SSG Mobile Wireless Enhancements

First Published: November 5, 2007
Last Updated: November 5, 2007

The Service Selection Gateway (SSG) is a Cisco IOS software feature set, supported on multiple platforms, that works with the Cisco Subscriber Edge Services Manager (SESM) and other components to provide a subscriber edge services solution. It implements Layer 3 service selection through selective routing of IP packets to destination networks on a per subscriber basis. SSG authenticates users, who are accessing the SSG services, based on the RADIUS access request received from the SESM or from the downstream device such as a Gateway GPRS Support Node (GGSN) or Packet Data Serving Node (PDSN).

The SSG Mobile Wireless Enhancements feature describes additional functionality enhancements including accounting-on-off packet suppression, accounting-start ignore configuration, and Packet of Disconnect (PoD) forwarding to the Network Access Server (NAS).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for SSG Mobile Wireless Enhancements" section on page 13.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

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

Prerequisites for SSG Mobile Wireless Enhancements

- Before implementing SSG Mobile Wireless enhancements, SSG must be enabled by using the **ssg enable** command.
- This enhancement supports General Packet Radio Service/Extensible Authentication Protocol (GPRS/EAP) for the SSG. You should understand the following technologies:
  - The Serving GPRS Support Node (SGSN) connects the radio access network (RAN) to the GPRS and the 3G Universal Mobile Telecommunication System (UMTS) core and tunnels user sessions to the GGSN. For more information, see *Cisco GGSN Release 7.0 Configuration Guide*.
  - The SSG EAP Transparency feature enables the Cisco Service Selection Gateway (SSG) on a Cisco router to act as a RADIUS proxy during EAP authentication and to create the host. For more information, see the *SSG EAP Transparency* feature module.
  - The Access Zone Router (AZR) provides connectivity, client address management, security services, and routing across a WAN from each access point to an operator's point of presence (POP) or data center. For more information, see the *Public Wireless LAN for Service Providers Solutions* document.

Restrictions for SSG Mobile Wireless Enhancements

SSG does not process multicast packets.

Information About SSG Mobile Wireless Enhancements

To implement SSG Mobile Wireless enhancements, you should understand the following concepts:

Accounting-On-Off Packet Suppression

While the Service Selection Gateway (SSG) is acting as a RADIUS proxy for the Gateway GPRS Support Node (GGSN), it also receives all accounting packets: accounting-on-off packets as well as accounting-start-stop packets. By default, only accounting-on-off packets are forwarded to the real authentication, authorization, and accounting (AAA) server.

The **forward accounting-on-off** command allows you to override this default behavior and to suppress transparent proxying of accounting packets.

SSG always proxies accounting-on-off packets received from client GGSNs. These packets are used to signal that the client GGSN has just rebooted (or is about to be rebooted). When SSG receives the packets, SSG destroys all host objects associated with the specified client GGSN before forwarding the packet. SSG uses the NAS IP address in the accounting-on-off packets to determine the affected GGSN. Determining the affected GGSN enables multiple tunnel interfaces to exist between the GGSN and SSG. Although there are multiple RADIUS clients configured at SSG, only a single accounting-on-off packet is generated by the GGSN. As part of the normal SSG functionality, SSG sends accounting-start-stop records for both the active host objects and for any services to which they are connected.

Consider the following scenario in a load-balancing environment. Assume that there are 10 GGSNs and 10 SSGs in the system. In this case, when the GGSN fails, there will be 10 accounting-off packets sent to the RADIUS load balancing (RLB) server farm. The RLB server farm replicates each accounting-off packet to the 10 SSGs. Each SSG in turn forwards these accounting-off packets to the AAA server. So there is a total of 100 accounting-off packets in a short period of time. For some customers the AAA server often has problems handling this high rate of accounting on and off packets, which increases the possibility of a system failure.

In a Cisco Mobile Exchange (CMX) solution, you can enable a server to stop forwarding the accounting-off packets in all the routers except for two or three routers. Enabling the server in this way ensures that the AAA server will not receive the accounting-off packets from every SSG in the system.

Accounting-Start Packet Discards to Retain a Host with Varying IP Addresses

Before Cisco IOS Release 12.4(15)T, the default behavior of the **session-identifier msid** command for SSG is to disconnect a host object if a second accounting-start packet is received for a Mobile Station Identifier (MSID) address with a different IP address. However, this behavior can cause a problem especially in the Public Wireless Local Area Network (PWLAN) space for clients with multiple interfaces (that is, wireless and Ethernet interfaces), which can result in packets sent from a single interface with multiple source IP addresses.

This enhancement to the **session-identifier msid unique ip** command instructs SSG to discard the subsequent accounting-start records with the same MSID but a different IP address.

PoD to NAS Forwarding

When SSG, acting as a RADIUS proxy, receives the Packet of Disconnect (PoD) from a RADIUS server, it cleans up the corresponding host object but does not forward the PoD to NAS. As a result, the NAS is not informed about the RADIUS server's decision to disconnect the user session.

