IP Services Gateway Overview

This chapter provides an overview of the IP Services Gateway (IPSG) product.

This chapter covers the following topics:

- Introduction, on page 1
- How it Works, on page 2
- In-line Services, on page 4
- Enhanced Feature Support, on page 4

Introduction

The IP Services Gateway (IPSG) is a stand-alone device capable of providing managed services to IP flows. The IPSG is situated on the network side of legacy, non-service capable GGSNs, PDSNs, HAs, and other subscriber management devices. The IPSG can provide per-subscriber services such as Enhanced Charging Service, Application Detection and Control, and others.

The IPSG allows the carrier to roll out advanced services without requiring a replacement of the HA, PDSN, GGSN, or other access gateways and eliminates the need to add multiple servers to support additional services.

IPSG only requires a RADIUS request (access and accounting messages) with all the required mandatory attributes to create a session. Currently, IPSG supports GGSN (2G, 3G), PDSN, HA, Broadband Remote Access Server (B-RAS). IPSG does not support the radio access types (RAT) of 4G (EUTRAN) and Wi-Fi and hence cannot be deployed with P-GW (with 4G, Wi-Fi access, 2G/3G SGSN based RATs).

Important Pre StarOS Release 21.3, IPSG supported only for 3G RAT type. From StarOS Release 21.3, 4G RAT Type and EPS QoS is supported. Support has been extended for IPSG to operate in the 4G RAT environment which enables IPSG to act as an inline service agent in the core 4G network.

For the list of AAA attributes supported by IPSG, refer to the *IP Services Gateway AAA AVP Support* appendix.

Qualified Platforms

IPSG is a StarOS™ application that runs on Cisco® ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

The IP Services Gateway is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on licensing requirements.

For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

How it Works

The IPSG supports the following service modes:

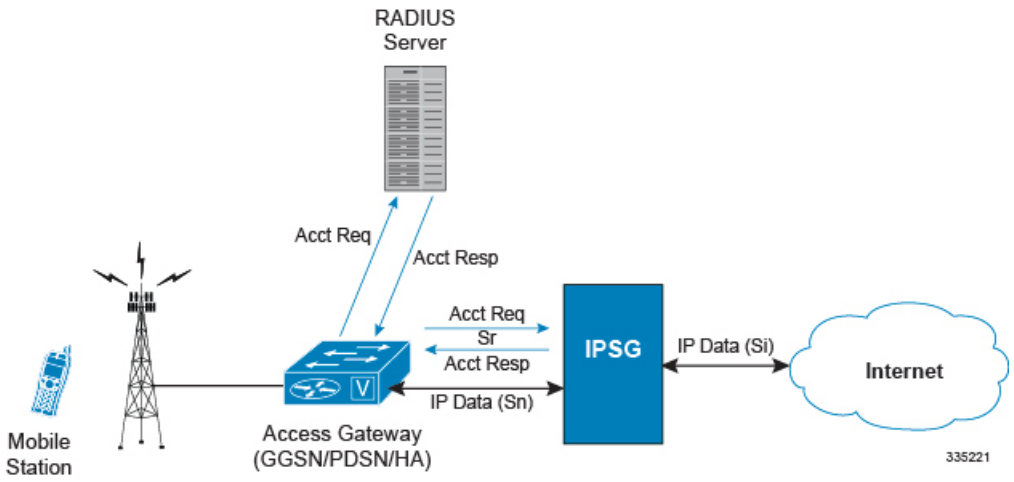
- RADIUS Server Mode, on page 2
- RADIUS Snoop Mode, on page 3

RADIUS Server Mode

When configured in RADIUS server mode, the IPSG inspects identical RADIUS accounting request packets sent to the RADIUS accounting server and the IPSG simultaneously.

