SSG Proxy for CDMA2000

The SSG Proxy for CDMA2000 feature allows you to extend the functionality of the existing SSG RADIUS proxy so that it may be used in CDMA2000 networks.

Code Division Multiple Access (CDMA) is a digital spread-spectrum modulation technique used mainly with personal communications devices such as mobile phones. CDMA digitizes the conversation and tags it with a special frequency code. The data is then scattered across the frequency band in a pseudorandom pattern. The receiving device is instructed to decipher only the data corresponding to a particular code to reconstruct the signal.

When used in a CDMA2000 network, the Service Selection Gateway (SSG) provides RADIUS proxy services to the Packet Data Serving Node (PDSN) and the Home Agent (HA) for both Simple IP and Mobile IP authentication. SSG also provides service selection management and policy-based traffic direction for subscribers.

SSG Proxy for CDMA2000, used with Cisco Subscriber Edge Services Manager (SESM), provides users with on-demand services and service providers with service management and subscriber management.

SSG Proxy for CDMA2000 supports time- and volume-based usage accounting for Simple IP and Mobile IP sessions. Prepaid and postpaid services are supported. Host accounting records can be sent to multiple network elements, including Content Service Gateways (CSGs), Content Optimization Engines (COEs), and Wireless Application Protocol (WAP) gateways.

Feature History for the SSG Proxy for CDMA2000 Feature

Release	Modification
12.2(15)B	This feature was introduced.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

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

Contents

Prerequisites for SSG Proxy for CDMA2000

PDSN

- All RADIUS packets (including Access-Request packets for the Cisco variant of Module Subscriber Identity (MSID) based access) generated by the PDSN must contain the 3GPP2-Correlation-ID VSA.
- Access-Request packets for the Cisco variant of MSID-based access generated by the PDSN must contain the 3GPP2-Correlation-ID Vendor Specific Attribute (VSA).
- Accounting-Start packets generated by the PDSN must contain the 3GPP2-IP-Technology VSA.

HA

- No RADIUS packets generated by the HA can contain the 3GPP2-Correlation-ID VSA.

Note The following HA prerequisites are not standard HA behavior and must be configured.

- The HA must issue Access-Requests for all Mobile IP sessions.
- The HA must issue Accounting-Start packets and Accounting-Stop packets for all Mobile IP sessions.
- The HA must provide the Acct-Session-ID attribute in all RADIUS packets it generates. This enables the system to differentiate between multiple sessions with the same Network Access Identifier (NAI).

Miscellaneous

- RADIUS Access-Accept packets sent by the RADIUS server must contain the 3GPP2-IP-Technology VSA.

Restrictions for SSG Proxy for CDMA2000

SSG Proxy for CDMA2000 requires non standard extensions to the Home Agent behavior. See Prerequisites for SSG Proxy for CDMA2000, page 2 for more information.

Use of Autodomain When SSG Is Acting As a RADIUS Proxy in CDMA2000 Networks

In autodomain mode, SSG bypasses user authentication at the Network Attached Storage (NAS) Authentication, Authorization and Accounting (AAA) server. SSG instead downloads a generic profile for the specified autodomain. This profile may be a service profile for simple autodomain or a virtual user profile in extended mode autodomain. When SSG is acting as a RADIUS proxy in a CDMA2000 network, the profile returned in an Access-Accept from the AAA server must contain the 3GPP2-IP-Technology VSA to indicate to SSG whether this call setup is for a Simple IP call or for a Mobile IP call. Even if a network supports only one type of user (either all Simple IP users or all Mobile IP users), the Access-Accept packets received from the AAA must contain the 3GPP2-IP-Technology VSA. In networks that support only one type of user, the autodomain profiles can be formatted to contain the correct attribute. In networks that support both Mobile IP and Simple IP users simultaneously, the Access-Accept packets must contain the correct attribute for the type of user. The AAA server must be able to modify the contents of the generic autodomain profile so that it contains the correct VSA. SSG must receive a real rather than a cached response from the AAA server for each user logon. SSG Service Profile Caching must be disabled when SSG Autodomain is enabled and SSG is acting as a RADIUS proxy in a CDMA2000 network that supports both Simple IP and Mobile IP users.

Information About SSG Proxy for CDMA2000

This section comprises the following information about the SSG Proxy for CMDA2000 feature:

SSG Proxy for CDMA2000

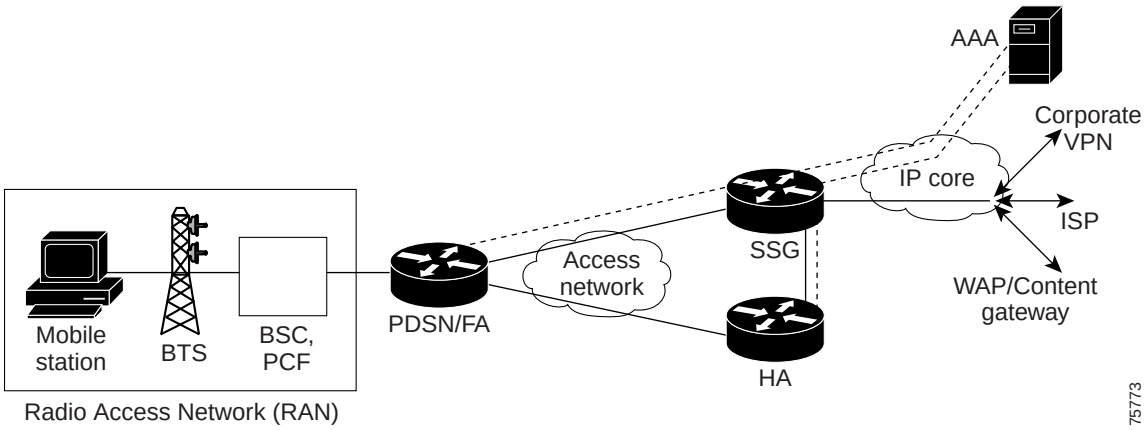
The SSG proxy for CDMA2000 extends the functionality of the existing SSG RADIUS proxy so that it may be used in CDMA2000 networks.

When used in a CDMA2000 network, SSG provides RADIUS proxy services to the packet data serving node (PDSN) and the Home Agent (HA) for both Simple IP and Mobile IP authentication. SSG also provides service selection management and policy-based traffic direction for subscribers.

SSG Proxy for CDMA2000, used with Cisco Subscriber Edge Services Manager (SESM), provides users with on-demand services and service providers with service management and subscriber management.

SSG Proxy for CDMA2000 supports time- and volume-based usage accounting for Simple IP and Mobile IP sessions. Prepaid and postpaid services are supported. Host accounting records can be sent to multiple network elements, including Content Service Gateways (CSGs), Content Optimization Engines (COEs), and Wireless Application Protocol (WAP) gateways.

Figure 1 CDMA Network



Key to Figure 1

Item	Description
BTS	Base Transceiver Station
BSC	Base Station Controller
PCF	Packet Control Function
PDSN/FA	Packet Data Serving Node / Foreign Agent
VPN	Virtual Private Network

CDMA

Code Division Multiple Access (CDMA) is a digital spread-spectrum modulation technique used mainly with personal communications devices such as mobile phones. CDMA digitizes the conversation and tags it with a special frequency code. The data is then scattered across the frequency band in a pseudorandom pattern. The receiving device is instructed to decipher only the data corresponding to a particular code to reconstruct the signal.

For more information about CDMA, see the “CDMA Overview” knowledge byte on the Mobile Wireless Knowledge Bytes web page:
http://www.cisco.com/warp/public/779/servpro/solutions/wireless_mobile/training.html.

CDMA2000

CDMA2000 Radio Transmission Technology (RTT) is a wideband, spread-spectrum radio interface that uses CDMA technology to satisfy the needs of third generation (3G) wireless communication systems. CDMA2000 is backward compatible with CDMA.