This enhancement disconnects the host object when the PoD is received from the AAA server and also forwards it to a downstream device. When SSG forwards the PoD to the downstream NAS, the NAS will send a PoD-ACK/NAK back to SSG. Previously, SSG would have deleted the host object for that particular user at this point. Therefore, this enhancement ensures that SSG ignores the PoD-ACK/NAKs and accounting-stop packets sent by the NAS in response to the forwarded PoD.

On receiving the POD request with radius code 40, SSG disconnects the user by deleting all host-related information maintained by SSG. The following points summarize the PoD support by SSG:

- The host is identified by the following properties:
  - Attribute 8: framed IP address
  - SSG account-info VSA: port bundle information present with S subattribute
- On finding the host, SSG deletes the host and connections made by the host.

- For a transparent autologon (TAL) user with no host object (a Transparent Passthrough [TP] user), the TP entry will be deleted.
- Inactive hosts will not be deleted.
- In radius-proxy mode, SSG deletes the host object, but PoD will not be forwarded to the downstream device. To clean up the session throughout the network, the AAA server will now send the PoD to downstream devices.

How to Configure SSG Mobile Wireless Enhancements

This section contains the following procedures:

- Suppressing Accounting On-Off Packets, page 4 (optional)
- Retaining a Host with Varying IP Addresses by Ignoring Accounting-Start Packets, page 5 (optional)

Suppressing Accounting On-Off Packets

Perform this task to configure SSG to suppress accounting-on-off packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg enable**
4. **ssg radius-proxy**
5. **no forward accounting-on-off**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg enable** **Example:** `Router(config)# ssg enable`	Enables SSG.
Step 4	**ssg radius-proxy** **Example:** `Router(config)# ssg radius-proxy`	Enables SSG RADIUS proxy.
Step 5	**no forward accounting-on-off** **Example:** `Router(config-radius-proxy)# no forward accounting-on-off`	Suppresses the forwarding of accounting-on-off packets.

Retaining a Host with Varying IP Addresses by Ignoring Accounting-Start Packets

Perform this task to configure SSG to enable client devices with multiple IP addresses to access the host.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg enable**
4. **ssg radius-proxy**
5. **client-address** *ip-address*
6. **key** *secret*
7. **session-identifier msid unique ip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg enable** **Example:** `Router(config)# ssg enable`	Enables SSG.
Step 4	**ssg radius-proxy** **Example:** `Router(config)# ssg radius-proxy`	Enables SSG RADIUS proxy.
Step 5	**client address** *ip-address* **Example:** `Router(config-radius-proxy)# client-address 172.16.1.1`	Specifies the IP address of the RADIUS client.
Step 6	**key** *secret* **Example:** `Router(config-radproxy-client)# key cisco`	Specifies the key shared with the RADIUS client.
Step 7	**session-identifier msid unique ip** **Example:** `Router(config-radproxy-client)# session-identifier msid unique ip`	Specifies the attribute for differentiating sessions. This example uses the MSID as session differentiator and its associated IP address.

Configuration Examples for SSG Mobile Wireless Enhancements

This section provides the following configuration examples:

- Suppressing Accounting On-Off Packets: Example, page 7
- Retaining a Host with Varying IP Addresses by Ignoring Accounting-Start Packets: Example, page 7

Suppressing Accounting On-Off Packets: Example

The following example shows how to suppress packet forwarding from the RADIUS client to the AAA server:

```
enable
configure terminal
ssg enable
ssg radius-proxy
no forward accounting-on-off
```

Retaining a Host with Varying IP Addresses by Ignoring Accounting-Start Packets: Example

The following example shows how to configure SSG to identify the specified client session based on the IP address associated with the MSID:

```
enable
configure terminal
ssg enable
ssg radius-proxy
client-address 172.16.1.1
key cisco
session-identifier msid unique ip
```

Additional References

The following sections provide references related to the SSG Mobile Wireless Enhancements feature.

Related Documents

Related Topic	Document Title
Selection Gateway commands: complete command syntax, command mode, command history, defaults, usage guidelines, and example	*Cisco IOS Service Selection Gateway Command Reference,* Release 12.4
SSG configuration tasks	*Cisco IOS Service Selection Gateway Configuration Guide,* Release 12.4 *Cisco Express Forwarding Overview* chapter in the *Cisco IOS Switching Services Configuration Guide,* Release 12.0 *SSG AutoDomain* feature module, Release 12.2(4)B *SSG EAP Transparency* feature module, Release 12.3(4)T

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2284	*PPP Extensible Authentication Protocol (EAP)*
RFC 2865	*Remote Authentication Dial-In User Services (RADIUS)*
RFC 2869	*RADIUS Delegated-IPv6-Prefix Attribute*
RFC 2548	*Microsoft Vendor-Specific RADIUS Attributes*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- forward accounting-on-off
- session-identifier

forward accounting-on-off

To allow forwarding of accounting-on-off packets generated by any RADIUS clients to the authentication, authorization, and accounting (AAA) server, use the **forward accounting-on-off** command in SSG radius-proxy mode. To suppress forwarding of accounting-on-off packets, use the **no** form of this command.

forward accounting-on-off

no forward accounting-on-off

Syntax Description

This command has no arguments or keywords.