As shown in the following figure, the IPSG inspects the RADIUS accounting request, extracts the required user information, then sends a RADIUS accounting response message back to the access gateway. The IPSG has three reference points: sn, si, and sr. The sn interface transmits/receives data packets to/from the access gateway (GGSN, HA, PDSN, etc.). The si interface transmits/receives data packets to/from the Internet or a packet data network. The sr interface receives RADIUS accounting requests from the access gateway. The system inspects the accounting request packets and extracts information to be used to determine the appropriate service(s) to apply to the flow.

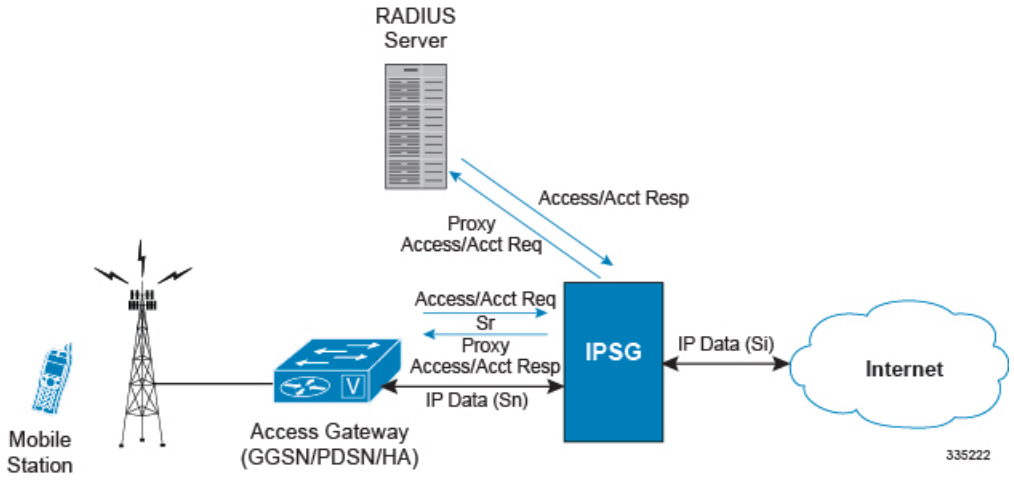
Figure 1: IPSG Message/Data Flow (RADIUS Server Mode)



RADIUS Proxy

In the event that the Access Gateway is incapable of sending two separate RADIUS Start messages, the IPSG can be configured as a RADIUS Proxy. As shown in the following figure, the IPSG receives an IPSG RADIUS proxy Access request, then generates the Authentication and Accounting requests to the AAA Server.

Figure 2: IPSG Message/Data Flow (RADIUS Server Mode - RADIUS Proxy)

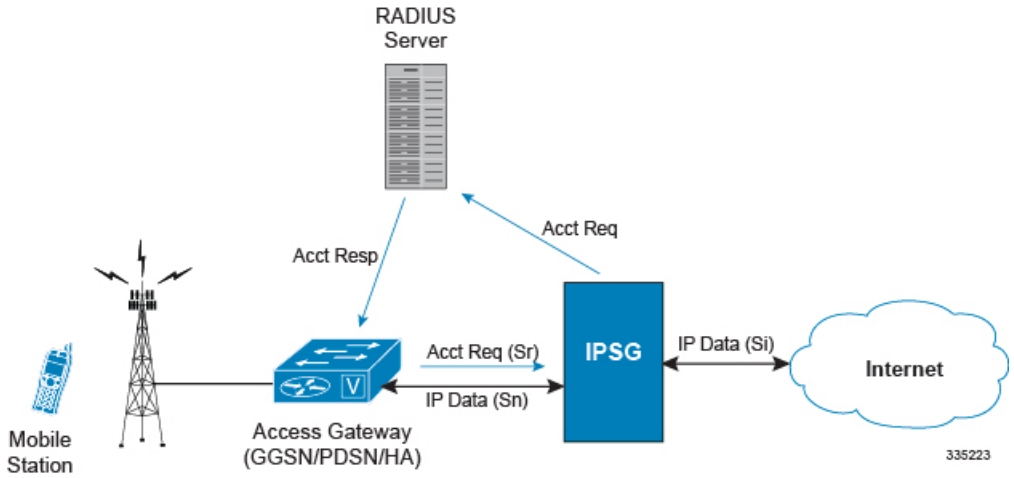


RADIUS Snoop Mode

When configured in RADIUS snoop mode, the IPSG simply inspects RADIUS accounting request packets sent to a RADIUS server through the IPSG.