For more information about CDMA2000, refer to the “CDMA2000 Overview” knowledge byte on the Mobile Wireless Knowledge Bytes web page:
http://www.cisco.com/warp/public/779/servpro/solutions/wireless_mobile/training.html

SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers who use broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, refer to the *Service Selection Gateway* document.

SSG Proxy for CDMA2000 for Simple IP

When used in a CDMA2000 environment, SSG acts as a RADIUS proxy to the Packet Data Serving Node (PDSN) and to the Home Agent for Simple IP authentication. SSG sets up a host object for the following three access modes:

- PAP/CHAP authentication. In this mode, Password Authentication Protocol/ Challenge Handshake Authentication Protocol (PAP/CHAP) is performed during PPP setup and the NAI is received from a mobile node (MN).
- MSID-based access. In this mode, the MN does not negotiate CHAP or PAP and no Network Access Identifier (NAI) is received by the PDSN. The PDSN does not perform additional authentication. PDSN constructs an NAI based on the MSID and generates accounting records. Because a user password is not available from the MN, a globally configured password is used as the service password.
- MSID-based access Cisco variant. In this mode, a Cisco PDSN supports MSID-based access by using a realm retrieved from the RADIUS server. This realm is retrieved during an extra authentication phase with the RADIUS server.

SSG operating in a CDMA2000 network correlates Accounting-Start and Accounting-Stop requests. A PDSN may send out many Accounting-Start and Accounting-Stop requests during a session. These Accounting-Start and Accounting-Stop requests can be generated by PDSN hand off, Packet Control Function (PCF) hand off, interim accounting, and time-of-date accounting. SSG terminates a session only when it receives an Accounting-Stop request with the 3GPP2-Session-Continue VSA set to “FALSE” or when a subsequent Accounting-Start request is not received within a configured timeout. PPP renegotiation during a PDSN hand off is treated as a new session.

In SSG Proxy for CDMA2000 for Simple IP, the end-user IP address may be assigned statically by the PDSN, RADIUS server, or SSG. The end-user IP address can also be assigned directly from the autodomain service.

Network Address Translation (NAT) is automatically performed when necessary. NAT is generally necessary when IP address assignment is performed by any mechanism other than directly from the autodomain service (which may be a VPN). You can also configure SSG to always use NAT.

If the user profile contains Cisco attribute-value (AV) pairs of Virtual Private Dialup Network (VPDN) attributes, SSG initiates Layer 2 Tunneling Protocol (L2TP) VPN.

SSG Proxy for CDMA2000 for Mobile IP

For Mobile IP, SSG functions as the RADIUS proxy for both PDSN and the HA. SSG proxies PPP PAP or CHAP and Mobile Node (MN)/Foreign Agent (FA) CHAP authentication. SSG Proxy for CDMA2000 for Mobile IP can assign IP addresses statically by the PDSN, RADIUS server, or SSG. The end user IP address can also be assigned directly from the autodomain service.

Home Agent-Mobile Node (HA-MN) authentication and reverse tunneling must be enabled so that SSG can create host objects for Mobile IP sessions based on proxied RADIUS packets received from the HA.

The Home Agent must generate RADIUS accounting packets so that SSG can discover the user IP address and detect the termination of the session. Multiple Mobile IP sessions with the same NAI are supported. RADIUS packets must contain the Accounting-Session-ID attribute to be associated with the correct user session. SSG correlates RADIUS packets from the PDSN in order to obtain MSID information for a host object of a Mobile IP session.

SSG can set up a host object either with or without PAP/CHAP performed during the original PPP session.

SSG initiates L2TP VPN according to the SSG tunnel service VSAs in the user's profile. If the user profile contains Cisco AV pairs of VPDN, SSG sets up the L2TP tunnel per these VPDN attributes. SSG removes these AV pairs when sending the Access-Accept packet back to the PDSN.

Either the HA or the RADIUS server can assign the user's IP address.

Dynamic Home Agent Assignment

Dynamic HA assignment based on a mobile user's location is supported.

The SSG Proxy for CDMA2000 feature provides three options for dynamic HA assignment:

- The RADIUS server selects the local HA or any HA that is configured for session requests. For foreign-user call requests, the AAA server assigns the HA.
- SSG modifies the fixed HA address received from the RADIUS server to a local HA address. This method can be implemented without making any changes to the RADIUS server configuration. SSG does not modify the HA address for a foreign user. The foreign-user call request is registered with the HA address assigned by the AAA server.
- The PDSN implements dynamic HA assignment based on detection of the PDSN hand off.

Multiple RADIUS Server Support

SSG Proxy for CDMA2000 provides geographical redundancy by copying host object accounting packets and sending them to multiple RADIUS servers.

Benefits of SSG Proxy for CDMA2000

SSG Proxy for CDMA2000 provides the following features and capabilities:

- Centralized L2TP VPN tunnel management for Simple IP and for Mobile IP
- Centralized management for user service access and user-specific routing
  - Automatic logon of a user to SSG when the user establishes a PPP session with the PDSN or a Mobile IP flow with the HA
  - Automatic logon of the user to a service based on the domain name, structured username (user@domain), and Mobile Station ID (MSID). This eliminates the need for a service provider to have to make changes to existing AAA servers for VPDN service.
- Dynamic HA assignment

- Multiservice networking, including simultaneous services and sequential services, without the user having to log out and log back in
- Packet filtering. SSG uses Cisco IOS access control lists (ACLs) to prevent users, services, and pass through traffic from accessing specific IP addresses and ports.
- Per-service and per-destination accounting and billing
- Prepaid for CDMA2000 services
- SSG TCP Redirect for Services to captive portals for unauthenticated users

How to Configure SSG Proxy for CDMA2000

This section contains the following procedures:

- Configuring Multiple RADIUS Server Support, page 7
- Configuring New Timers, page 9
- Configuring Session Identification Attributes, page 12
- Configuring Home Agent IP Addresses, page 13

Configuring Multiple RADIUS Server Support

This command is used to provide geographical redundancy for accounting records by allowing copies of host object accounting packets to be sent to multiple RADIUS servers. Note this is distinct from RADIUS server failover - the requirement here is that clones of accounting packets are always forwarded to each of the configured servers, not just when the primary server fails. To configure the support for multiple RADIUS servers, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **server** *ip-address* [**auth** *auth-port*][**acct** *acct-port*]
5. Repeat Step 4 to configure additional RADIUS servers.
6. **exit**
7. **aaa group server radius** *group-name*
8. **server** *ip-address* [**auth** *auth-port*][**acct** *acct-port*]
9. Repeat Step 8 to configure additional RADIUS servers.
10. **exit**
11. **aaa accounting network ssg_broadcast_accounting start-stop broadcast group** *group-name 1* **group** *group-name 2*

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	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius myservergroup1`	Groups RADIUS server hosts into distinct lists and distinct methods. • *group-name*—Character string used to name the group of servers.
Step 4	**server** *ip-address* [**auth** *auth-port*] [**acct** *acct-port*] **Example:** `Router(config-sg-radius)# server 1.2.3.4 [auth 1645] [acct 1646]`	Configures the IP address of the RADIUS server for the group server. • *ip-address*—IP address of the RADIUS server host. • **auth** *auth-port*—(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The [*auth-port*] argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0. • **acct** *acct-port*—(Optional) Specifies the UDP destination port for accounting requests. The [*acct-port*] argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.
Step 5	Repeat Step 4 to configure additional RADIUS servers.	
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits server group RADIUS configuration mode.
Step 7	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius myservergroup2`	Configures the second, redundant RADIUS server.
Step 8	**server** *ip-address* [**auth** *auth-port*] [**acct** *acct-port*] **Example:** `Router(config-sg-radius)# server 1.2.3.5 [auth 1645] [acct 1646]`	Configures the IP address of the second RADIUS server for the group server.
Step 9	Repeat Step 8 to configure additional RADIUS servers.	

