against the subscriber traffic. <ul style="list-style-type: none"> • If the destination IP address is not configured, a default network must be configured and routable from SSG in order for this command to be effective. • If the destination IP address is not configured, any traffic going to the default network with the destination port will fall into the destination port range and will be port mapped. • You can use multiple entries of the destination access-list and destination range commands. The port ranges and access lists are checked against the subscriber traffic in the order in which they were defined.

	Command or Action	Purpose
Step 3	<p>destination access-list <i>access-list-number</i></p> <p>Example: Router(config-ssg-portmap)# destination access-list 100</p>	<p>Identifies packets for port-mapping by specifying an access list to compare against the subscriber traffic. Port map will be applied to traffic matching the mentioned access list.</p> <ul style="list-style-type: none"> You can use multiple entries of the destination access-list and destination range commands. The port ranges and access lists are checked in the order in which they are defined.
Step 4	<p>source ip {<i>ip-address</i> <i>interface</i>}</p> <p>Example: Router(config-ssg-portmap)# source ip 10.0.50.1</p>	<p>Specifies an SSG source IP address. If you specify an interface instead of an IP address, SSG uses the main IP address of the specified interface.</p> <ul style="list-style-type: none"> You can use multiple entries of the source ip command. All SSG source IP addresses configured using the source ip command must be routable in the management network where SESM resides.
Step 5	<p>length <i>bits</i></p> <p>Example: Router(config-ssg-portmap)# length 5</p>	<p>Modifies the port-bundle length, in bits, used to determine the number of ports per bundle and the number of bundles per group. Default value is 4. A value of 'n' will result in 2^n ports per bundle.</p>
Step 6	<p>no host overlap</p> <p>Example: Router(config-ssg-portmap)# no host overlap</p>	<p>Disables SSG support of overlapping host IP addresses.</p> <ul style="list-style-type: none"> Use this command to enable subscriber-side interface redundancy when SSG port-bundle host-key functionality is configured and there are no overlapping IP host addresses.
Step 7	<p>exit</p> <p>Example: Router(config-ssg-portmap)# exit</p>	<p>Exits ssg-port-map configuration mode.</p>

Verifying SSG Port-Bundle Host-Key Configuration

Perform this task to verify SSG port-bundle host-key configuration and operation.

SUMMARY STEPS

- show running-config**
- show ssg port-map status** [*free* | *inuse* | *reserved*]
- show ssg port-map ip** *ip-address* **port** *port-number*

DETAILED STEPS

-
- Step 1** To verify the SSG Port-Bundle Host-Key configuration, use the **show running-config** command in privileged EXEC mode.
- Step 2** To display a summary of all port-bundle groups, use the **show ssg port-map status** command with no keywords:
- ```
Router# show ssg port-map status
```

```
Bundle-length = 4
```

```
Bundle-groups:-
```

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

Use the **show ssg port-map status** command with the **free**, **reserved**, or **inuse** keyword to display port bundles with the specified status:

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

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

| Port-bundle | Subscriber Address | Interface       |
|-------------|--------------------|-----------------|
| 64          | 10.10.3.1          | Virtual-Access2 |

**Step 3** To display information about a specific port bundle, use the **show ssg port-map ip** command:

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

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

```
Port-mappings:-
```

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

## Configuring SSG to AAA Server Interaction

SSG communicates with a AAA server for authorization, authentication and accounting using the RADIUS protocol. SSG and the AAA server interact to authenticate subscribers, and to retrieve subscriber and service profiles. Perform this task to configure the shared key between SSG and the AAA server.

### Prerequisites

In order for SSG to communicate with SESM and the AAA servers, the AAA servers must be configured correctly. See the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* for the AAA and RADIUS commands and tasks for configuring AAA servers.

### SUMMARY STEPS

1. **ssg service-password** *password*

## DETAILED STEPS

|                                                                                                                                               |                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> <code>ssg service-password password</code><br><br><b>Example:</b><br>Router(config)# <code>ssg service-password password</code> | Sets the password used to authenticate the SSG with the local AAA server while downloading service profiles. <ul style="list-style-type: none"> <li>This value must match the value configured for the AAA server service profiles.</li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Monitoring and Maintaining Initial SSG Communication

Perform this task to monitor and maintain initial SSG communication. The commands do not have to be entered in a particular order.