As shown in the following figure, the IPSG has three reference points: sn, si, and sr. The sn interface transmits/receives data packets to/from the access gateway (GGSN, HA, PDSN, etc.). The si interface transmits/receives data packets to/from the Internet or a packet data network. The sr interface receives RADIUS accounting requests from the access gateway. The system inspects the accounting request packets and extracts information to be used to determine the appropriate service(s) to apply to the flow. Information is not extracted from the RADIUS accounting responses so they are sent directly to the access gateway by the RADIUS Server, but can also be sent back through the IPSG.

Figure 3: IPSG Message/Data Flow (RADIUS Snoop Mode)



In-line Services

As described previously, the IPSG provides a method of inspecting RADIUS packets to discover user identity for the purpose of applying enhanced services to the subsequent data flow. Internal applications such as the Enhanced Charging Service, Content Filtering, and Application Detection and Control are primary features that take advantage of the IPSG service.

Application Detection and Control

Application Detection and Control (ADC) is an in-line service feature that detects peer-to-peer protocols in real time and applies actions such as permitting, blocking, charging, bandwidth control, and TOS marking.

For more information, refer to the *Application Detection and Control Administration Guide*.

Content Filtering

Content Filtering is an in-line service feature that filters HTTP and WAP requests from mobile subscribers based on the URLs in the requests. This enables operators to filter and control the content that an individual subscriber can access, so that subscribers are inadvertently not exposed to universally unacceptable content and/or content inappropriate as per the subscribers' preferences.

For more information, refer to the *Content Filtering Services Administration Guide*.

Enhanced Charging Service

Enhanced Charging Service (ECS)/Active Charging Service (ACS) is the primary vehicle performing packet inspection and applying rules to the session which includes the delivery of enhanced services.

For more information, refer to the *Enhanced Charging Service Administration Guide*.

Enhanced Feature Support

This section describes the enhanced features supported by IPSG.

Accounting-On and Accounting-Off Messages

This feature introduces IPSG support for Accounting-On and Accounting-Off RADIUS accounting messages, in addition to the existing start, interim-update, and stop messages. The Accounting-On message sent by the peer RADIUS client indicates that the RADIUS client has restarted and is ready to accept calls.

An Accounting-Off message indicates that the peer RADIUS client is shutting down.

IPSG clears the existing subscriber sessions on receiving the Accounting-On/Off messages, and proxies the message to the RADIUS server (Proxy mode). The existing sessions are cleared based on the NAS-IP address of the subscriber that was assigned when the Acct-start message was created . If there is no NAS-IP-Address available, the peer IP address is considered as the NAS-IP-Address for the session. IPSG clears calls based on the NAS-IP address AVP in the Accounting-On/Off message irrespective of the origin of the message.

IPSG Server Mode

In the server mode, IPSG acts like the RADIUS server and on receiving an Accounting-On message, IPSG clears the existing sessions based on the NAS-IP address and sends a response to the RADIUS client.

When an Accounting-Off message is received, IPSG clears the existing sessions mapped to that NAS-IP address and sends a response to the client.

Only the first Accounting-On/Off message from the RADIUS client is addressed and the sessions are not cleared for retries. However, a response is sent to the RADIUS client for the retries.

IPSG Proxy Mode

In the proxy mode, when IPSG receives the Accounting-On/Off message from the RADIUS client, IPSG clears the subscriber sessions based on the NAS-IP address and proxies the message to the RADIUS server. IPSG then proxies the response from the RADIUS server back to the RADIUS client. Only the first Accounting-On/Off message from the RADIUS client is addressed. The corresponding messages are proxied directly to the RADIUS server and the response proxied back to the RADIUS client.