	Command or Action	Purpose
Step 10	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits server group RADIUS configuration mode.
Step 11	**aaa accounting network ssg_broadcast_accounting start-stop broadcast group** *group-name* **group** *group-name* **Example:** `Router(config)# aaa accounting network ssg_broadcast_accounting start-stop broadcast group myservergroup1 group myservergroup2`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. • **ssg_broadcast_accounting**—Configures the broadcast group. • **start-stop**—Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server. • **broadcast**—Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. • **group** *group-name*—Uses a subset of RADIUS servers for accounting as defined by the **server group** *group-name* command.

Configuring New Timers

During the lifetime of an SSG RADIUS proxy session, SSG expects to receive certain external events which are required for the session to continue. For example, SSG may require to receive the IP address of the session via a RADIUS Accounting-Start from the client device. Whilst SSG is waiting for such external events, internal timers are running. If these timers expire then the RADIUS proxy session is terminated. These commands are used to modify the default values of these timers. The timers applicable to the RADIUS Proxy for CDMA2000 feature are as follows:

- **hand-off**
  During all types of hand offs the existing accounting session is terminated and a new session started. This timer is started on reception of the RADIUS Accounting-Stop which terminates the original session, and is stopped on reception of the RADIUS Accounting-Start signalling the new accounting session.
- **ip-address**
  This timer runs whilst SSG is waiting to receive an IP-Address for a session, via a RADIUS Accounting-Start from the client device.
- **msid**
  This timer runs during Mobile IP setup, when SSG is waiting to receive the MSID from the PDSN/FA.

In addition to these timers, an idle timer may also be configured for RADIUS proxy sessions. This specifies the maximum period a session is allowed to remain idle (i.e. no data traffic received) before it is terminated.

To configure the SSG RADIUS Proxy timers, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **ssg enable**
5. **ssg proxy-radius**
6. **server-port** [**auth** *auth-port*][**acct** *acct-port*]
7. **timeouts**
8. **hand-off** *timeout*
9. **idle** *timeout*
10. **ip-address** *timeout*
11. **msid** *timeout* **retry** *retries*

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	**ip cef** **Example:** `Router(config)# ip cef`	Enables Cisco Express Forwarding (CEF).
Step 4	**ssg enable** **Example:** `Router(config)# ssg enable`	Enables SSG.
Step 5	**ssg proxy-radius** **Example:** `Router(config)# ssg proxy-radius`	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.

	Command or Action	Purpose
Step 6	**server-port** [**auth** *auth-port*][**acct** *acct-port*] **Example:** `Router(config-radius-proxy)# server-port [auth 1645][acct 1646]`	Configures the authentication and accounting ports. • **auth**—(Optional) Configures the authentication port. • *auth-port*—(Optional) Specifies the authentication port number. The default authentication port is 1645. The valid range is 0 to 65535. • **acct**—(Optional) Configures the accounting port. • *acct-port*—(Optional) Specifies the accounting port number. The default accounting port is 1646. The valid range is 0 to 65535.
Step 7	**timeouts** **Example:** `Router(config-radius-proxy)# timeouts`	Enters SSG-radius-proxy-timeouts mode.
Step 8	**hand-off** *timeout* **Example:** `Router(config-radproxy-timer)# hand-off 30`	Configures the RADIUS proxy hand off timeout. Valid range is 1 to 30 seconds.
Step 9	**idle** *timeout* **Example:** `Router(config-radproxy-timer)# idle 150`	Configures a host object timeout value. Valid range is 30 to 65536 seconds.
Step 10	**ip-address** *timeout* **Example:** `Router(config-radproxy-timer)# ip-address 25`	Configures an SSG RADIUS proxy IP address timeout. Valid range is 1 to 30 seconds.
Step 11	**msid** *timeout* **retry** *retries* **Example:** `Router(config-radproxy-timer)# msid 4 retry 9`	Configures the SSG RADIUS proxy mobile station ID (MSID) timeout. Valid range is 1 to 5 seconds. • *timeout*—Timeout value, in seconds. Valid range is 1 to 5 seconds. The default is 1 second. • **retry** *retries*—Specifies the maximum number of times the MSID timer is restarted before SSG assumes it is not going to receive an MSID from the PDSN. Valid range is 1 to 20 retries. The default is 10 retries.

Configuring Session Identification Attributes

By default, SSG selects the attribute used for session identification based on the type of client device. SSG assigns the 3GPP2-Correlation-ID attribute for PDSNs, Accounting-Session-ID attribute for HAs, and Calling-Station-ID attribute for non-CDMA2000 devices. You can override this automatic selection by using the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **ssg enable**
5. **ssg proxy-radius**
6. **client-address** [*ip-address*]
7. **key** [*secret*]
8. **session-identifier** {**auto** | **msid** | **correlation-id** | **accounting-session-id** | **ip** | **username**}
9. **remove vsa** {**3gpp2** | **cisco**}

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	`ip cef`
	
	Example:
	`Router(config)# ip cef`
		Enables CEF.

Step 4	`ssg enable`
	
	Example:
	`Router(config)# ssg enable`
		Enables SSG.

Step 5	`ssg proxy-radius`
	
	Example:
	`Router(config)# ssg proxy-radius`
		Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.

	Command or Action	Purpose
Step 6	**client-address** *ip-address* **Example:** Router(config-radius-proxy)# **client-address** *1.2.3.6*	Configures the RADIUS-client to proxy requests from the specified IP address to the RADIUS server and enters SSG-radius-proxy-Client mode.
Step 7	**key** *secret* **Example:** Router(config-radproxy-client)# **key** *mypassword*	(Optional) Configures the shared secret between SSG and the RADIUS client. The *secret* attribute describes the shared secret.
Step 8	**session-identifier** {**auto** | **msid** | **correlation-id** | **accounting-session-id** | **ip** | **username**} **Example:** Router(config-radproxy-client)# **session-identifier auto** Router(config-radproxy-client)# **session-identifier msid** Router(config-radproxy-client)# **session-identifier correlation-id** Router(config-radproxy-client)# **session-identifier accounting-session-id** Router(config-radproxy-client)# **session-identifier username**	(Optional) Overrides SSG's automatic RADIUS client session identification. • **auto**—Automatically determines the session identifier. • **msid**—Uses the MSID as the client session identifier. • **correlation-id**—Uses the Correlation-ID as the session identifier. • **accounting-session-id**—Uses the Accounting-Session-ID as the session identifier. • **ip**—Specifies the user IP address as the session identifier. • **username**—Specifies the username as the session identifier.
Step 9	**remove vsa** {**3gpp2** | **cisco**} **Example:** Router(config-radproxy-client)# **remove vsa 3gpp2** Router(config-radproxy-client)# **remove vsa cisco**	(Optional) Removes a VSA for a RADIUS client. • **3gpp2**—Removes all 3GPP2 VSAs. • **cisco**—Removes all Cisco VSAs.

Configuring Home Agent IP Addresses

SSG supports dynamic assignment of the Home Agent IP address using these commands. The HA IP address will only be dynamically assigned for sessions from a domain configured using these commands, where the domain is derived from the structured username of the session. The actual HA IP address assigned may be configured globally (i.e. the same for all recognized domains) or on a per-domain basis. To configure Home Agent domain names and Home Agent IP addresses, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip cef**
4. **ssg enable**
5. **ssg proxy-radius**
6. **home-agent address** [*ip-address*]
7. **home-agent domain** [*domain-name*] **address** [*ip-address*]

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	**ip cef** **Example:** `Router(config)# ip cef`	Enables CEF.
Step 4	**ssg enable** **Example:** `Router(config)# ssg enable`	Enables SSG.
Step 5	**ssg proxy-radius** **Example:** `Router(config)# ssg proxy-radius`	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
Step 6	**home-agent address** *ip-address* **Example:** `Router(config-radius-proxy)# home-agent address 1.2.3.7`	Configures an IP address for a Home Agent in a CDMA2000 network.
Step 7	**home-agent domain** *domain-name* [**address** *ip-address*] **Example:** `Router(config-radius-proxy)# home-agent domain mydomain.com address 1.2.3.8`	Configures a domain for a Home Agent in a CDMA2000 network. Optionally configures an IP address for the domain.