## SUMMARY STEPS

1. `show ssg connection ip-address service-name [interface]`
2. `show ssg host [ip-address [interface]`
3. `show ssg port-map ip ip-address port port-number`
4. `show ssg port-map status [free | reserved | inuse]`
5. `show ssg interface [interface | brief]`
6. `show ssg summary`
7. `clear ssg connection ip-address service-name [interface]`
8. `clear ssg host ip-address interface`

## DETAILED STEPS

|               | Command or Action                                                                                                                                         | Purpose                                                                                                                                                                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <code>show ssg connection ip-address service-name [interface]</code><br><br><b>Example:</b><br>Router# <code>show ssg connection 19.1.1.19 InstMsg</code> | (Optional) Displays the connections of a given host and a service name.                                                                                                                                                                         |
| <b>Step 2</b> | <code>show ssg host [ip-address [interface]   username]</code><br><br><b>Example:</b><br>Router# <code>show ssg host 10.3.1.1</code>                      | (Optional) Displays the information about a subscriber and current connections of the subscriber.                                                                                                                                               |
| <b>Step 3</b> | <code>show ssg port-map ip ip-address port port-number</code><br><br><b>Example:</b><br>Router# <code>show ssg port-map ip 10.13.60.2 port 64</code>      | (Optional) Displays the following information about a port bundle: <ul style="list-style-type: none"> <li>Port maps in the port bundle</li> <li>Subscriber's IP address</li> <li>Interface through which the subscriber is connected</li> </ul> |

|               | <b>Command or Action</b>                                                                                                                                        | <b>Purpose</b>                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 4</b> | <p><b>show ssg port-map status</b> [<i>free</i>   <i>reserved</i>   <i>inuse</i>]</p> <p><b>Example:</b><br/>Router# show ssg port-map status</p>               | <p>(Optional) Displays information on port-bundle groups, including the following:</p> <ul style="list-style-type: none"> <li>• List of port-bundle groups</li> <li>• Port-bundle length</li> <li>• Number of free, reserved, and in-use port bundles in each group</li> </ul>           |
| <b>Step 5</b> | <p><b>show ssg interface</b> [<i>interface</i>   <i>brief</i>]</p> <p><b>Example:</b><br/>Router# show ssg interface atm 3/0.10</p>                             | <p>(Optional) Displays information about SSG interfaces.</p> <ul style="list-style-type: none"> <li>• Use this command without any keywords or arguments to display information about all SSG interfaces.</li> </ul>                                                                     |
| <b>Step 6</b> | <p><b>show ssg summary</b></p> <p><b>Example:</b><br/>Router# show ssg summary</p>                                                                              | <p>(Optional) Displays a summary of the SSG configuration.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> |
| <b>Step 7</b> | <p><b>clear ssg connection</b> <i>ip-address service-name</i> [<i>interface</i>]</p> <p><b>Example:</b><br/>Router# clear ssg connection 10.18.1.1 Service1</p> | <p>(Optional) Removes the connections of a given host and a service name.</p>                                                                                                                                                                                                            |
| <b>Step 8</b> | <p><b>clear ssg host</b> <i>ip-address interface</i></p> <p><b>Example:</b><br/>Router# clear ssg host 192.168.1.1 fastethernet</p>                             | <p>(Optional) Removes or disables a given host or subscriber.</p>                                                                                                                                                                                                                        |

## Troubleshooting Initial SSG Communication

Perform the following steps to troubleshoot the communication between SSG and the AAA server:

### SUMMARY STEPS

1. `debug radius`
2. `debug ssg port-map {events | packets}`

### DETAILED STEPS

|        | Command or Action                                                                                                            | Purpose                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>debug radius</code><br><br><b>Example:</b><br>Router # <code>debug radius</code>                                       | Displays debugging information associated with RADIUS. <ul style="list-style-type: none"> <li>• Use this command to troubleshoot communication between SSG and the AAA server.</li> </ul> |
| Step 2 | <code>debug ssg port-map {events   packets}</code><br><br><b>Example:</b><br>Router # <code>debug ssg port-map events</code> | Displays debug messages for port-mapping.                                                                                                                                                 |

## Configuration Examples for Establishing Initial SSG Communication

This section contains the following examples:

- [SSG Interface Direction: Examples, page 20](#)
- [SSG Interface Redundancy: Examples, page 21](#)
- [SSG Port-Bundle Host-Key Configuration: Example, page 22](#)
- [SSG and AAA Server Interaction Configuration: Example, page 22](#)
- [Establishing Initial SSG Communication: Example, page 23](#)

### SSG Interface Direction: Examples

#### Setting the Direction of a Single Interface: Example

The following example shows how to configure Fast Ethernet interface 1/0 as a downlink interface:

```
ip cef
ssg enable
!
interface FastEthernet 1/0
 ssg direction downlink
```

**Setting the Direction of a Range of PVCs: Example**

The following example show how to create a range called “MyRange” and set the direction of all subinterfaces in the range to downlink:

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

## SSG Interface Redundancy: Examples

**Service Bound to Multiple Uplink Interfaces: Example**

In the following example, a service called “sample-service” is bound to two uplink interfaces: ATM interface 1/0.1 is the primary interface, and ATM interface 1/0.2 is the secondary interface. Both interfaces are configured as members of groupA.

```
ip cef
ssg enable
!
ssg bind service sample-service atm 1/0.1
ssg bind service sample-service atm 1/0.2 100
!
interface ATM 1/0.1 point-to-point
 ip address 10.1.0.1 255.255.0.0
 ssg direction uplink member groupA
!
interface ATM 1/0.2 point-to-point
 ip address 10.2.0.1 255.255.0.0
 ssg direction uplink member groupA
!
```

**Service Bound to Next Hop with Multiple Uplink Interfaces: Example**

In the following example, a service called “sample-serviceA” is bound to next-hop gateway 10.1.1.1. Next-hop gateway 10.1.1.1 is reachable through two uplink interfaces: ethernet interface 1/0 and Ethernet interface 2/0. The group name “service-groupA” indicates that both interfaces share the same service (“sample-serviceA”).

For any services bound to either of the two interfaces, downstream traffic from the service is accepted on either interface.

```
ip cef
ssg enable
!
ssg bind service sample-serviceA 10.1.1.1
!
interface ethernet 1/0
 ip address 10.0.1.1 255.255.255.0
 ssg direction uplink member service-groupA
!
interface ethernet 2/0
 ip address 10.0.2.1 255.255.255.0
 ssg direction uplink member service-groupA
!
ip route 10.1.1.1 255.255.255.255 eth 1/0 10
ip route 10.1.1.1 255.255.255.255 eth 2/0 20
!
```

**Service Bound to Multiple Next Hops: Example**

## Service Bound to Multiple Next Hops: Example

In the following example, a service called “serviceB” is bound to two next-hop gateways, 10.0.0.1 and 20.0.0.1, that are reachable through two uplink interfaces, Ethernet interface 1/0 and Ethernet interface 2/0 respectively. The group name “groupB” indicates that both interfaces share the same service (“serviceB”).

For any services bound to either of the two interfaces, downstream traffic from the service is accepted on either interface.

```
ip cef
ssg enable
!
ssg bind service serviceB 10.0.0.1
ssg bind service serviceB 20.0.0.1
!
interface ethernet 1/0
 ip address 10.0.0.2 255.255.255.0
 ssg direction uplink member groupB
!
interface ethernet 2/0
 ip address 20.0.0.2 255.255.255.0
 ssg direction uplink member groupB
!
```

**SSG Port-Bundle Host-Key Configuration: Example**

In the following example, packets that match the specified TCP port range or that are permitted by access list 100 will be port-mapped. Loopback interface 1 is specified as the SSG source IP address.

```
ssg port-map
 destination range 8080 to 10100 ip 10.13.6.100
 port-map destination access-list 100
 port-map source ip Loopback1
```

**SSG and AAA Server Interaction Configuration: Example**

In the following example, AAA and SSG features are enabled and configured to establish the interaction between the two.

```
! enable aaa; enable groups for PPP authentication,
! service-profile authorization/download, l2tp authorization and
! accounting method-list (in the order shown below)
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa authorization network ssg_aaa_author_internal_list none
aaa accounting network default start-stop group radius
!

! Enables CEF
ip cef
!
! Enables SSG
ssg enable
Configures password for service-profile download
ssg service-password servicecisco
```

```

!
! Configures SSG communication with the RADIUS server
!
radius-server host 192.168.2.62 auth-port 1812 acct-port 1813 key cisco
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication

```

## Establishing Initial SSG Communication: Example

The following example illustrates all the tasks that must be completed to enable SSG and establish initial communication with other network devices.

```

!
! Configures AAA and enables communication with the AAA server
aaa new-model
!
! Configures login access
aaa authentication banner CCCCC !!! Cisco SSG !!! aaa authentication fail-message CCC !!!
Unauthorized Access Is Not Permitted !!!
aaa authentication password-prompt Password:
aaa authentication username-prompt Username:
aaa authentication login default local group radius
aaa authentication login console local
!
! Configures PPP authentication, service-profile authorization,
! l2tp tunnel authorization, accounting-list
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa authorization network ssg_aaa_author_internal_list none
aaa accounting network default start-stop group radius
!
aaa nas port extended
aaa session-id common
!
!
! Enables CEF
ip cef
!
! Enables SSG
ssg enable
! Configures the default network
ssg default-network 192.168.2.0 255.255.255.0
! Configures the shared key between SSG and the AAA server
ssg service-password servicecisco
!
! Configures SSG-SESM API communication
ssg radius-helper auth-port 1812 acct-port 1813
ssg radius-helper key cisco
!
! Configures SSG port-bundle host-key
ssg port-map
destination range 80 to 80 ip 192.168.2.55
destination range 443 to 443 ip 192.168.2.55
destination range 8090 to 8101 ip 192.168.2.55
source ip Loopback10
source ip Loopback11
!
! Configures an interface towards services (uplink interface)
interface FastEthernet1/0.1
description SSG-Service internet