Cisco Ultra Traffic Optimization

In a high-bandwidth bulk data flow scenario, user experience is impacted due to various wireless network conditions and policies like shaping, throttling, and other bottlenecks that induce congestion, especially in the RAN. This results in TCP applying its saw-tooth algorithm for congestion control and impacts user experience, and overall system capacity is not fully utilized.

The Cisco Ultra Traffic Optimization solution provides clientless optimization of TCP and HTTP traffic. This solution is integrated with Cisco IPSG and has the following benefits:

- Increases the capacity of existing cell sites and therefore, enables more traffic transmission.
- Improves Quality of Experience (QoE) of users by providing more bits per second.
- Provides instantaneous stabilizing and maximizing per subscriber throughput, particularly during network congestion.

For detailed information on Cisco Ultra Traffic Optimization solution, refer to the *Cisco Ultra Traffic Optimization* chapter in the *IPSG Administration Guide*.

Content Service Steering

Content Service Steering (CSS), defines how traffic is handled by the system based on the content of the data presented by a mobile subscriber. CSS can be used to direct traffic to in-line services that are internal to the system. CSS controls how subscriber data is forwarded to a particular in-line service, but does not control the content.

IPSG supports steering subscriber sessions to Content Filtering Service based on their policy setting. If a subscriber does not have a policy setting (ACL name) requiring Content Filtering, their session will bypass the Content Filtering Service and will be routed on to the destination address.

If subscriber policy entitlements indicate that filtering is required for a subscriber, CSS is used to steer subscriber sessions to the Content Filtering in-line service.

If a subscriber is using a mobile application with protocol type not supported, their session will bypass the Content Filtering Service and will be efficiently routed on to destination address.

For more information regarding CSS, refer to the *Content Service Steering* chapter in the *System Administration Guide*.

Dynamic RADIUS Extensions (Change of Authorization)

Dynamic RADIUS extension support provides operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

The system supports the configuration and use of the following dynamic RADIUS extensions:

- Change of Authorization: The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.
- Disconnect Message: The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the RADIUS Change of Authorization (CoA) extension.

Important For more information on dynamic RADIUS extensions support, refer the *CoA, RADIUS, and Session Redirection (Hotlining)* appendix of this guide.

Gx Interface Support

To support roaming IMS subscribers in a GPRS/UMTS network, the IPSG must be able to charge only for the amount of resources consumed by the particular IMS application and bandwidth used. The IPSG must also allow for the provisioning and control of the resources used by the IMS subscriber. To facilitate this, the IPSG supports the R7 Gx interface to a Policy Control and Charging Rule Function (PCRF).

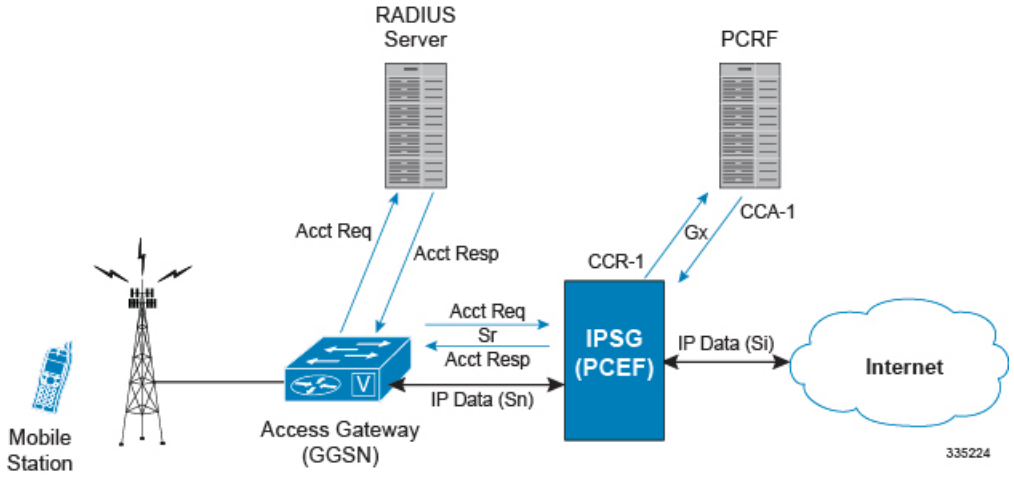
For detailed information on Gx Interface support, refer to the *Gx Interface Support* appendix in the *IP Services Gateway Administration Guide*.