Verifying SSG Proxy for CDMA2000

To verify SSG Proxy for CDMA2000, enter the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show running-config**
4. **show ssg host** [*ip-address*]

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	**show running-config** **Example:** `Router# show running-config`	Displays the current configuration.
Step 4	**show ssg host** [*ip-address*] **Example:** `Router# show ssg host 10.0.0.0`	Displays information about a subscriber and current connections of the subscriber.

Examples

To verify SSG Proxy for CDMA2000, enter the following commands:

Step 1 Enter the **show running-config** command.

```
Router# show running-config

.
.
.
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname host1
```

```
!
aaa new-model
!
aaa group server radius OPERATIONS
 server 10.10.50.181 auth-port 1645 acct-port 1646
!
aaa group server radius RASCUSTOMER
 server 10.10.50.180 auth-port 1645 acct-port 1646
!
aaa authentication login vty line
aaa authentication ppp default local group radius
aaa authorization exec vty none
aaa authorization network default local group radius none
aaa authorization network ssg_aaa_author_internal_list none
aaa accounting update periodic 1
aaa accounting network ssg_broadcast_accounting start-stop broadcast group OPERATIONS
group RASCUSTOMER
aaa nas port extended
aaa session-id common
enable password password1
!
username cisco password 0 cisco
redundancy
 main-cpu
  auto-sync standard
 no secondary console enable
!
ip subnet-zero
ip cef
no ip domain-lookup
!
ip dhcp-client network-discovery informs 2 discovers 2 period 15
vpdn enable
vpdn search-order domain
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-mac 1000
 pppoe limit per-vc 1000
!
vpdn-group 3
 request-dialin
  protocol l2tp
  domain tunsvc
  domain banking
 local name dial-tunnel
!
!
!
ssg enable
ssg default-network 10.0.48.0 255.255.255.0
ssg service-password servicecisco
ssg radius-helper auth-port 1812 acct-port 1813
ssg radius-helper key cisco
ssg maxservice 12
ssg accounting interval 300000
ssg bind service vidconf ATM0/0/0.159
ssg bind service banking ATM0/0/0.156
ssg bind service internet-red ATM0/0/0.152
ssg bind service games ATM0/0/0.155
ssg bind service corporate ATM0/0/0.154
ssg bind service shop ATM0/0/0.158
```

```
ssg bind service distlearn ATM0/0/0.157
ssg bind service internet-green ATM0/0/0.153
ssg bind service iptv ATM0/0/0.160
ssg bind service internet-blue ATM0/0/0.151
ssg bind direction downlink Ethernet0/0/0
ssg bind direction downlink FastEthernet0/0/0
!
ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 10.0.48.3
  key cisco
 !
 client-address 10.0.48.4
  key cisco
 !
 timeouts
  idle 60000
 !
 address-pool 77.77.77.77 77.77.77.88 domain msid3.access
 address-pool 88.88.88.88 88.88.88.99 domain corporate3
 address-pool 99.99.99.99 99.99.99.111 domain nat-test
 address-pool 66.66.66.66 66.66.66.77 domain corporate
 home-agent address 4.3.2.1
!
ssg auto-domain
 exclude apn corporate
 exclude apn corporate3
!
local-profile local1
  attribute 26 9 251 "D192.1.1.1"
.
.
.
radius-server host 10.0.48.3 auth-port 1812 acct-port 1813 key troy
radius-server host 10.10.50.181 auth-port 1645 acct-port 1646
radius-server host 10.10.50.180 auth-port 1645 acct-port 1646
radius-server retransmit 3
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 key troy
radius-server vsa send accounting
radius-server vsa send authentication
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
 login authentication vty
!
end
```

Step 2 Enter the **show ssg host** command to view information about a host object including client device type. The following output shows host object information for Simple IP:

```
Router# show ssg host 10.0.0.0

----------------------- HostObject Content -----------------------
Activated: TRUE
Interface:
```

```
User Name: user1
Host IP: 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
```

The following output shows host object information for Mobile IP:

```
Router# show ssg host 10.0.0.101

----------------------- HostObject Content -----------------------
Activated: TRUE
Interface:
User Name: user1
Host IP: 10.0.0.101
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
```

Configuration Examples for SSG Proxy for CDMA2000

Configuring Multiple RADIUS Server Support: Example

The following example shows how to configure multiple RADIUS servers in a CDMA2000 network. Configuring multiple RADIUS servers provides geographical redundancy by sending copies of host object accounting packets to multiple RADIUS servers.

```
aaa group server radius billing
 server 10.0.0.1 auth-port 1812 acct-port 1813
 end
!
aaa server group server radius hotstandby
 server 10.0.0.2 auth-port 1813 acct-port 1813
 end
!
aaa accounting network ssg_broadcast_accounting start-stop broadcast group billing group
hotstandby
```

Configuring New Timers: Examples

The following example shows how to enable SSG RADIUS Proxy and to configure a hand off timeout of 25 seconds:

```
ip cef
ssg enable
ssg proxy-radius
 server-port auth 1812 acct 1813
 hand-off 25
```

The following example shows how to enable SSG RADIUS Proxy and to configure an idle timeout of 60 seconds:

```
ip cef
ssg enable
ssg proxy-radius
 server-port auth 1812 acct 1813
 idle 60
```

The following example shows how to enable SSG RADIUS Proxy and to configure an IP address timeout of 10 seconds:

```
ip cef
ssg enable
ssg proxy-radius
 server-port auth 1812 acct 1813
 ip-address 60
```

The following example shows how to enable SSG RADIUS Proxy and to configure an MSID timeout of 3 seconds:

```
ip cef
ssg enable
ssg proxy-radius
 server-port auth 1812 acct 1813
 msid 3 retry 3
```

Configuring Session Identification Attributes: Examples

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

```
ip cef
ssg enable
ssg proxy-radius
 client-address 172.16.0.0
 key cisco
 session-identifier msid
```

The following example shows how to configure SSG to identify the specified client session based on the 3GPP2-Correlation-ID attribute:

```
ssg enable
ssg proxy-radius
 client-address 172.16.0.0
 key cisco
 session-identifier correlation-id
```

The following example shows how to configure SSG to identify the specified client session based on the Accounting-Session-ID attribute:

```
ssg enable
ssg proxy-radius
 client-address 172.16.0.0
 key cisco
 session-identifier accounting-session-id
```

Configuring Home Agent IP Addresses: Example

The following example shows how to configure a Home Agent with IP address 172.16.0.0 and with a domain name of “hadomain1”.

```
ip cef
ssg enable
ssg proxy-radius
 home-agent address 172.16.0.0
 home-agent domain hadomain1
```

Removing VSA Types: Examples

The following example shows how to remove all Cisco VSAs from a RADIUS response sent to a RADIUS client:

```
ssg enable
ssg proxy-radius
 client-address 172.16.0.0
 remove vsa cisco
```

The following example shows how to remove all 3GPP2 VSAs from a RADIUS response sent to a RADIUS client:

```
ssg enable
ssg proxy-radius
 client-address 172.16.0.0
  remove vsa 3gpp2
```

Additional References

The following sections provide references related to SSG Proxy for CDMA2000.