```

```

encapsulation dot1Q 10
ip address 10.1.1.41 255.255.255.0
ip nat outside
ip nbar protocol-discovery
no ip mroute-cache
ssg direction uplink
!
! Configures an interface towards subscribers (downlink interface)
interface FastEthernet2/0.1
description Subscriber Access
encapsulation dot1Q 70
ip address 10.1.1.1 255.255.255.0
ssg direction downlink
!
! Configures SSG communication with the RADIUS server
radius-server attribute 44 include-in-access-req
radius-server attribute 55 include-in-acct-req
radius-server attribute nas-port format d
radius-server host 192.168.2.62 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 5
radius-server timeout 30
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!

```

## Additional References

The following sections provide references related to establishing SSG connectivity.

## Related Documents

| Related Topic              | Document Title                                                                    |
|----------------------------|-----------------------------------------------------------------------------------|
| Configuring SESM           | <a href="#">Cisco Subscriber Edge Services Manager</a> documentation              |
| RADIUS commands            | <a href="#">Cisco IOS Security Command Reference</a>                              |
| RADIUS configuration tasks | “Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> |
| SSG commands               | <a href="#">Cisco IOS Service Selection Gateway Command Reference</a>             |

## MIBs

| MIBs                                                                                                                                                                                                                                                                                                                                                  | MIBs Link                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The Service Selection Gateway MIB enables network administrators to use Simple Network Management Protocol (SNMP) to monitor and manage SSG. The SSG MIB contains objects that correspond to and allow the monitoring of several important SSG features.</p> <p>For detailed list of MIB objects and their definitions, see the CISCO-SSG-MIB.</p> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for Implementing SSG

Table 3 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the [Service Selection Gateway Features Roadmap](#).

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


**Note**

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for Implementing SSG: Initial Tasks

| Feature Name                                          | Releases                                            | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initial SSG Communication                             | 12.0(3)DC<br>12.3(4)B<br>12.2(11)T<br>12.3T<br>12.4 | <p>The Initial SSG Communication feature comprises initial tasks you need to perform to enable SSG on the router and to establish SSG communication with other key components of the network, including Subscriber Edge Services Manager (SESM) and the authentication, authorization, and accounting (AAA) server.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Enabling SSG, page 3</a></li> <li>• <a href="#">Configuring the Default Network, page 10</a></li> <li>• <a href="#">Configuring SSG-SESM API Communication, page 11</a></li> </ul> |
| SSG Direction Configuration for Interfaces and Ranges | 12.2T<br>12.3(4)T                                   | <p>SSG implements service selection through selective routing of IP packets to destination networks on a per-subscriber basis. SSG uses the concept of interface direction (uplink or downlink) to help determine the forwarding path of incoming packets. An uplink interface is an interface towards the services; a downlink interface is an interface towards the subscribers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring SSG Interface Direction, page 4</a></li> </ul>                                                          |

**Table 3** Feature Information for Implementing SSG: Initial Tasks (continued)

| Feature Name                    | Releases                               | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSG Interface Redundancy        | 12.3(8)T                               | <p>SSG interface redundancy allows services to be associated with more than one interface to protect against link failures.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Uplink Interface Redundancy Overview, page 4</a></li> <li>• <a href="#">Downlink Interface Redundancy Overview, page 5</a></li> <li>• <a href="#">SSG Uplink Interface Redundancy Topologies, page 5</a></li> <li>• <a href="#">SSG Interface Redundancy: Examples, page 21</a></li> </ul>                                           |
| SSG Port-Bundle Host-Key        | 12.3(4)B<br>12.2(11)T<br>12.3T<br>12.4 | <p>The SSG Port-Bundle Host Key feature enhances communication and functionality between the Service Selection Gateway (SSG) and the Cisco Subscriber Edge Services Manager (SESM) by introducing a mechanism that uses the host source IP address and source port to identify and monitor subscribers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring SSG Port-Bundle Host-Key Functionality, page 12</a></li> <li>• <a href="#">Configuring SSG to AAA Server Interaction, page 17</a></li> </ul> |
| SSG Unconfig                    | 12.2T<br>12.3(4)T                      | <p>The Unconfig feature releases and cleans up system resources acquired by SSG.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">System Resource Cleanup When SSG Is Unconfigured, page 3</a></li> </ul> <p>The following command was introduced by this feature: <b>no ssg enable force-cleanup</b>.</p>                                                                                                                                                                                                        |
| Implementing SSG: Initial Tasks | 15.0(1)M                               | This feature was removed in Cisco IOS Release 15.0(1)M.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2005–2009 Cisco Systems, Inc. All rights reserved.