Note the following for IPSG:

- Only single bearer/session concept is supported. Multiple bearer concept is not applicable.
- Only PCRF binding is applicable. PCEF binding is not applicable.

The following figure shows the interface and basic message flow of the Gx interface.

Figure 4: IPSG Message/Data Flow (RADIUS Server Mode - IMS Auth Service)



IPSG also supports IMS Authorization Service Session Recovery with the following limitations:

- Active calls only
- The number of rules recovered is limited to the following:
  - 3 flow-descriptions per charging-rule-definition
  - 3 Charging-rule-definitions per PDP context
- The above are combined limits for opened/closed gates and for uplink and downlink rules. IMSA sessions with rules more than the above are not recoverable.

Gy Interface Support

This is a Diameter protocol-based interface over which the IPSG communicates with a Charging Trigger Function (CTF) server that provides online charging data. Gy interface support provides an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an "online" or "prepaid" style. Both time- and volume-based charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.

For more information on Gy interface support, refer to the *Gy Interface Support* appendix in the *IP Services Gateway Administration Guide*.

Lawful Intercept

The Cisco Lawful Intercept feature is supported on the IPSG. Lawful Intercept is a license-enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity. For additional information and documentation on the Lawful Intercept feature, contact your Cisco account representative.

Multiple IPSG Services

Multiple IPSG services, can be configured on the system using different contexts. Each such IPSG service functions independently as an IPSG. Both source and destination contexts must be different for each IPSG service.

Overlapping IP Support over VLAN

Support for overlapping IP addresses for subscribers serviced by access networks on IPSG using VLANs is now possible through this feature. Overlapping IP addresses can be set up by defining multiple interfaces on the Sn interface (access side) and binding them to separate VLANs, while a single interface is setup to separate traffic using VPNv4 on the Si side (network side). When IPSG receives a packet, the appropriate session is identified based on the combination of IP address and VLAN. Currently, a maximum of 500 VLANs can be configured.

IPSG running on Cisco ASR 5500 acts as a BGPv4 peer (BGP proxy) per VLAN on the Sn interface, and MP-BGP peer on the Si interface. There can be 500 BGPv4 peers on the access side. IPSG can support a maximum of 64 BGP sessions per context, and hence 8 contexts are required to address 500 BGP sessions. On the Si interface, one VPNv4 per context is used, with a maximum of 8 VPNv4 contexts (if 8 contexts are used). The Sn and Si interfaces must be in the same context.

The session creation and deletion on IPSG is triggered on receiving the enriched AAA Accounting Start/Stop requests from the Cisco Account Register (CAR) AAA. The VLAN information is forwarded using the SN1-Assigned-VLAN-ID AVP.

This feature can be enabled using the CLI in the IPSG RADIUS Server Configuration Mode. Refer the *IP Services Gateway Configuration* chapter for configuration information.