Related Documents

Related Topic	Document Title
CMDA and CMDA2000	"CDMA Overview" and "CDMA2000 Overview" on the Mobile Wireless Knowledge Bytes web page: http://www.cisco.com/warp/public/779/servpro/solutions/wireless_mobile/training.html
Cisco IOS voice, video and fax commands	*Cisco IOS Voice, Video, and Fax Command Reference*
Cisco IOS voice, video and fax configuration	*Cisco IOS Voice, Video, and Fax Configuration Guide*
SSG AutoLogon Using Proxy Radius	*SSG AutoLogon Using Proxy Radius*
SSG Prepaid	*SSG Prepaid*
SSG Service Profile Caching	*SSG Service Profile Caching*
SSG TCP Redirect for Services	*SSG TCP Redirect for Services*

Standards

Standards	Title
CDMA IS-95	CDMA One standard
TIA/EIA/IS-835,	CDMA2000 Wireless IP Network Standard
ANSI/TIA/EIA-41	Cellular Radio telecommunications Intersystem Operations

MIBs

MIBs	MIBs Link
SNMP MIB	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

RFCs	Title
No new or modified RFCs are supported by this feature. Support for existing RFCs has not been modifued by this feature.	

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents the following new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3T command reference publications.

client-address

To configure a RADIUS client to proxy requests from the specified IP address to the RADIUS server and to enter SSG-radius-proxy-client mode, use the **client-address** command in SSG-radius-proxy mode. To remove a client from the client list, use the **no** form of this command.

client-address *ip-address* [**key** *secret*]

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

Syntax Description

ip-address	IP address of a RADIUS client.
key	(Optional) Shared secret between SSG and the RADIUS client.
secret	(Optional) Description of the shared secret.

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(15)B	This command was enhanced to enter SSG-radius-proxy-Client mode. The **key** keyword and the *secret* attribute were made optional.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use this command to configure the RADIUS client to proxy requests from the specified IP address to the RADIUS server. You can also use this command to enter SSG-radius-proxy-client mode.

From SSG-radius-proxy-client mode, use the **key** keyword and the *secret* attribute to configure the shared secret between SSG and the RADIUS client. Use the *secret* attribute to configure each client IP with a unique shared secret. This shared secret should be the same one configured on the RADIUS client.

Examples

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

```
client-address 172.16.0.0
```

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

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

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

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

Related Commands

Command	Description
address-pool	Defines local IP pools to be used by SSG to assign IP addresses to users for which SSG is acting as a RADIUS client.
clear ssg radius-proxy client-address	Clears all hosts connected to a specific RADIUS client.
key (SSG-radius-proxy-client)	Configures the shared secret between SSG and a RADIUS client.
session-identifier	Overrides SSG's automatic RADIUS client session identification.
show ssg radius-proxy	Displays the pool of IP addresses configured for a router or for a specific domain.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.

hand-off

To configure a Service Selection Gateway (SSG) RADIUS proxy hand off timeout, use the **hand-off** command in SSG-radius-proxy-timers configuration mode. To disable the hand-off timeout, use the **no** form of this command.

hand-off *timeout*

no hand-off *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is 1 to 30 seconds. The default is 5 seconds.

Defaults

The hand off timeout is set to 5 seconds.

Command Modes

SSG-radius-proxy-timers

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.

Usage Guidelines

Use this command to configure an SSG RADIUS proxy hand off timeout. You can use this command when a PPP session is not disabled and the host object remains active after a base station controller (BSC) hand off.

A Session-Continue vendor specific attribute (VSA) with a value of 1 in an Accounting-Stop packet indicates that a BSC/packet control function (PCF) hand off is in progress. When SSG detects the BSC/PCF hand off, it keeps the host object and begins the configured hand off timeout. If SSG does not receive an Accounting-Start for this host object before the hand off timeout expires, it deletes the host object.

Examples

The following example shows how to configure a hand off timeout value of 25 seconds:

```
ssg radius-proxy
 ssg timeouts
 hand-off 25
```

Related Commands

Command	Description
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.

Command	Description
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timeouts mode.

home-agent (SSG-radius-proxy)

To configure an IP address or domain for a Home Agent (HA) in a CDMA2000 network, use the **home-agent** command in SSG-radius-proxy configuration mode. To remove an HA address or domain, use the **no** form of this command.

home-agent {**address** *ip-address* | **domain** *domain-name* [**address** *ip-address*]}

no home-agent {**address** *ip-address* | **domain** *domain-name* [**address** *ip-address*]}

Syntax Description

address *ip-address*	IP address of the local Home Agent.
domain *domain-name*	Domain of the local Home Agent.
address *ip-address*	(Optional) IP address of the domain of the Home Agent.

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy

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.

Usage Guidelines

Use the **home-agent** command to configure a list of domain names for which dynamic Home Agent (HA) IP address assignment is applicable. You can configure each domain name with an HA address. You should also configure the IP address of a default local HA.

Use the **no home-agent address** command to remove any configured domain names. Use the **no home-agent domain** command to remove an entry for a specified domain.

SSG determines that an Access-Request packet is for a new Mobile IP session when it receives a 3GPP2-Home-Agent-Attribute VSA with a value of 0.0.0.0. For authenticated users with a domain recognized by SSG that has a preconfigured HA address, the 3GPP2-Home-Agent-Attribute is changed to the per-domain HA address. For authenticated users with a domain recognized by SSG that does not have a preconfigured HA address, the 3GPP2-Home-Agent-Attribute is changed to the IP address of the default local HA.

For authenticated users with a domain that is not recognized by SSG, the 3GPP2-Home-Agent-Attribute is not changed.

Examples

The following example shows how to set the IP address of the default local HA to 172.16.0.0:

```
ssg radius-proxy
 home-agent address 172.16.0.0
```

The following example shows how to set the IP address of the HA to 172.16.0.0, for users in domain "home1.com":

```
ssg radius-proxy
 home-agent domain home1.com address 172.16.0.0
```

Related Commands

Command	Description
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.

idle (SSG-radius-proxy-timers)

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

idle *timeout*

no idle *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is 30 to 65536 seconds. There is no default value.

Defaults

No idle timeout value is configured.

Command Modes

SSG-radius-proxy-timers

Command History

Release	Modification
12.2(15)B	This command was introduced to replace the **idle-timeout** command.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

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

Note Timeout values configured in the user profile that appears in the Access-Accept take precedence over any timeout value configured by the **timeouts (SSG-radius-proxy)** command.

Note This command replaces the **idle-timeout** command in SSG-radius-proxy configuration mode.

Examples

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

```
ssg radius-proxy
 ssg timeouts
 idle 60
```

Related Commands

Command	Description
hand-off	Configures an SSG RADIUS proxy hand off timeout.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

ip-address (SSG-radius-proxy-timers)

To configure a Service Selection Gateway (SSG) RADIUS proxy IP address timeout, use the **ip-address** command in SSG-radius-proxy-timers configuration mode. To disable the IP address timeout, use the **no** form of this command.

ip-address *timeout*

no ip-address *timeout*

Syntax Description

timeout	Timeout value, in seconds. Valid range is 1 to 30 seconds. The default is 5 seconds.

Defaults

The default value of this timeout is 5 seconds.

Command Modes

SSG-radius-proxy-timers

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.

Usage Guidelines

Use this command to configure an SSG RADIUS proxy IP address timeout.

If SSG, acting as a RADIUS proxy for a client, does not allocate an IP address in the Access-Accept, a dormant host object is created. The dormant host object is not activated until SSG receives an Accounting-Start packet from the client device, containing a valid IP address.

When an IP address timeout is configured, SSG starts this timer on creation of the dormant host object. If a valid IP address is not received via an Accounting-Start packet from the client device, prior to the expiration of this timeout, the dormant host object is destroyed.

Examples

The following example shows how to configure an SSG RADIUS proxy IP address timeout of 10 seconds:

```
ssg radius-proxy
 ssg timeouts
 ip-address 10
```

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.
hand-off	Configures an SSG RADIUS proxy hand off timeout.

Command	Description
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

key (SSG-radius-proxy-client)

To configure a shared secret between the Service Selection Gateway (SSG) and a RADIUS client, use the **key** command in SSG-radius-proxy-client mode. To deconfigure the shared secret, use the **no** form of this command.

key *secret*

no key *secret*

Syntax Description

secret	Description of the shared secret.

Defaults

No default behavior or values.

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.