Command Default

Accounting-on-off packets generated by RADIUS clients are not sent to the AAA server.

Command Modes

SSG radius-proxy

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following example shows how to allow packet forwarding from the RADIUS client to the AAA server:

```
Router(config)# ssg enable
Router(config)# ssg radius-proxy
Router(config-radius-proxy)# forward accounting-on-off
```

Related Commands

Command	Description
forward accounting-start-stop	Allows accounting start, stop, and update packets generated by any RADIUS clients to the AAA server.

session-identifier

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 [**acct-sess-id** | **auto** | **correlation-id** | [**msid** [**unique ip** | **username**]]

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

Syntax Description

acct-sess-id	(Optional) Uses the accounting session identifier as session differentiator.
auto	(Optional) Determines the session differentiator automatically.
correlation-id	(Optional) Specifies the correlation identifier as session differentiator.
msid	(Optional) Uses the Mobile Station Identifier (MSID) as session differentiator.
unique	(Optional) Specifies a unique MSID.
ip	(Optional) Specifies the IP address associated with the MSID.
username	(Optional) Specifies the user's name as a session differentiator.

Defaults

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.
12.4(15)T	The **unique**, **ip**, and **username** keywords were added to the **msid** keyword.

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 172.16.1.1 to the RADIUS server, assign the shared secret "cisco" key to the client, and use the Accounting-Session-ID attribute to identify the specified client session:

```
client-address 172.16.1.1
 key cisco
 session-identifier acct-sess-id
```

The following example shows how to configure SSG to identify the specified client session based on the IP address associated with MSID:

```
Router(config)# ssg enable
Router(config)# ssg radius-proxy
Router(config-radius-proxy)# client-address 172.16.1.1
Router(config-radproxy-client)# key cisco
Router(config-radproxy-client)# session-identifier msid unique ip
```

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.

Feature Information for SSG Mobile Wireless Enhancements

Table 1 lists the release history for this feature.

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 1 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 1 Feature Information for SSG Mobile Wireless Enhancements

Feature Name	Releases	Feature Information
SSG Mobile Wireless Enhancements	12.4(15)T	The Service Selection Gateway (SSG) is a Cisco IOS software feature set, supported on multiple platforms, that works with the Cisco Subscriber Edge Services Manager (SESM) and other components to provide a subscriber edge services solution. It implements Layer 3 service selection through selective routing of IP packets to destination networks on a per subscriber basis. SSG authenticates users, who are accessing the SSG services, based on the RADIUS access request received from the SESM or from the downstream device such as GGSN/PDSN. The SSG Mobile Wireless Enhancements feature describes additional functionality enhancements including accounting-on-off suppression, accounting-start ignore configuration, and Packet of Disconnect (PoD) forwarding to the Network Access Server (NAS). The following commands were introduced or modified by this feature: **forward accounting-on-off**, **session-identifier**.

Glossary

AAA—authentication, authorization, and accounting. The network security service that provides the primary framework through which you set up access control on your router or access server.

CEF—Cisco Express Forwarding. An advanced Layer 3 IP switching technology.

CMX—Cisco Mobile Exchange. A standards-based framework that links the radio-access network (RAN) to IP networks and their value-added, content-based IP services.

EAP—Extensible Authentication Protocol. A framework for transporting authentication protocols. It can be used for authenticating dial-up and VPN connections, and also Local Area Network (LAN) ports in conjunction with IEEE 802.1X.

GGSN—Gateway GPRS Support Node. The General Packet Radio Service (GPRS) provides packet radio access for mobile Global System for Mobile Communications (GSM).

NAS—Network Access Server. Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the PSTN).

PDSN—Packet Data Serving Node. PDSN provides the primary wireless mobile data access to the Internet, intranets, and Wireless Application Protocol (WAP) servers for mobile stations utilizing a CDMA2000 Radio Access Network (RAN).

PoD—Packet of Disconnect. A RADIUS access-request packet that is intended to be used where the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS access-accept packet.

PWLAN—Public Wireless Local Area Network. A network comprised of a public switched telephone network, a digital subscriber line access multiplexer, and at least one public telephone.

RADIUS—Remote Authentication Dial-In User Service. A distributed client/server system that secures networks against unauthorized access.

SESM—Subscriber Edge Services Manager. An extensible set of applications providing on-demand services and service management.

SSG—Service Selection Gateway.

TAL—Transparent autologin. This feature enables Service Selection Gateway (SSG) to authenticate and authorize a user on the basis of the source IP address of packets received from the user.

TP—Transparent passthrough user. This allows unauthenticated traffic to pass through an interface.

VSA—vendor specific attribute. VSAs allow vendors to support their own proprietary RADIUS attributes that are not included in RFCs 2865 and 2866.

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