Call Flows for Overlapping IP Support over VLAN

The following call flow illustration and descriptions explain how a session is created:

Figure 5: Session Creation Call Flow

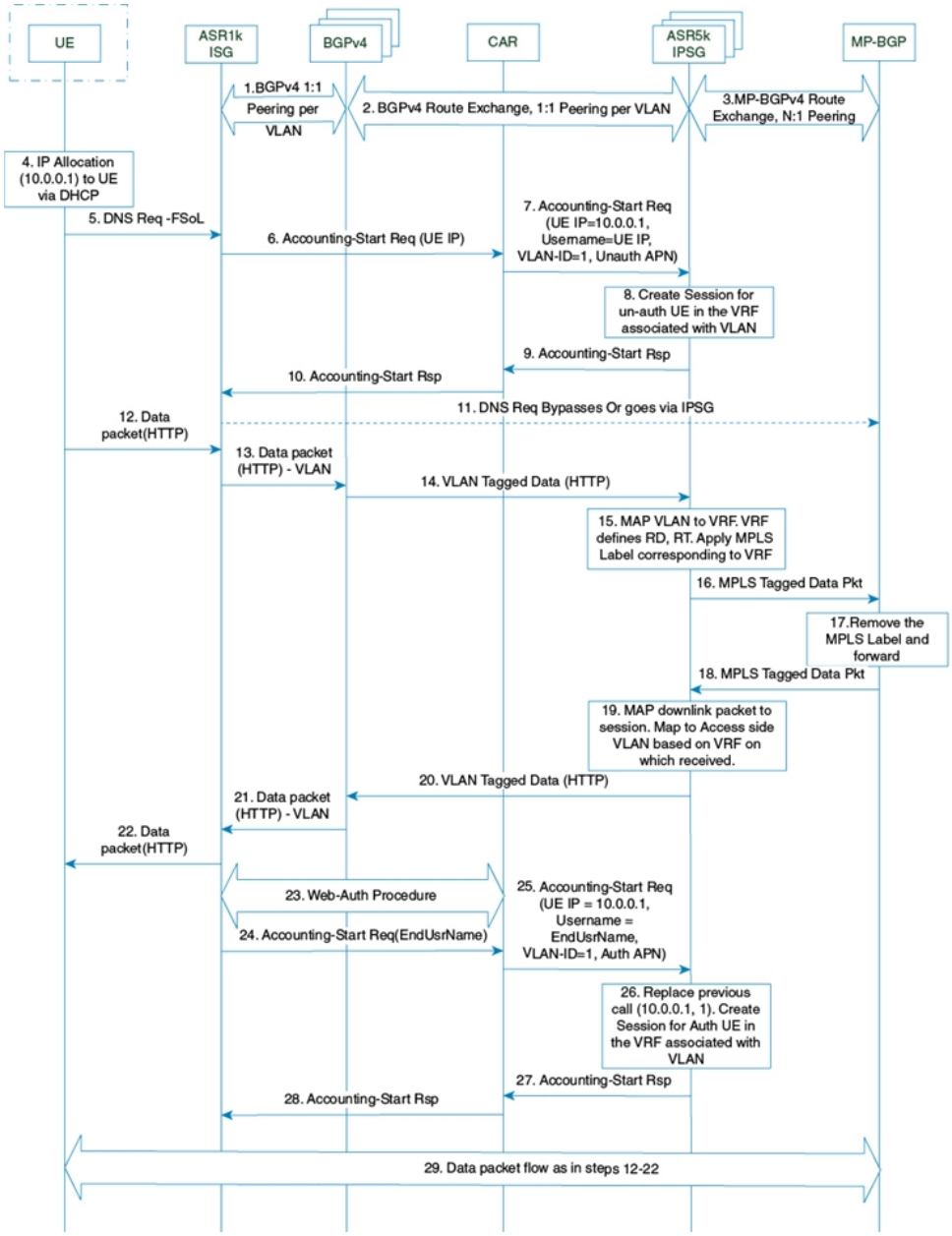


Table 1: Session Creation Call Flow Descriptions

Step	Description
1—3	BGP peering is established and routes exchange between ISG, BGPv4 routers, IPSG and MP-BGP router.