Usage Guidelines

Use this command to configure a shared secret between SSG and a RADIUS client. Use the *secret* attribute to configure each client IP with a unique shared secret. This shared secret should be the same one that is configured on the RADIUS client.

Note The **key** command in SSG-radius-proxy-client mode replaces the **client-address key** command in SSG-radius-proxy mode.

Examples

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

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

Related Commands

Command	Description
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.

msid (SSG-radius-proxy-timers)

To configure a Service Selection Gateway (SSG) RADIUS proxy mobile station ID (MSID) timeout, use the **msid** command in SSG-radius-proxy-timers configuration mode. To disable the MSID timeout, use the **no** form of this command.

msid *timeout* **retry** *retries*

no msid *timeout* **retry** *retries*

Syntax Description

timeout	Timeout value in seconds. Valid range is 1 to 5 seconds. The default is 1 second.
retry *retries*	Maximum number of retries. Valid range is 1 to 20 retries. The default is 10 retries.

Defaults

The default value of this timeout is 1 second, with a default retry count of 10.

Command Modes

SSG-radius-proxy-timers.

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.

Usage Guidelines

Use this command to configure an MSID timeout.

Configure the MSID timer to associate an MSID to the host object for a Mobile IP connection. The MSID is associated with a host object only after SSG receives the Accounting-Start packets from the Packet Data Serving Node (PDSN)/Foreign Agent (FA) and the Home Agent (HA). The host object address is not assigned until SSG receives the Accounting-Start packet from the HA. If the Accounting-Start packet from the PDSN/FA arrives before the Accounting-Start packet from the HA, the host object cannot be located, and the MSID is not associated with the host object. When this occurs, the retry timer is started. When the retry timer expires, the MSID is associated with the host object.

If SSG does not receive the Account-Start packet with the correct MSID from the PDSN before the timeout expires, the host object is removed.

Examples

The following example shows how to configure an SSG RADIUS proxy MSID timeout of 3 seconds with 5 retries:

```
ssg radius-proxy
 ssg timeouts
 msid 3 retry 5
```

Related Commands

Command	Description
hand-off	Configures an SSG RADIUS proxy hand off timeout.
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.
timeouts (SSG-radius-proxy)	Enters SSG-radius-proxy-timers mode.

remove vsa

To allow all 3GPP2 vendor specific attributes (VSAs) or all Cisco VSAs from Access-Accept packets proxied from a AAA server to a RADIUS client to be removed, use the **remove vsa** command in SSG-radius-proxy-client mode. To enable all 3GPP2 VSAs or Cisco VSAs to be passed transparently, use the **no** form of this command.

remove vsa {**3gpp2** | **cisco**}

no remove vsa {**3gpp2** | **cisco**}

Syntax Description

3gpp2	Removes all Third Generation Partnership Project 2 (3GPP2) VSAs.
cisco	Removes all Cisco VSAs.

Defaults

By default, SSG removes all Cisco VSAs from Access-Accept packets proxied from the AAA server to the client device. All 3GPP2 VSAs are, by default, passed transparently.

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.

Usage Guidelines

Use this command to remove all 3GPP2 VSAs or Cisco VSAs from a RADIUS client.

By default, SSG removes all Cisco VSAs from Access-Accept packets proxied from the AAA server to the client device. This is because the client device is unlikely to understand the VSAs, and their presence may cause interoperation difficulties. The "no remove vsa cisco" command may be used to allow these attributes to be passed transparently.

You can use this command to remove all 3GPP2 VSAs in addition to Cisco VSAs by using the **3gpp2** keyword. 3GPP2 VSAs are not filtered by default, whereas Cisco VSAs are filtered by default. SSG VSAs (a subset of Cisco VSAs) are always removed, irrespective of any configuration.

Examples

The following example shows how to remove all 3GPP2 VSAs from an Accept-Accept packet proxied from the AAA server to the client device:

```
remove vsa 3gpp2
```

The following example shows how to transparently pass all Cisco VSAs in an Accept-Accept packet proxied from the AAA server to the client device:

```
remove vsa cisco
```

```
no remove vsa cisco
```

Related Commands

Command	Description
client-address	Configures a RADIUS client to proxy requests from the specified IP address to a RADIUS server and enters SSG-radius-proxy-client mode.

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 [**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.

Defaults

SSG selects the attribute used for session identification based on 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.

Usage Guidelines

By default, SSG automatically selects the attribute to use for session identification based on 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, 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.

timeouts (SSG-radius-proxy)

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

timeouts

no timeouts

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

SSG-radius-proxy configuration

Command History

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

Usage Guidelines

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

Examples

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

```
ssg radius-proxy
 ssg radius-proxy timeouts
```

Related Commands

Command	Description
hand-off	Configures an SSG RADIUS proxy hand off timeout.
idle (SSG-radius-proxy-timers)	Configures a host object timeout value.
ip-address (SSG-radius-proxy-timers)	Configures an SSG RADIUS proxy IP address timeout.
key (SSG-radius-proxy-client)	Configures a shared secret between SSG and a RADIUS client.
ssg radius-proxy	Enables SSG RADIUS Proxy and enters SSG-radius-proxy mode.

debug ssg ctrl-errors

To display all error messages for control modules, use the **debug ssg ctrl-errors** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ssg ctrl-errors

no debug ssg ctrl-errors

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled by default

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)DC	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use this command to show error messages for the control modules.These modules include all those that manage the user authentication and service login and logout (RADIUS, PPP, Subblock, and Accounting). An error message is the result of an error detected during normal execution.

Examples

The following example shows how output is generated by using the **debug ssg ctrl-errors** command when a host logs into and logs out from a service:

```
Router# debug ssg ctrl-errors

Mar 29 13:51:30 [192.168.5.1.15.21] 59:00:15:38:%VPDN-6-AUTHORERR:L2F NAS
LowSlot6 cannot locate a AAA server for Vi6 user User1
Mar 29 13:51:31 [192.168.5.1.15.21] 60:00:15:39:%LINEPROTO-5-UPDOWN:Line
protocol on Interface Virtual-Access6, changed state to down
```

Related Commands

Command	Description
debug radius	Displays information associated with RADIUS.
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.

debug ssg ctrl-events

To display all event messages for control modules, use the **debug ssg ctrl-events** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ssg ctrl-events

no debug debug ssg ctrl-events

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled by default

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)DC	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

This command displays event messages for the control modules, which include all modules that manage the user authentication and service login and logout (RADIUS, PPP, Subblock, and Accounting). An event message is an informational message generated during normal execution.

Examples

The following example shows how output is generated by the **debug ssg ctrl-events** command when a host logs in to a service:

```
Router# debug ssg ctrl-events
Mar 16 16:20:30 [192.168.6.1.7.141] 799:02:26:51:SSG-CTL-EVN:Service logon is accepted.
Mar 16 16:20:30 [192.168.6.1.7.141] 800:02:26:51:SSG-CTL-EVN:Send cmd 11 to host
172.16.6.13. dst=192.168.100.24:36613
```

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-packet	Displays packet contents handled by control modules.
debug ssg data	Displays all data-path packets.

debug ssg ctrl-packets

To display packet contents handled by control modules, use the **debug ssg ctrl-packets** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ssg ctrl-packets

no debug ssg ctrl-packets

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)DC	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use this command to show packet messages for the control modules. These modules include all those that manage the user authentication and service login and logout (RADIUS, PPP, Subblock, and Accounting). A packet message displays the contents of a package.

Examples

The following example shows how output is generated by using the **debug ssg ctrl-packet** command when a host logs out of a service:

```
Router# debug ssg ctrl-packets

Mar 16 16:23:38 [192.168.6.1.7.141] 968:02:30:00:SSG-CTL-PAK:Received Packet:
Mar 16 16:23:38 [192.168.6.1.7.141] 980:02:30:00:SSG-CTL-PAK:Sent packet:
Mar 16 16:23:39 [192.168.6.1.7.141] 991:02:30:00:SSG-CTL-PAK:
Mar 16 16:23:39 [192.168.6.1.7.141] 992:Received Packet:
```

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 data	Displays all data-path packets.

debug ssg data

To display all data-path packets, use the **debug ssg data** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ssg data

no debug ssg data

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled by default

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)DC	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

The **debug ssg data** command shows packets for the data modules. These modules include all those that forward data packets (Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), tunneling, fast switching, IP stream, and multicast).

Examples

This example shows how output is generated by using the **debug ssg data** command when a host logs into and out of a service:

```
router# debug ssg data
Mar 29 13:45:16 [192.168.5.1.15.21] 45:00:09:24:
SSG-DATA:PS-UP-SetPakOutput=1(Vi6:172.16.5.50->199.199.199.199)
Mar 29 13:45:16 [192.168.5.1.15.21] 46:00:09:24:
SSG-DATA:PS-DN-SetPakOutput=1(Fa0/0/0:171.69.2.132->172.16.5.50)
Mar 29 13:45:16 [192.168.5.1.15.21] 47:00:09:24:
SSG-DATA:FS-UP-SetPakOutput=1(Vi6:172.16.5.50->171.69.43.34)
Mar 29 13:45:16 [192.168.5.1.15.21] 48:00:09:24:
```

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 radius

To display information associated with RADIUS, use the **debug radius** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug radius [**brief** | **hex**]

no debug radius [**brief** | **hex**]

Syntax Description

brief	(Optional) Displays abbreviated debug output.
hex	(Optional) Displays debugging output in hexadecimal notation.

Defaults

Debugging output in ASCII format is enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(1)T	This command was introduced.
12.2(11)T	The **brief** and **hex** keywords were added. The default output format became ASCII rather than hexadecimal.

Usage Guidelines

RADIUS is a distributed security system that secures networks against unauthorized access. Cisco supports RADIUS under the authentication, authorization, and accounting (AAA) security system. When RADIUS is used on a router, you can use the **debug radius** command to display detailed debugging and troubleshooting information in ASCII format. Use the **debug radius brief** command for abbreviated output displaying client/server interaction and minimum packet information. Use the **debug radius hex** command to display packet dump information that has not been truncated in hex format.

Examples

The following is sample output from the debug radius command:

```
Router# debug radius

Radius protocol debugging is on
Radius packet hex dump debugging is off
Router#
00:02:50: RADIUS: ustruct sharecount=3
00:02:50: Radius: radius_port_info() success=0 radius_nas_port=1
00:02:50: RADIUS: Initial Transmit ISDN 0:D:23 id 0 10.0.0.1:1824, Accounting-Request, len
358
00:02:50: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:02:50: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:02:50: RADIUS:  NAS-Port-Type       [61]  6   Async
00:02:50: RADIUS:  User-Name           [1]   12  "4085554206"
00:02:50: RADIUS:  Called-Station-Id   [30]  7   "52981"
00:02:50: RADIUS:  Calling-Station-Id  [31]  12  "4085554206"
00:02:50: RADIUS:  Acct-Status-Type    [40]  6   Start
```

```
00:02:50: RADIUS:  Service-Type        [6]   6   Login
00:02:50: RADIUS:  Vendor, Cisco       [26]  27  VT=33 TL=21 h323-gw-id=5300_43.
00:02:50: RADIUS:  Vendor, Cisco       [26]  55  VT=01 TL=49
h323-incoming-conf-id=8F3A3163 B4980003 0 29BD0
00:02:50: RADIUS:  Vendor, Cisco       [26]  31  VT=26 TL=25 h323-call-origin=answer
00:02:50: RADIUS:  Vendor, Cisco       [26]  32  VT=27 TL=26 h323-call-type=Telephony
00:02:50: RADIUS:  Vendor, Cisco      [26]  57  VT=25 TL=51 h323-setup-time=*16:02:48.681
PST Fri Dec 31 1999
00:02:50: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:02:50: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:02:50: RADIUS:  Delay-Time          [41]  6   0
00:02:51: RADIUS: Received from id 0 1.7.157.1:1824, Accounting-response, len 20
00:02:51: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
00:03:01: RADIUS: ustruct sharecount=3
00:03:01: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:01: RADIUS: Initial Transmit ISDN 0:D:23 id 1 1.7.157.1:1823, Access-Request, len
171
00:03:01: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:03:01: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:03:01: RADIUS:  NAS-Port-Type       [61]  6   Async
00:03:01: RADIUS:  User-Name           [1]   8   "123456"
00:03:01: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:03:01: RADIUS:  Calling-Station-Id  [31]  12  "4085554206"
00:03:01: RADIUS:  User-Password       [2]   18  *
00:03:01: RADIUS:  Vendor, Cisco       [26]  36  VT=01 TL=30 h323-ivr-out=transactionID:0
00:03:01: RADIUS: Received from id 1 1.7.157.1:1823, Access-Accept, len 115
00:03:01: RADIUS:  Service-Type        [6]   6   Login
00:03:01: RADIUS:  Vendor, Cisco       [26]  29  VT=101 TL=23 h323-credit-amount=45
00:03:01: RADIUS:  Vendor, Cisco       [26]  27  VT=102 TL=21 h323-credit-time=33
00:03:01: RADIUS:  Vendor, Cisco       [26]  26  VT=103 TL=20 h323-return-code=0
00:03:01: RADIUS:  Class               [25]  7   6C6F63616C
00:03:01: RADIUS: saved authorization data for user 62321E14 at 6233D258
00:03:13: %ISDN-6-DISCONNECT: Interface Serial0:22  disconnected from 4085274206, call
lasted 22 seconds
00:03:13: RADIUS: ustruct sharecount=2
00:03:13: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:13: RADIUS: Sent class "local" at 6233D2C4 from user 62321E14
00:03:13: RADIUS: Initial Transmit ISDN 0:D:23 id 2 1.7.157.1:1824, Accounting-Request,
len 775
00:03:13: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:03:13: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:03:13: RADIUS:  NAS-Port-Type       [61]  6   Async
00:03:13: RADIUS:  User-Name           [1]   8   "123456"
00:03:13: RADIUS:  Called-Station-Id   [30]  7   "52981"
00:03:13: RADIUS:  Calling-Station-Id  [31]  12  "4085274206"
00:03:13: RADIUS:  Acct-Status-Type    [40]  6   Stop
00:03:13: RADIUS:  Class               [25]  7   6C6F63616C
00:03:13: RADIUS:  Undebuggable        [45]  6   00000001
00:03:13: RADIUS:  Service-Type        [6]   6   Login
00:03:13: RADIUS:  Vendor, Cisco       [26]  27  VT=33 TL=21 h323-gw-id=5300_43.
00:03:13: RADIUS:  Vendor, Cisco       [26]  55  VT=01 TL=49
h323-incoming-conf-id=8F3A3163 B4980003 0 29BD0
00:03:13: RADIUS:  Vendor, Cisco       [26]  31  VT=26 TL=25 h323-call-origin=answer
00:03:13: RADIUS:  Vendor, Cisco       [26]  32  VT=27 TL=26 h323-call-type=Telephony
00:03:13: RADIUS:  Vendor, Cisco      [26]  57  VT=25 TL=51 h323-setup-time=*16:02:48.681
PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  59  VT=28 TL=53
h323-connect-time=*16:02:48.946 PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  62  VT=29 TL=56in=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  23  VT=01 TL=17 pre-bytes-out=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  21  VT=01 TL=15 pre-paks-in=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 pre-paks-out=0
```

```
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 nas-rx-speed=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 nas-tx-speed=0
00:03:13: RADIUS:  Delay-Time          [41]  6   0
00:03:13: RADIUS: Received from id 2 1.7.157.1:1824, Accounting-response, len 20
h323-disconnect-time=*16:03:11.306 PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  32  VT=30 TL=26 h323-disconnect-cause=10
00:03:13: RADIUS:  Vendor, Cisco       [26]  28  VT=31 TL=22 h323-voice-quality=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:03:13: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:03:13: RADIUS:  Acct-Input-Octets   [42]  6   0
00:03:13: RADIUS:  Acct-Output-Octets  [43]  6   88000
00:03:13: RADIUS:  Acct-Input-Packets  [47]  6   0
00:03:13: RADIUS:  Acct-Output-Packets [48]  6   550
00:03:13: RADIUS:  Acct-Session-Time   [46]  6   22
00:03:13: RADIUS:  Vendor, Cisco       [26]  30  VT=01 TL=24 subscriber=RegularLine
00:03:13: RADIUS:  Vendor, Cisco       [26]  35  VT=01 TL=29 h323-ivr-out=Tariff:Unknown
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 pre-bytes-
```

Related Commands

Command	Description
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.

show ssg connection

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)DC	This command was introduced.
12.2(2)B	The *interface* argument was added.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use the **show ssg connection** to display the connections of a given host and a service name.