Step	Description
6—10	**Unauthenticated Phase**: In the pre-auth stage, the applicable username and other attributes pertaining to the subscriber are not available. The session creation request (Accounting-Start Req) at IPSG contains Username=UE IP (this should be string type), Framed-IP-Address=UE IP, Calling-Station-Id="000000000000000", 3GPP-IMSI="000000000000000", SN-Assigned-VLAN-ID=VlanId, Called-Station-Id="UnauthEud"; 3GPP-RAT-Type="UTRAN".
12—22	HTTP redirection occurs at IPSG.
23	The user between the ISG and CAR/SIS is authenticated using and user credentials like EndUserName, EndUserId used for 3GPP-IMSI , Calling-Station-id, auth APN to be used etc are obtained.
24—28	ISG/CAR send a new Accounting Start with the actual user credentials obtained from CAR/SIS subsystems. The same IP address and VLAN ID used during the un-phase is used again. The Username, Calling-Station-Id and APN are updated to reflect the actual user credentials. The replacement feature at IPSG based on diff-key is enabled at IPSG so the new session request replaces the earlier one for the same IP and VLAN-ID. Otherwise, ISG/CAR sends an Accounting-Stop for the previous session created for the un-authenticated user before sending the Accounting-Start for the authenticated user.
29	The uplink and downlink data call flow is same as steps 12-22, where the VLAN tagged data on the Sn interface is mapped to the MPLS tagged data on the Si side and vice-versa.

Dictionary Requirements

This section provides AVP requirements for the overlapping IP support over VLAN feature.

The following are the AVPs required, based on dictionaries starent-vsa1 or custom54

AVP	STARENT-VSA1	CUSTOM54	Additional Information
Acct-Status-Type	Mandatory	Mandatory	—

AVP	STARENT-VSA1	CUSTOM54	Additional Information
User-Name	Mandatory	Optional	For custom54, if present, this AVP is used. Otherwise, a default value "void" is used as the username in ipsgmgr.
Calling-Station-Id	Optional	Mandatory	For starent-vsa1, this AVP will be set to null and processed in ipsgmgr.
Framed-Ip-Address	Mandatory	Mandatory	Optional if an IPv6 prefix exists. Optional for Radio Access requests.
Acct-Session-Id	Mandatory	Mandatory	Optional for Radio Access requests.
Called-Station-Id	Mandatory	Mandatory	Optional for Subscriber profile and Radio Access requests.
SN-Assigned-VLAN-ID	Mandatory	Mandatory	This AVP is used to forward the VLAN ID.
SN-Transparent-Data	Optional	Optional	—
SN-Vpn-Name	Mandatory	Mandatory	This AVP is used to forward the VPN name (destination context).

Radius Client IP Validation

This feature enables IPSG to validate RADIUS accounting messages from different configured RADIUS client IP addresses, and forward requests to the session manager.

In an architecture where multiple sites of IPSG and Radius Proxies exist, GGSN forwards RADIUS accounting messages to IPSG through its Radius Proxy. In an event where the Radius Proxy is unreachable, GGSN forwards subsequent messages using the RADIUS Proxy belonging to another site. IPSG updates the RADIUS client IP in the subscriber session, and forwards all control messages from the session manager to the alternate client.

This feature can be enabled using the **validate-client-ip** keyword in the **radius accounting** command under the IPSG RADIUS Server Configuration Mode. By default, the RADIUS client IPs are validated, and can be disabled using the **disable radius accounting validate-client-ip** command.

Session Recovery

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes (for example, Session Manager and AAA Manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (for example, a Session Manager task aborts). The system spawns new instances of "standby mode" session and AAA Managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN Manager, are performed on a physically separate packet processing card to ensure that a double software fault (for example, Session Manager and VPN Manager fails at same time on same card) cannot occur. The packet processing card used to host the VPN Manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

For more information on Session Recovery, refer to the *Session Recovery* chapter in the *System Administration Guide*.

Note that the Inter-Chassis Session Recovery feature is not supported in this release.