Examples

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 autologon

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

Table 1 describes the significant fields shown in the display.

Table 1 show ssg connection Field Descriptions

Field	Description
User Name	The name of the user that owns this connection
Owner Host	The IP address of the user that owns this connection

Table 1 show ssg connection Field Descriptions (continued)

Field	Description
Associated Service	The name of the service the user is connected to
Connection State	Indicates status of connection ("UP", "PENDING", "DOWN", "AUTHENTICATED" or "FAILED")

Related Commands

Command	Description
show ssg host	Displays information about a subscriber and current connections of the subscriber.
show ssg radius-proxy	Displays a list of all RADIUS proxy clients, or details of a particular RADIUS proxy client.
show ssg service	Displays the information for a service.

show ssg service

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

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

Syntax Description

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*.

Defaults

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3) DC	This command was introduced on the Cisco 6400 node route processor.
12.1(1) DC1	The output of this command was modified on the Cisco 6400 node route processor to display the following Service-Info Attributes when they are present in the proxy RADIUS service profile: • Service-Defined Cookie • Full Username Attribute
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use this command to display connection information for a service.

Examples

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

```
Router# show ssg service serv1-proxy


----------------------- ServiceInfo Content ----------------------
Uplink IDB:FastEthernet0/0/0
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 2 describes the significant fields shown in the display.

Table 2 show ssg service Field Descriptions

Field	Description
Uplink IDB	The uplink interface that connects to the service
Name	The name of the service
Type	The service type. Can be PASS-THROUGH, PROXY or TUNNEL
Mode	The service mode. Can be CONCURRENT, SEQUENTIAL or EXCLUSIVE
Authentication Type	Type of authentication required. Can be PAP or CHAP

Related Commands

Command	Description
show ssg connection	Displays the connections of a given host and a service name.
show ssg host	Displays information about a subscriber and current connections of the subscriber.
show ssg radius-proxy	Displays a list of all RADIUS proxy clients, or details of a particular RADIUS proxy client.

show ssg host

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

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

Syntax Description

ip-address	(Optional) IP address of the host.
interface	(Optional) Interface through which the host is connected.
username	(Optional) Usernames logged into the active hosts.

Defaults

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(2)B	The *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 enhanced to display additional status information associated with a host object.
12.3(4)T	Enhancements were integrated into Cisco IOS Release 12.3(4)T

Examples

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
Host IP: 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
```

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:command example
```

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
```

The following example shows the *interface* argument being used 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 user


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

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

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
Host IP: 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
```

Table 3 describes the significant fields shown in the display.

Table 3 show ssg host Field Descriptions

Field	Description
Device:	Type of device. Device types can be HA, 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.

Related Commands

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

show ssg radius-proxy

To display a list of all RADIUS proxy clients, or 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*] [**address-pool** [**domain** *domain-name*] [**free** | **inuse**]]

Syntax Description

ip-address	(Optional) Details for the RADIUS proxy client at this IP address.
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.

Defaults

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(15)B	This command was enhanced to allow display of a list of RADIUS proxy clients.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

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        Device type     Users
10.0.48.3       PDSN             2
10.0.48.4       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
19.1.5.1
19.1.5.2
19.1.5.3
19.1.5.4
19.1.5.5
19.1.5.6
19.1.5.7
19.1.5.8
19.1.5.9
19.1.5.10
```

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

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

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

```
19.1.5.26
19.1.5.27
19.1.5.28
19.1.5.29
19.1.5.30
```

Table 4 describes the significant fields shown in the display.

Table 4 show ssg radius proxy Field Descriptions

Field	Description
Client IP	IP address of the client device
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	The 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 data	Displays all data-path packets.
debug ssg ctrl-event	Displays all event messages for control modules.
debut ssg ctrl-packet	Displays packet contents handled by control modules.
debug ssg-ctrl-errors	Displays all error messages for control modules.
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.

Glossary

3G—Third Generation.

3GPP2—Third Generation Partnership Project 2. A collaborative 3G telecommunications standards-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 Cellular Radiotelecommunication Intersystem Operations networks, and for radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41.

AAA—Authentication, Authorization and Accounting.

Access-Accept—Response packet from the RADIUS server notifying the access server that the user is authenticated. This packet contains the user profile, which defines the specific AAA functions assigned to the user.

Access-Request—Request packet sent to the RADIUS server by the access server requesting authentication of the user.

APN—Access Point Name. Identifies a PDN that is configured on and accessible from a GGSN in a GPRS network.

BSC—Base Station Controller. The part of the wireless system's infrastructure that controls one or multiple cell sites' radio signals, thus reducing the load on the switch. Performs radio signal management functions for base transceiver stations, managing functions such as frequency assignment and hand off.

CDMA—Code Division Multiple Access. A method of dividing a radio spectrum to be shared by multiple users through the assignment of unique codes. CDMA implements spread-spectrum transmission.

CDMA2000—The 3G technology that is an evolutionary outgrowth of CDMA.

CHAP—Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.

DHCP—Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

FA—Foreign Agent. A Mobile IP node that resides near the subscriber-side edge of a mobile server provider network.

GGSN—Gateway GPRS Support Node. A wireless gateway that allows mobile cell phone users to access the public data network (PDN) or specified private IP networks.

GPRS—General Packet Radio System. Service defined and standardized by the European Telecommunication Standards Institute (ETSI). GPRS is an IP packet-based data service for Global System for Mobile Communications (GSM) networks.

HA—Home Agent. A Mobile IP node that resides in the user’s home network and acts as the anchor point for Mobile IP signaling and data to provide seamless mobility.

ISP—Internet Service Provider. Company that provides Internet access to other companies and individuals.

L2TP—Layer 2 Tunneling Protocol. Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines features of two existing tunneling protocols: Cisco Layer 2 Forwarding (L2F) and Microsoft Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs.

MN—Mobile Node. The end-user’s mobile client device.

MS—Mobile Station

MSID—Mobile Station ID. The header field type for Wireless Application Protocol (WAP).

NAI—Network Access Identifier. A user identification string that appears in PPP and RADIUS authentication and accounting requests.

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).

PAP—Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP is supported only on PPP lines. Compare with CHAP.

PCF—Packet Control Function.

PDSN—Packet Data Serving Node. The gateway between CDMA2000 Radio Access Network (RAN) and the Internet.

PPP—Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

RADIUS—Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

SESM—Cisco Subscriber Edge Services Manager. Cisco SESM is part of a Cisco solution that allows subscribers of DSL, cable, wireless, and dialup to simultaneously access multiple services provided by different Internet service providers, application service providers, and Corporate Access Servers.

SSG—Service Selection Gateway. SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services.

VPDN—Virtual Private Dialup Network. Also known as Virtual Private Dial Network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. VPDNs are a cost-effective method of establishing a long distance, point-to-point connection between remote dial users and a private network.

VSA—Vendor-Specific Attribute. An attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting attribute-value (AV) pair.

Note Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.